SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 April 2026

Generated on 29 April 2026

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-33819	Deserialization of untrusted data in Microsoft Bing allows an unauthorized attacker to execute code over a network.	10.0	More Details
CVE-2026-35431	Server-side request forgery (ssrf) in Microsoft Entra ID Entitlement Management allows an unauthorized attacker to perform spoofing over a network.	10.0	More Details
CVE-2026-41679	Paperclip is a Node.js server and React UI that orchestrates a team of AI agents to run a business. Prior to version 2026.416.0, an unauthenticated attacker can achieve full remote code execution on any network-accessible Paperclip instance running in `authenticated` mode with default configuration. No user interaction, no credentials, just the target's address. The chain consists of six API calls. The attack is fully automated, requires no user interaction, and works against the default deployment configuration. Version 2026.416.0 patches the issue.	10.0	More Details
CVE-2026-33453	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Apache Camel Camel-Coap component. Apache Camel's camel-coap component is vulnerable to Camel message header injection, leading to remote code execution when routes forward CoAP requests to header-sensitive producers (e.g. camel-exec) The camel-coap component maps incoming CoAP request URI query parameters directly into Camel Exchange In message headers without applying any HeaderFilterStrategy. Specifically, CamelCoapResource.handleRequest() iterates over OptionSet.getUriQuery() and calls camelExchange.getIn().setHeader(...) for every query parameter. CoAPEndpoint extends DefaultEndpoint rather than DefaultHeaderFilterStrategyEndpoint, and CoAPComponent does not implement HeaderFilterStrategyComponent; the component contains no references to HeaderFilterStrategy at all. As a result, an unauthenticated attacker who can send a single CoAP UDP packet to a Camel route consuming from coap:// can inject arbitrary Camel internal headers (those prefixed with Camel*) into the Exchange. When the route delivers the message to a header-sensitive producer such as camel-exec, camel-sql, camel-bean, camel-file, or template components (camel-freemarker, camel-velocity), the injected headers can alter the producer's behavior. In the case of camel-exec, the CamelExecCommandExecutable and CamelExecCommandArgs headers override the executable and arguments configured on the endpoint, resulting in arbitrary OS command execution under the privileges of the Camel process. The producer's output is written back to the Exchange body and returned in the CoAP response payload by CamelCoapResource, giving the attacker an interactive RCE channel without any need for out-of-band exfiltration. Exploitation prerequisites are minimal: a single unauthenticated UDP datagram to the CoAP port (default 5683). CoAP (RFC 7252) has no built-in authentication, and DTLS is optional and disabled by default. Because the protocol is UDP-based, HTTP-layer WAF/IDS controls do not apply. This issue affects Apache Camel: from 4.14.0 through 4.14.5, from 4.18.0 before 4.18.1, 4.19.0. Users are recommended to upgrade to version 4.18.1 or 4.19.0, fixing the issue.	10.0	More Details
CVE-2026-41478	Saltcorn is an extensible, open source, no-code database application builder. Prior to 1.4.6, 1.5.6, and 1.6.0-beta.5, a SQL injection vulnerability in Saltcorn's mobile-sync routes allows any authenticated low-privilege user with read access to at least one table to inject arbitrary SQL through sync parameters. This can lead to full database exfiltration, including admin password hashes and configuration secrets, and may also enable database modification or destruction depending on the backend. This vulnerability is fixed in 1.4.6, 1.5.6, and 1.6.0-beta.5.	9.9	More Details
	A critical XSS vulnerability affected hackage-server and hackage.haskell.org. HTML and JavaScript files provided in source packages or via the documentation upload facility were served as-is on the main hackage.haskell.org		

CVE-2026-40470	domain. As a consequence, when a user with latent HTTP credentials browses to the package pages or documentation uploaded by a malicious package maintainer, their session can be hijacked to upload packages or documentation, amend maintainers or other package metadata, or perform any other action the user is authorised to do.	9.9	More Details
CVE-2026-21515	Exposure of sensitive information to an unauthorized actor in Azure IOT Central allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2026-39440	Improper Control of Generation of Code ('Code Injection') vulnerability in Funnelforms LLC FunnelFormsPro allows Remote Code Inclusion.This issue affects FunnelFormsPro: from n/a through 3.8.1.	9.9	More Details
CVE-2026-40453	The fix for CVE-2025-27636 added setLowerCase(true) to HttpHeaderFilterStrategy so that case-variant header names such as 'CAmelExecCommandExecutable' are filtered out alongside 'CamelExecCommandExecutable'. The same setLowerCase(true) call was not applied to five non-HTTP HeaderFilterStrategy implementations: JmsHeaderFilterStrategy and ClassicJmsHeaderFilterStrategy in camel-jms, SjmsHeaderFilterStrategy in camel-sjms, CoAPHeaderFilterStrategy in camel-coap, and GooglePubsubHeaderFilterStrategy in camel-google-pubsub. Because those strategies use case-sensitive String.startsWith('Camel'/'camel') filtering while the Camel Exchange stores headers in a case-insensitive map, an attacker with JMS (or equivalent) producer access to the broker consumed by a Camel route can inject case-variant Camel internal headers, which are then resolved by downstream components such as camel-exec and camel-file using their canonical casing. This enables remote code execution and arbitrary file write on routes that forward JMS messages to header-driven components. This issue affects Apache Camel: from 3.0.0 before 4.14.6, from 4.15.0 before 4.18.2, from 4.19.0 before 4.20.0. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.2.	9.9	More Details
CVE-2026-41228	Froxlor is open source server administration software. Prior to version 2.3.6, the Froxlor API endpoint `Customers.update` (and `Admins.update`) does not validate the `def_language` parameter against the list of available language files. An authenticated customer can set `def_language` to a path traversal payload (e.g., `../../../../../var/customers/webs/customer1/evil`), which is stored in the database. On subsequent requests, `Language::loadLanguage()` constructs a file path using this value and executes it via `require`, achieving arbitrary PHP code execution as the web server user. Version 2.3.6 fixes the issue.	9.9	More Details
CVE-2026-40472	In hackage-server, user-controlled metadata from .cabal files are rendered into HTML href attributes without proper sanitization, enabling stored Cross-Site Scripting (XSS) attacks.	9.9	More Details
CVE-2026-7240	A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setVpnAccountCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument User leads to os command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-7241	A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setWiFiBasicCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument wifiOff results in os command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-7242	A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setOpenVpnClientCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument enabled can lead to os command injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-41898	rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.9.24 to before 0.10.78, the FFI trampolines behind SslContextBuilder::set_psk_client_callback, set_psk_server_callback, set_cookie_generate_cb, and set_stateless_cookie_generate_cb forwarded the user closure's returned usize directly to OpenSSL without checking it against the &mut [u8] that was handed to the closure. This can lead to buffer overflows and other unintended consequences. This vulnerability is fixed in 0.10.78.	9.8	More Details
CVE-2026-41681	rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.10.39 to before 0.10.78, EVP_DigestFinal() always writes EVP_MD_CTX_size(ctx) to the out buffer. If out is smaller than that, MdCtxRef::digest_final() writes past its end, usually corrupting the stack. This is reachable from safe Rust. This vulnerability is fixed in 0.10.78.	9.8	More Details
CVE-2026-41678	rust-openssl provides OpenSSL bindings for the Rust programming language. From to before 0.10.78, aes::unwrap_key() contains an incorrect assertion: it checks that out.len() + 8 <= in_.len(), but this condition is reversed. The intended invariant is out.len() >= in_.len() - 8, ensuring the output buffer is large enough. Because of the inverted check, the function only accepts buffers at or below the minimum required size and rejects larger ones. If a smaller buffer is provided the function will write past the end of out by in_.len() - 8 - out.len() bytes, causing an out-of-bounds write from a safe public function. This vulnerability is fixed in 0.10.78.	9.8	More Details
CVE-2026-7243	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function setRadvdCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument maxRtrAdvInterval leads to os command injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-41676	rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.9.27 to before 0.10.78, Deriver::derive (and PkeyCtxRef::derive) sets len = buf.len() and passes it as the in/out length to EVP_PKEY_derive, relying on OpenSSL to honor it. On OpenSSL 1.1.x, X25519, X448, DH and HKDF-extract ignore the incoming *keylen, unconditionally writing the full shared secret (32/56/prime-size bytes). A caller passing a short slice gets a heap/stack overflow from safe code. OpenSSL 3.x providers do check, so this only impacts older OpenSSL. This vulnerability is fixed in 0.10.78.	9.8	More Details

CVE-2026-31609	In the Linux kernel, the following vulnerability has been resolved: smb: client: avoid double-free in smbd_free_send_io() after smbd_send_batch_flush() smbd_send_batch_flush() already calls smbd_free_send_io(), so we should not call it again after smbd_post_send() moved it to the batch list.	9.8	More Details
CVE-2026-39920	BridgeHead FileStore versions prior to 24A (released in early 2024) expose the Apache Axis2 administration module on network-accessible endpoints with default credentials that allows unauthenticated remote attackers to execute arbitrary OS commands. Attackers can authenticate to the admin console using default credentials, upload a malicious Java archive as a web service, and execute arbitrary commands on the host via SOAP requests to the deployed service.	9.8	More Details
CVE-2026-6911	Missing JWT signature verification in AWS Ops Wheel allows unauthenticated attackers to forge JWT tokens and gain unintended administrative access to the application, including the ability to read, modify, and delete all application data across tenants and manage Cognito user accounts within the deployment's User Pool, via a crafted JWT sent to the API Gateway endpoint. To remediate this issue, users should redeploy from the updated repository and ensure any forked or derivative code is patched to incorporate the new fixes.	9.8	More Details
CVE-2026-31669	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix slab-use-after-free in __inet_lookup_established The ehash table lookups are lockless and rely on SLAB_TYPESAFE_BY_RCU to guarantee socket memory stability during RCU read-side critical sections. Both tcp_prot and tcpv6_prot have their slab caches created with this flag via proto_register(). However, MPTCP's mptcp_subflow_init() copies tcpv6_prot into tcpv6_prot_override during inet_init() (fs_initcall, level 5), before inet6_init() (module_init/device_initcall, level 6) has called proto_register(&tcpv6_prot). At that point, tcpv6_prot.slab is still NULL, so tcpv6_prot_override.slab remains NULL permanently. This causes MPTCP v6 subflow child sockets to be allocated via kmalloc (falling into kmalloc-4k) instead of the TCPv6 slab cache. The kmalloc-4k cache lacks SLAB_TYPESAFE_BY_RCU, so when these sockets are freed without SOCK_RCU_FREE (which is cleared for child sockets by design), the memory can be immediately reused. Concurrent ehash lookups under rcu_read_lock can then access freed memory, triggering a slab-use-after-free in __inet_lookup_established. Fix this by splitting the IPv6-specific initialization out of mptcp_subflow_init() into a new mptcp_subflow_v6_init(), called from mptcp_proto_v6_init() before protocol registration. This ensures tcpv6_prot_override.slab correctly inherits the SLAB_TYPESAFE_BY_RCU slab cache.	9.8	More Details
CVE-2026-31668	In the Linux kernel, the following vulnerability has been resolved: seg6: separate dst_cache for input and output paths in seg6 lwtunnel The seg6 lwtunnel uses a single dst_cache per encap route, shared between seg6_input_core() and seg6_output_core(). These two paths can perform the post-encap SID lookup in different routing contexts (e.g., ip rules matching on the ingress interface, or VRF table separation). Whichever path runs first populates the cache, and the other reuses it blindly, bypassing its own lookup. Fix this by splitting the cache into cache_input and cache_output, so each path maintains its own cached dst independently.	9.8	More Details
CVE-2026-31659	In the Linux kernel, the following vulnerability has been resolved: batman-adv: reject oversized global TT response buffers batadv_tt_prepare_tvlv_global_data() builds the allocation length for a global TT response in 16-bit temporaries. When a remote originator advertises a large enough global TT, the TT payload length plus the VLAN header offset can exceed 65535 and wrap before kmalloc(). The full-table response path still uses the original TT payload length when it fills tt_change, so the wrapped allocation is too small and batadv_tt_prepare_tvlv_global_data() writes past the end of the heap object before the later packet-size check runs. Fix this by rejecting TT responses whose TVLV value length cannot fit in the 16-bit TVLV payload length field.	9.8	More Details
CVE-2026-31657	In the Linux kernel, the following vulnerability has been resolved: batman-adv: hold claim backbone gateways by reference batadv_bla_add_claim() can replace claim->backbone_gw and drop the old gateway's last reference while readers still follow the pointer. The netlink claim dump path dereferences claim->backbone_gw->orig and takes claim->backbone_gw->crc_lock without pinning the underlying backbone gateway. batadv_bla_check_claim() still has the same naked pointer access pattern. Reuse batadv_bla_claim_get_backbone_gw() in both readers so they operate on a stable gateway reference until the read-side work is complete. This keeps the dump and claim-check paths aligned with the lifetime rules introduced for the other BLA claim readers.	9.8	More Details
CVE-2026-31649	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix integer underflow in chain mode The jumbo_frm() chain-mode implementation unconditionally computes len = nopaged_len - bmax; where nopaged_len = skb_headlen(skb) (linear bytes only) and bmax is BUF_SIZE_8KiB or BUF_SIZE_2KiB. However, the caller stmmac_xmit() decides to invoke jumbo_frm() based on skb->len (total length including page fragments): is_jumbo = stmmac_is_jumbo_frm(priv, skb->len, enh_desc); When a packet has a small linear portion (nopaged_len <= bmax) but a large total length due to page fragments (skb->len > bmax), the subtraction wraps as an unsigned integer, producing a huge len value (~0xFFFFxxxx). This causes the while (len != 0) loop to execute hundreds of thousands of iterations, passing skb->data + bmax * i pointers far beyond the skb buffer to dma_map_single(). On IOMMU-less SoCs (the typical deployment for stmmac), this maps arbitrary kernel memory to the DMA engine, constituting a kernel memory disclosure and potential memory corruption from hardware. Fix this by introducing a buf_len local variable clamped to min(nopaged_len, bmax). Computing len = nopaged_len - buf_len is then always safe: it is zero when the linear portion fits within a single descriptor, causing the while (len != 0) loop to be skipped naturally, and the fragment loop in stmmac_xmit() handles page fragments afterward.	9.8	More Details
CVE-2026-31637	In the Linux kernel, the following vulnerability has been resolved: rxrpc: reject undecryptable rxkad response tickets rxkad_decrypt_ticket() decrypts the RXKAD response ticket and then parses the buffer as plaintext without checking whether crypto_skcipher_decrypt() succeeded. A malformed RESPONSE can therefore use a non-block-aligned ticket length, make the decrypt operation fail, and still drive the ticket parser with attacker-controlled bytes. Check the decrypt result and abort the connection with RXKADBADTICKET when ticket decryption fails.	9.8	More Details
CVE-2026-7244	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setWiFiEasyGuestCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument merge results in os command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix integer overflow in		

CVE-2026-31633	rxgk_verify_response() In rxgk_verify_response(), there's a potential integer overflow due to rounding up token_len before checking it, thereby allowing the length check to be bypassed. Fix this by checking the unrounded value against len too (len is limited as the response must fit in a single UDP packet).	9.8	More Details
CVE-2026-31608	In the Linux kernel, the following vulnerability has been resolved: smb: server: avoid double-free in smb_direct_free_sendmsg after smb_direct_flush_send_list() smb_direct_flush_send_list() already calls smb_direct_free_sendmsg(), so we should not call it again after post_sendmsg() moved it to the batch list.	9.8	More Details
CVE-2026-31607	In the Linux kernel, the following vulnerability has been resolved: usbip: validate number_of_packets in usbip_pack_ret_submit() When a USB/IP client receives a RET_SUBMIT response, usbip_pack_ret_submit() unconditionally overwrites urb->number_of_packets from the network PDU. This value is subsequently used as the loop bound in usbip_recv_iso() and usbip_pad_iso() to iterate over urb->iso_frame_desc[], a flexible array whose size was fixed at URB allocation time based on the *original* number_of_packets from the CMD_SUBMIT. A malicious USB/IP server can set number_of_packets in the response to a value larger than what was originally submitted, causing a heap out-of-bounds write when usbip_recv_iso() writes to urb->iso_frame_desc[i] beyond the allocated region. KASAN confirmed this with kernel 7.0.0-rc5: BUG: KASAN: slab-out-of-bounds in usbip_recv_iso+0x46a/0x640 Write of size 4 at addr ffff888106351d40 by task vhci_rx/69 The buggy address is located 0 bytes to the right of allocated 320-byte region [ffff888106351c00, ffff888106351d40) The server side (stub_rx.c) and gadget side (vudc_rx.c) already validate number_of_packets in the CMD_SUBMIT path since commits c6688ef9f297 ("usbip: fix stub_rx: harden CMD_SUBMIT path to handle malicious input") and b78d830f0049 ("usbip: fix vudc_rx: harden CMD_SUBMIT path to handle malicious input"). The server side validates against USBIP_MAX_ISO_PACKETS because no URB exists yet at that point. On the client side we have the original URB, so we can use the tighter bound: the response must not exceed the original number_of_packets. This mirrors the existing validation of actual_length against transfer_buffer_length in usbip_recv_xbuff(), which checks the response value against the original allocation size. Kelvin Mbogo's series ("usb: usbip: fix integer overflow in usbip_recv_iso()", v2) hardens the receive-side functions themselves; this patch complements that work by catching the bad value at its source -- in usbip_pack_ret_submit() before the overwrite -- and using the tighter per-URB allocation bound rather than the global USBIP_MAX_ISO_PACKETS limit. Fix this by checking rpdu->number_of_packets against urb->number_of_packets in usbip_pack_ret_submit() before the overwrite. On violation, clamp to zero so that usbip_recv_iso() and usbip_pad_iso() safely return early.	9.8	More Details
CVE-2026-31589	In the Linux kernel, the following vulnerability has been resolved: mm: call ->free_folio() directly in folio_unmap_invalidate() We can only call filemap_free_folio() if we have a reference to (or hold a lock on) the mapping. Otherwise, we've already removed the folio from the mapping so it no longer pins the mapping and the mapping can be removed, causing a use-after-free when accessing mapping->a_ops. Follow the same pattern as __remove_mapping() and load the free_folio function pointer before dropping the lock on the mapping. That lets us make filemap_free_folio() static as this was the only caller outside filemap.c.	9.8	More Details
CVE-2026-31536	In the Linux kernel, the following vulnerability has been resolved: smb: server: let send_done handle a completion without IB_SEND_SIGNALED With smbdirect_send_batch processing we likely have requests without IB_SEND_SIGNALED, which will be destroyed in the final request that has IB_SEND_SIGNALED set. If the connection is broken all requests are signaled even without explicit IB_SEND_SIGNALED.	9.8	More Details
CVE-2026-25660	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. Authentication bypass occurs when the URL ends with Authentication with certain function calls. This bypass allows assigning arbitrary permission to any user existing in CodeChecker. This issue affects CodeChecker: through 6.27.3.	9.8	More Details
CVE-2026-41492	Dgraph is an open source distributed GraphQL database. Prior to 25.3.3, Dgraphl exposes the process command line through the unauthenticated /debug/vars endpoint on Alpha. Because the admin token is commonly supplied via the --security "token=..." startup flag, an unauthenticated attacker can retrieve that token and replay it in the X-Dgraph-AuthToken header to access admin-only endpoints. This is a variant of the previously fixed /debug/pprof/cmdline issue, but the current fix is incomplete because it blocks only /debug/pprof/cmdline and still serves http.DefaultServeMux, which includes expvar's /debug/vars handler. This vulnerability is fixed in 25.3.3.	9.8	More Details
CVE-2026-7202	A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setWiFiWpsStart of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument wscDisabled leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-7204	A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setPptpServerCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument enable causes os command injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-7203	A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument enable results in os command injection. The attack can be launched remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-7154	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setAdvancedInfoShow of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument tty_server can lead to os command injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-7153	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setMiniuiHomeInfoShow of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument sys_info results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details

CVE-2026-7152	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument telnet_enabled leads to os command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-35903	MERCURY MIPC252W IP camera 1.0.5 Build 230306 Rel.79931n contains an improper authentication vulnerability in the RTSP service. After successful Digest authentication in an initial DESCRIBE request, the device does not verify the Digest response parameter in subsequent RTSP requests within the same session. As a result, RTSP methods such as SETUP, PLAY, and TEARDOWN can be processed even when the Authorization header contains an empty or invalid response value, as long as the nonce and session identifier correspond to a previously authenticated session. This allows an attacker with network access to reuse session parameters and issue unauthorized RTSP control commands without computing a valid Digest response.	9.8	More Details
CVE-2026-31255	A command injection vulnerability exists in Tenda AC18 V15.03.05.05_multi. The vulnerability is located in the /goform/SetSambaCfg interface, where improper handling of the guestuser parameter allows attackers to execute arbitrary system commands.	9.8	More Details
CVE-2026-7140	A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function CsteSystem of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument HTTP leads to os command injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-7139	A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setWiFiAclRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument mode causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2026-7138	A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setNtpCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument tz results in os command injection. The attack can be executed remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2026-7137	A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setStorageCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument sambaEnabled leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-7136	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. Affected by this issue is the function setDmzCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument wanIdx can lead to os command injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-41462	ProjeQtor versions 7.0 through 12.4.3 contain an unauthenticated SQL injection vulnerability in the login functionality where the login variable is directly concatenated into a SQL query without parameterization or sanitization. Attackers can inject arbitrary SQL expressions through the username field at the authentication endpoint to create privileged accounts, read sensitive data, and execute operating system commands if the database user has elevated permissions.	9.8	More Details
CVE-2026-30352	A remote code execution (RCE) vulnerability in the /devserver/start endpoint of leonvanzyl autocoder commit 79d02a allows attackers to execute arbitrary code via providing a crafted command parameter.	9.8	More Details
CVE-2026-7125	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. Affected by this issue is the function setWiFiEasyCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument merge leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-7124	A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. Affected by this vulnerability is the function setIpv6LanCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument addrPrefixLen can lead to os command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-7123	A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function setIptvCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument setIptvCfg results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-7122	A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This impacts the function setUPnPCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument enable leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-7121	A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument wizard causes os command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2026-22337	Incorrect Privilege Assignment vulnerability in Directorist Directorist Social Login allows Privilege Escalation.This issue affects Directorist Social Login: from n/a before 2.1.4.	9.8	More Details
CVE-2026-	The fix for CVE-2024-52046 in Apache MINA AbstractIoBuffer.getObject() was incomplete. The classname allowlist of classes allowed to be deserialized was applied too late after a static initializer in a class to be read might already have been executed. Affected versions are Apache MINA 2.0.0 <= 2.0.27, 2.1.0 <= 2.1.10, and 2.2.0 <= 2.2.5. The	9.8	More Details

41409	problem is resolved in Apache MINA 2.0.28, 2.1.11, and 2.2.6 by applying the classname allowlist earlier. Affected are applications using Apache MINA that call IoBuffer.getObject(). Applications using Apache MINA are advised to upgrade		
CVE-2026-41635	Apache MINA's AbstractIoBuffer.resolveClass() contains two branches, one of them (for static classes or primitive types) does not check the class at all, bypassing the classname allowlist and allowing arbitrary code to be executed. The fix checks if the class is present in the accepted class filter before calling Class.forName(). Affected versions are Apache MINA 2.0.0 <= 2.0.27, 2.1.0 <= 2.1.10, and 2.2.0 <= 2.2.5. The problem is resolved in Apache MINA 2.0.28, 2.1.11, and 2.2.6 by applying the classname allowlist earlier. Affected are applications using Apache MINA that call IoBuffer.getObject(). Applications using Apache MINA are advised to upgrade.	9.8	More Details
CVE-2026-40860	JmsBinding.extractBodyFromJms() in camel-jms, and the equivalent JmsBinding class in camel-sjms, deserialized the payload of incoming JMS ObjectMessage values via javax.jms.ObjectMessage.getObject() without applying any ObjectInputFilter, class allowlist or class denylist. Because this code path is reached whenever the mapJmsMessage option is enabled (the default) and Camel acts as a JMS consumer, an attacker able to publish a crafted ObjectMessage to a queue or topic consumed by a Camel application could achieve remote code execution when a deserialization gadget chain was present on the classpath. The same handling was reached transitively through camel-sjms2 (whose Sjms2Endpoint extends SjmsEndpoint) and through camel-amqp (whose AMQPJmsBinding extends JmsBinding), and by other JMS-family components built on JmsComponent such as camel-activemq and camel-activemq6. This issue affects Apache Camel: from 3.0.0 before 4.14.7, from 4.15.0 before 4.18.2, from 4.19.0 before 4.20.0. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.7. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.2.	9.8	More Details
CVE-2026-7037	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setVpnPassCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument pptpPassThru results in os command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-6951	Versions of the package simple-git before 3.36.0 are vulnerable to Remote Code Execution (RCE) due to an incomplete fix for [CVE-2022-25912](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-3112221) that blocks the -c option but not the equivalent --config form. If untrusted input can reach the options argument passed to simple-git, an attacker may still achieve remote code execution by enabling protocol.ext.allow=always and using an ext:: clone source.	9.8	More Details
CVE-2026-32644	Specific firmware versions of Milesight AIOT cameras use SSL certificates with default private keys.	9.8	More Details
CVE-2026-1951	Delta Electronics AS320T has no checking of the length of the buffer with the directory name vulnerability.	9.8	More Details
CVE-2026-1952	Delta Electronics AS320T has denial of service via the undocumented subfunction vulnerability.	9.8	More Details
CVE-2026-1950	Delta Electronics AS320T has No checking of the length of the buffer with the file name vulnerability.	9.8	More Details
CVE-2026-7156	A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function CsteSystem of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument HTTP results in os command injection. The attack may be launched remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2026-31175	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunEnable parameter to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-23751	Kofax Capture, now referred to as Tungsten Capture, version 6.0.0.0 (other versions may be affected) exposes a deprecated .NET Remoting HTTP channel on port 2424 via the Ascent Capture Service that is accessible without authentication and uses a default, publicly known endpoint identifier. An unauthenticated remote attacker can exploit .NET Remoting object unmarshalling techniques to instantiate a remote System.Net.WebClient object and read arbitrary files from the server filesystem, write attacker-controlled files to the server, or coerce NTLMv2 authentication to an attacker-controlled host, enabling sensitive credential disclosure, denial of service, remote code execution, or lateral movement depending on service account privileges and network environment.	9.8	More Details
CVE-2025-62373	Pipecat is an open-source Python framework for building real-time voice and multimodal conversational agents. Versions 0.0.41 through 0.0.93 have a vulnerability in `LivekitFrameSerializer` – an optional, non-default, undocumented frame serializer class (now deprecated) intended for LiveKit integration. The class's `deserialize()` method uses Python's `pickle.loads()` on data received from WebSocket clients without any validation or sanitization. This means that a malicious WebSocket client can send a crafted pickle payload to execute arbitrary code on the Pipecat server. The vulnerable code resides in `src/pipecat/serializers/livekit.py` (around line 73), where untrusted WebSocket message data is passed directly into `pickle.loads()` for deserialization. If a Pipecat server is configured to use LivekitFrameSerializer and is listening on an external interface (e.g. 0.0.0.0), an attacker on the network (or the internet, if the service is exposed) could achieve remote code execution (RCE) on the server by sending a malicious pickle payload. Version 0.0.94 contains a fix. Users of Pipecat should avoid or replace unsafe deserialization and improve network security configuration. The best mitigation is to stop using the vulnerable LivekitFrameSerializer altogether. Those who require LiveKit functionality should upgrade to the latest Pipecat version and switch to the recommended `LiveKitTransport` or another secure method provided by the framework. Additionally, always follow secure coding practices: never trust client-supplied data, and avoid Python pickle (or similar unsafe deserialization) in network-facing components.	9.8	More Details
CVE-2026-	Delta Electronics AS320T has incorrect calculation of the buffer size on the stack in the GET/PUT request handler of		

1949	the web service.	9.8	More Details
CVE-2026-41460	SocialEngine versions 7.8.0 and prior contain a SQL injection vulnerability in the /activity/index/get-memberall endpoint where user-supplied input passed via the text parameter is not sanitized before being incorporated into a SQL query. An unauthenticated remote attacker can exploit this vulnerability to read arbitrary data from the database, reset administrator account passwords, and gain unauthorized access to the Packages Manager in the Admin Panel, potentially enabling remote code execution.	9.8	More Details
CVE-2026-6887	Borg SPM 2007 (Sales Ended in 2008) developed by BorG Technology Corporation has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2026-6886	Borg SPM 2007 (Sales Ended in 2008) developed by BorG Technology Corporation has a Authentication Bypass vulnerability, allowing unauthenticated remote attackers to log into the system as any user.	9.8	More Details
CVE-2026-6885	Borg SPM 2007 (Sales Ended in 2008) developed by BorG Technology Corporation has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	9.8	More Details
CVE-2026-3844	The Breeze Cache plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'fetch_gravatar_from_remote' function in all versions up to, and including, 2.4.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. The vulnerability can only be exploited if "Host Files Locally - Gravatars" is enabled, which is disabled by default.	9.8	More Details
CVE-2026-41179	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Starting in version 1.48.0 and prior to version 1.73.5, the RC endpoint `operations/fsinfo` is exposed without `AuthRequired: true` and accepts attacker-controlled `fs` input. Because `rc.GetFs(...)` supports inline backend definitions, an unauthenticated attacker can instantiate an attacker-controlled backend on demand. For the WebDAV backend, `bearer_token_command` is executed during backend initialization, making single-request unauthenticated local command execution possible on reachable RC deployments without global HTTP authentication. Version 1.73.5 patches the issue.	9.8	More Details
CVE-2026-41176	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. The RC endpoint `options/set` is exposed without `AuthRequired: true`, but it can mutate global runtime configuration, including the RC option block itself. Starting in version 1.45.0 and prior to version 1.73.5, an unauthenticated attacker can set `rc.NoAuth=true`, which disables the authorization gate for many RC methods registered with `AuthRequired: true` on reachable RC servers that are started without global HTTP authentication. This can lead to unauthorized access to sensitive administrative functionality, including configuration and operational RC methods. Version 1.73.5 patches the issue.	9.8	More Details
CVE-2026-29198	In Rocket.Chat <8.3.0, <8.2.1, <8.1.2, <8.0.3, <7.13.5, <7.12.6, <7.11.6, and <7.10.9, a NoSQL injection vulnerability can lead to account takeover of the first user with a generated token when an OAuth app is configured.	9.8	More Details
CVE-2026-41873	** UNSUPPORTED WHEN ASSIGNED ** Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Pony Mail leading to admin account takeover. This issue affects all versions of the Lua implementation of Pony Mail. There is a Python implementation under development under the name "Pony Mail Foal" that is not affected by this issue, but hasn't been released yet. As the Lua implementation of this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2026-24178	NVIDIA NVFlare Dashboard contains a vulnerability in the user management and authentication system where an unauthenticated attacker may cause authorization bypass through user-controlled key. A successful exploit of this vulnerability may lead to privilege escalation, data tampering, information disclosure, code execution, and denial of service.	9.8	More Details
CVE-2026-34415	Xerte Online Toolkits versions 3.15 and earlier contain an incomplete input validation vulnerability in the elFinder connector endpoint that fails to block PHP-executable extensions .php4 due to an incorrect regex pattern. Unauthenticated attackers can exploit this flaw combined with authentication bypass and path traversal vulnerabilities to upload malicious PHP code, rename it with a .php4 extension, and execute arbitrary operating system commands on the server.	9.8	More Details
CVE-2018-25272	ELBA5 5.8.0 contains a remote code execution vulnerability that allows attackers to obtain database credentials and execute arbitrary commands with SYSTEM level permissions. Attackers can connect to the database using default connector credentials, decrypt the DBA password, and execute commands via the xp_cmdshell stored procedure or add backdoor users to the BEDIENER table.	9.8	More Details
CVE-2018-25270	ThinkPHP 5.0.23 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by invoking functions through the routing parameter. Attackers can craft requests to the index.php endpoint with malicious function parameters to execute system commands with application privileges.	9.8	More Details
CVE-2026-31501	In the Linux kernel, the following vulnerability has been resolved: net: ti: icssg-prueth: fix use-after-free of CPPI descriptor in RX path cppi5_hdesc_get_psdata() returns a pointer into the CPPI descriptor. In both emac_rx_packet() and emac_rx_packet_zc(), the descriptor is freed via k3_cppi_desc_pool_free() before the psdata pointer is used by emac_rx_timestamp(), which dereferences psdata[0] and psdata[1]. This constitutes a use-after-free on every received packet that goes through the timestamp path. Defer the descriptor free until after all accesses through the psdata pointer are complete. For emac_rx_packet(), move the free into the requeue label so both early-exit and success paths free the descriptor after all accesses are done. For emac_rx_packet_zc(), move the free to the end of	9.8	More Details

	the loop body after emac_dispatch_skb_zc() (which calls emac_rx_timestamp()) has returned.		
CVE-2026-31478	In the Linux kernel, the following vulnerability has been resolved: ksmbd: replace hardcoded hdr2_len with offsetof() in smb2_calc_max_out_buf_len() After this commit (e2b76ab8b5c9 "ksmbd: add support for read compound"), response buffer management was changed to use dynamic iov array. In the new design, smb2_calc_max_out_buf_len() expects the second argument (hdr2_len) to be the offset of ->Buffer field in the response structure, not a hardcoded magic number. Fix the remaining call sites to use the correct offsetof() value.	9.8	More Details
CVE-2026-31463	In the Linux kernel, the following vulnerability has been resolved: iomap: fix invalid folio access when i_blkbits differs from I/O granularity Commit aa35dd5cbc06 ("iomap: fix invalid folio access after folio_end_read()") partially addressed invalid folio access for folios without an ifs attached, but it did not handle the case where 1 << inode->i_blkbits matches the folio size but is different from the granularity used for the IO, which means IO can be submitted for less than the full folio for the !ifs case. In this case, the condition: if (*bytes_submitted == folio_len) ctx->cur_folio = NULL; in iomap_read_folio_iter() will not invalidate ctx->cur_folio, and iomap_read_end() will still be called on the folio even though the IO helper owns it and will finish the read on it. Fix this by unconditionally invalidating ctx->cur_folio for the !ifs case.	9.8	More Details
CVE-2026-31444	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free and NULL deref in smb_grant_oplock() smb_grant_oplock() has two issues in the oplock publication sequence: 1) opinfo is linked into ci->m_op_list (via opinfo_add) before add_lease_global_list() is called. If add_lease_global_list() fails (kmalloc returns NULL), the error path frees the opinfo via __free_opinfo() while it is still linked in ci->m_op_list. Concurrent m_op_list readers (opinfo_get_list, or direct iteration in smb_break_all_levII_oplock) dereference the freed node. 2) opinfo->o_fp is assigned after add_lease_global_list() publishes the opinfo on the global lease list. A concurrent find_same_lease_key() can walk the lease list and dereference opinfo->o_fp->f_ci while o_fp is still NULL. Fix by restructuring the publication sequence to eliminate post-publish failure: - Set opinfo->o_fp before any list publication (fixes NULL deref). - Preallocate lease_table via alloc_lease_table() before opinfo_add() so add_lease_global_list() becomes infallible after publication. - Keep the original m_op_list publication order (opinfo_add before lease list) so concurrent opens via same_client_has_lease() and opinfo_get_list() still see the in-flight grant. - Use opinfo_put() instead of __free_opinfo() on err_out so that the RCU-deferred free path is used. This also requires splitting add_lease_global_list() to take a preallocated lease_table and changing its return type from int to void, since it can no longer fail.	9.8	More Details
CVE-2026-31436	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix possible wrong descriptor completion in llist_abort_desc() At the end of this function, d is the traversal cursor of flist, but the code completes found instead. This can lead to issues such as NULL pointer dereferences, double completion, or descriptor leaks. Fix this by completing d instead of found in the final list_for_each_entry_safe() loop.	9.8	More Details
CVE-2026-6235	The Sendmachine for WordPress plugin for WordPress is vulnerable to authorization bypass via the 'manage_admin_requests' function in all versions up to, and including, 1.0.20. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to overwrite the plugin's SMTP configuration, which can be leveraged to intercept all outbound emails from the site (including password reset emails).	9.8	More Details
CVE-2026-41304	WWBN AVideo is an open source video platform. In versions 29.0 and below, the `cloneServer.json.php` endpoint in the CloneSite plugin constructs shell commands using user-controlled input (`url` parameter) without proper sanitization. The input is directly concatenated into a `wget` command executed via `exec()`, allowing command injection. An attacker can inject arbitrary shell commands by breaking out of the intended URL context using shell metacharacters (e.g., `;`). This leads to Remote Code Execution (RCE) on the server. Commit 473c609fc2defdea8b937b00e86ce88eba1f15bb contains a fix.	9.8	More Details
CVE-2026-39087	An issue in Ntfy ntfy.sh before v.2.21 allows a remote attacker to execute arbitrary code via the parseActions function	9.8	More Details
CVE-2025-50229	Jizhicms v2.5.4 is vulnerable to SQL injection in the product editing module.	9.8	More Details
CVE-2026-31177	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunMinAlive parameter to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-41265	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the specific flaw exists within the run method of the Airtable_Agents class. The issue results from the lack of proper sandboxing when evaluating an LLM generated python script. Using prompt injection techniques, an unauthenticated attacker with the ability to send prompts to a chatflow using the Airtable Agent node may convince an LLM to respond with a malicious python script that executes attacker controlled commands on the flowise server. This vulnerability is fixed in 3.1.0.	9.8	More Details
CVE-2026-33078	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Versions prior to 8.2.6.4 have a SQL injection vulnerability in the haproxy_section_save function in app/routes/config/routes.py. The server_ip parameter, sourced from the URL path, is passed unsanitized through multiple function calls and ultimately interpolated into a SQL query string using Python string formatting, allowing attackers to execute arbitrary SQL commands. Version 8.2.6.4 fixes the issue.	9.8	More Details
CVE-2026-33076	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to version 8.2.6.4, the haproxy_section_save interface presents a vulnerability that could lead to remote code execution due to path traversal and writing into scheduled tasks. Version 8.2.6.4 fixes the issue.	9.8	More Details
CVE-2026-40630	A vulnerability in SenseLive X3050’s web management interface allows unauthorized access to certain configuration endpoints due to improper access control enforcement. An attacker with network access to the device may be able to bypass the intended authentication mechanism and directly interact with sensitive configuration functions.	9.8	More Details

CVE-2026-40620	A vulnerability in SenseLive X3050’s embedded management service allows full administrative control to be established without any form of authentication or authorization on the SenseLive config application. The service accepts management connections from any reachable host, enabling unrestricted modification of critical configuration parameters, operational modes, and device state through a vendor-supplied or compatible client.	9.8	More Details
CVE-2026-35503	A vulnerability in SenseLive X3050’s web management interface allows authentication logic to be performed entirely on the client side, relying on hardcoded values within browser-executed scripts rather than server-side verification. An attacker with access to the login page could retrieve these exposed parameters and gain unauthorized access to administrative functionality.	9.8	More Details
CVE-2026-7248	A vulnerability was found in D-Link DI-8100 16.07.26A1. This affects the function tgfile_htm of the file tgfile.htm of the component CGI Endpoint. The manipulation of the argument fn results in buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-25775	A vulnerability in SenseLive X3050’s remote management service allows firmware retrieval and update operations to be performed without authentication or authorization. The service accepts firmware-related requests from any reachable host and does not verify user privileges, integrity of uploaded images, or the authenticity of provided firmware.	9.8	More Details
CVE-2026-26210	KTransformers through 0.5.3 contains an unsafe deserialization vulnerability in the balance_serve backend mode where the scheduler RPC server binds a ZMQ ROUTER socket to all interfaces with no authentication and deserializes incoming messages using pickle.loads() without validation. Attackers can send a crafted pickle payload to the exposed ZMQ socket to execute arbitrary code on the server with the privileges of the ktransformers process.	9.8	More Details
CVE-2026-41276	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, this vulnerability allows remote attackers to bypass authentication on affected installations of FlowiseAI Flowise. Authentication is not required to exploit this vulnerability. The specific flaw exists within the resetPassword method of the AccountService class. There is no check performed to ensure that a password reset token has actually been generated for a user account. By default the value of the reset token stored in a users account is null, or an empty string if they've reset their password before. An attacker with knowledge of the user's email address can submit a request to the "/api/v1/account/reset-password" endpoint containing a null or empty string reset token value and reset that user's password to a value of their choosing. This vulnerability is fixed in 3.1.0.	9.8	More Details
CVE-2026-41268	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, Flowise is vulnerable to a critical unauthenticated remote command execution (RCE) vulnerability. It can be exploited via a parameter override bypass using the FILE-STORAGE:: keyword combined with a NODE_OPTIONS environment variable injection. This allows for the execution of arbitrary system commands with root privileges within the containerized Flowise instance, requiring only a single HTTP request and no authentication or knowledge of the instance. This vulnerability is fixed in 3.1.0.	9.8	More Details
CVE-2026-6942	radare2-mcp version 1.6.0 and earlier contains an os command injection vulnerability that allows remote attackers to execute arbitrary commands by bypassing the command filter through shell metacharacters in user-controlled input passed to r2_cmd_str(). Attackers can inject shell metacharacters through the jsonrpc interface parameters to achieve remote code execution on the host running radare2-mcp without requiring authentication.	9.8	More Details
CVE-2026-7155	A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. This impacts the function setLoginPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument admpass leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-41264	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the specific flaw exists within the run method of the CSV_Agents class. The issue results from the lack of proper sandboxing when evaluating an LLM generated python script. An attacker can leverage this vulnerability to execute code in the context of the user running the server. Using prompt injection techniques, an unauthenticated attacker with the ability to send prompts to a chatflow using the CSV Agent node may convince an LLM to respond with a malicious python script that executes attacker controlled commands on the Flowise server. This vulnerability is fixed in 3.1.0.	9.8	More Details
CVE-2026-31178	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunMaxAlive parameter to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-25874	LeRobot through 0.5.1 contains an unsafe deserialization vulnerability in the async inference pipeline where pickle.loads() is used to deserialize data received over unauthenticated gRPC channels without TLS in the policy server and robot client components. An unauthenticated network-reachable attacker can achieve arbitrary code execution on the server or client by sending a crafted pickle payload through the SendPolicyInstructions, SendObservations, or GetActions gRPC calls.	9.8	More Details
CVE-2026-31181	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunServerAddr parameter to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-31533	In the Linux kernel, the following vulnerability has been resolved: net/tls: fix use-after-free in -EBUSY error path of tls_do_encryption The -EBUSY handling in tls_do_encryption(), introduced by commit 859054147318 ("net: tls: handle backlogging of crypto requests"), has a use-after-free due to double cleanup of encrypt_pending and the scatterlist entry. When crypto_aead_encrypt() returns -EBUSY, the request is enqueued to the cryptd backlog and the async callback tls_encrypt_done() will be invoked upon completion. That callback unconditionally restores the scatterlist entry (sge->offset, sge->length) and decrements ctx->encrypt_pending. However, if tls_encrypt_async_wait() returns an error, the synchronous error path in tls_do_encryption() performs the same cleanup again, double-decrementing encrypt_pending and double-restoring the scatterlist. The double-decrement corrupts the encrypt_pending sentinel (initialized to 1), making tls_encrypt_async_wait() permanently skip the wait for pending async callbacks. A subsequent sendmsg can then free the tls_rec via bpf_exec_tx_verdict() while a	9.8	More Details

	cryptd callback is still pending, resulting in a use-after-free when the callback fires on the freed record. Fix this by skipping the synchronous cleanup when the -EBUSY async wait returns an error, since the callback has already handled encrypt_pending and sge restoration.		
CVE-2026-41247	elFinder is an open-source file manager for web, written in JavaScript using jQuery UI. Prior to 2.1.67, elFinder contains a command injection vulnerability in the resize command. The bg (background color) parameter is accepted from user input and passed through image resize/rotate processing. In configurations that use the ImageMagick CLI backend, this value is incorporated into shell command strings without sufficient escaping. An attacker able to invoke the resize command with a crafted bg value may achieve arbitrary command execution as the web server process user. This vulnerability is fixed in 2.1.67.	9.8	More Details
CVE-2026-6356	A vulnerability in the web application allows standard users to escalate their privileges to those of a super administrator through parameter manipulation, enabling them to access and modify sensitive information.	9.6	More Details
CVE-2026-6919	Use after free in DevTools in Google Chrome prior to 147.0.7727.117 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-6920	Out of bounds read in GPU in Google Chrome on Android prior to 147.0.7727.117 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-7321	Sandbox escape due to incorrect boundary conditions in the WebRTC: Networking component. This vulnerability was fixed in Firefox ESR 140.10.1.	9.6	More Details
CVE-2026-33471	nimiq-block contains block primitives to be used in Nimiq's Rust implementation. `SkipBlockProof::verify` computes its quorum check using `BitSet.len()`, then iterates `BitSet` indices and casts each `usize` index to `u16` (`slot as u16`) for slot lookup. Prior to version 1.3.0, if an attacker can get a `SkipBlockProof` verified where `MultiSignature.signers` contains out-of-range indices spaced by 65536, these indices inflate `len()` but collide onto the same in-range `u16` slot during aggregation. This makes it possible for a malicious validator with far fewer than `2f+1` real signer slots to pass skip block proof verification by multiplying a single BLS signature by the same factor. The patch for this vulnerability is included as part of v1.3.0. No known workarounds are available.	9.6	More Details
CVE-2026-24303	Improper access control in Microsoft Partner Center allows an authorized attacker to elevate privileges over a network.	9.6	More Details
CVE-2026-40471	hackage-server lacked Cross-Site Request Forgery (CSRF) protection across its endpoints. Scripts on foreign sites could trigger requests to hackage server, possibly abusing latent credentials to upload packages or perform other administrative actions. Some unauthenticated actions could also be abused (e.g. creating new user accounts).	9.6	More Details
CVE-2026-33454	The Camel-Mail component is vulnerable to Camel message header injection. The custom header filter strategy used by the component (MailHeaderFilterStrategy) only filters the 'out' direction via setOutFilterStartsWith, while it does not configure the 'in' direction via setInFilterStartsWith. As a result, when a Camel application consumes mail through camel-mail (for example via from(\"imap://...\") or from(\"pop3://...\")) the inbound filter check is skipped and Camel-prefixed MIME headers are mapped unfiltered into the Exchange. An attacker who can deliver an email to a mailbox monitored by such a consumer can inject Camel-specific headers that, for some Camel components downstream of the mail consumer (such as camel-bean, camel-exec, or camel-sql), can alter the behaviour of the route. This is the same pattern that was previously addressed in camel-undertow (CVE-2025-30177) and the broader incoming-header filter (CVE-2025-27636 and CVE-2025-29891). This issue affects Apache Camel: from 3.0.0 before 4.14.6, from 4.15.0 before 4.18.1. Users are recommended to upgrade to version 4.19.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.1. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6.	9.4	More Details
CVE-2026-31448	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid infinite loops caused by residual data On the mkdir/mknod path, when mapping logical blocks to physical blocks, if inserting a new extent into the extent tree fails (in this example, because the file system disabled the huge file feature when marking the inode as dirty), ext4_ext_map_blocks() only calls ext4_free_blocks() to reclaim the physical block without deleting the corresponding data in the extent tree. This causes subsequent mkdir operations to reference the previously reclaimed physical block number again, even though this physical block is already being used by the xattr block. Therefore, a situation arises where both the directory and xattr are using the same buffer head block in memory simultaneously. The above causes ext4_xattr_block_set() to enter an infinite loop about "inserted" and cannot release the inode lock, ultimately leading to the 143s blocking problem mentioned in [1]. If the metadata is corrupted, then trying to remove some extent space can do even more harm. Also in case EXT4_GET_BLOCKS_DELALLOC_RESERVE was passed, remove space wrongly update quota information. Jan Kara suggests distinguishing between two cases: 1) The error is ENOSPC or EDQUOT - in this case the filesystem is fully consistent and we must maintain its consistency including all the accounting. However these errors can happen only early before we've inserted the extent into the extent tree. So current code works correctly for this case. 2) Some other error - this means metadata is corrupted. We should strive to do as few modifications as possible to limit damage. So I'd just skip freeing of allocated blocks. [1] INFO: task syz.0.17:5995 blocked for more than 143 seconds. Call Trace: inode_lock_nested include/linux/fs.h:1073 [inline] __start_dirop fs/namei.c:2923 [inline] start_dirop fs/namei.c:2934 [inline]	9.4	More Details
CVE-2026-3893	The Carlson VASCO-B GNSS Receiver lacks an authentication mechanism, allowing an attacker with network access to directly access and modify its configuration and operational functions without needing credentials.	9.4	More Details
CVE-2024-46636	NASA Earth Observing System Data and Information System (EOSDIS) MODAPS v8.1 was discovered to contain a SQL injection vulnerability in the category parameter	9.4	More Details
	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6t_eui64: reject invalid MAC header for all packets `eui64_mt6()` derives a modified EUI-64 from the Ethernet source address and compares it with the low		

CVE-2026-31685	64 bits of the IPv6 source address. The existing guard only rejects an invalid MAC header when `par->fragoff != 0`. For packets with `par->fragoff == 0`, `eui64_mt6()` can still reach `eth_hdr(skb)` even when the MAC header is not valid. Fix this by removing the `par->fragoff != 0` condition so that packets with an invalid MAC header are rejected before accessing `eth_hdr(skb)`.	9.4	More Details
CVE-2026-33102	Url redirection to untrusted site ('open redirect') in M365 Copilot allows an unauthorized attacker to elevate privileges over a network.	9.3	More Details
CVE-2026-32210	Server-side request forgery (ssrf) in Microsoft Dynamics 365 (Online) allows an unauthorized attacker to perform spoofing over a network.	9.3	More Details
CVE-2026-41064	WWBN AVideo is an open source video platform. In versions up to and including 29.0, an incomplete fix for AVideo's `test.php` adds `escapeshellarg` for wget but leaves the `file_get_contents` and `curl` code paths unsanitized, and the URL validation regex `/^http/` accepts strings like `httpevil[.]com`. Commit 78bccae74634ead68aa6528d631c9ec4fd7aa536 contains an updated fix.	9.3	More Details
CVE-2026-42363	An insufficient encryption vulnerability exists in the Device Authentication functionality of GeoVision GV-IP Device Utility 9.0.5. Listening to broadcast packets can lead to credentials leak. An attacker can listen to broadcast messages to trigger this vulnerability. When interacting with various Geovision devices on the network, the utility may send privileged commands; in order to do so, the username and password of the device need to be provided. In some instances the command is broadcasted over UDP and the username/password are encrypted using a cryptographic protocol that appears to be derivated from Blowfish. However the symmetric key used for the encryption is also included in the packet, and thus the security of the username/password only relies on the "obscurity" of the encryption scheme. An attacker on the same LAN can listen to the broadcast traffic once an admin user interacts with the device, and decrypt the credentials using their own implementation of the algorithm. With this password the attacker would have full control over the device configuration, allowing them to change its ip address or even reset it to factory default.	9.3	More Details
CVE-2026-22336	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Directorist Booking allows SQL Injection.This issue affects Directorist Booking: from n/a before 3.0.2.	9.3	More Details
CVE-2026-40976	In certain circumstances, Spring Boot's default web security is ineffective allowing unauthorized access to all endpoints. For an application to be vulnerable, it must: be a servlet-based web application; have no Spring Security configuration of its own and rely on the default web security filter chain; depend on spring-boot-actuator-autoconfigure; not depend on spring-boot-health. If any of the above does not apply, the application is not vulnerable. Affected: Spring Boot 4.0.0–4.0.5; upgrade to 4.0.6 or later per vendor advisory.	9.1	More Details
CVE-2026-40575	OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Versions 7.5.0 through 7.15.1 may trust a client-supplied `X-Forwarded-Uri` header when `--reverse-proxy` is enabled and `--skip-auth-regex` or `--skip-auth-route` is configured. An attacker can spoof this header so OAuth2 Proxy evaluates authentication and skip-auth rules against a different path than the one actually sent to the upstream application. This can result in an unauthenticated remote attacker bypassing authentication and accessing protected routes without a valid session. Impacted users are deployments that run oauth2-proxy with `--reverse-proxy` enabled and configure at least one `--skip-auth-regex` or `--skip-auth-route` rule. This issue is patched in `v7.15.2`. Some workarounds are available for those who cannot upgrade immediately. Strip any client-provided `X-Forwarded-Uri` header at the reverse proxy or load balancer level; explicitly overwrite `X-Forwarded-Uri` with the actual request URI before forwarding requests to OAuth2 Proxy; restrict direct client access to OAuth2 Proxy so it can only be reached through a trusted reverse proxy; and/or remove or narrow `--skip-auth-regex` / `--skip-auth-route` rules where possible. For nginx-based deployments, ensure `X-Forwarded-Uri` is set by nginx and not passed through from the client.	9.1	More Details
CVE-2026-31682	In the Linux kernel, the following vulnerability has been resolved: bridge: br_nd_send: linearize skb before parsing ND options br_nd_send() parses neighbour discovery options from ns->opt[] and assumes that these options are in the linear part of request. Its callers only guarantee that the ICMPv6 header and target address are available, so the option area can still be non-linear. Parsing ns->opt[] in that case can access data past the linear buffer. Linearize request before option parsing and derive ns from the linear network header.	9.1	More Details
CVE-2026-41473	CyberPanel versions prior to 2.4.4 contain an authentication bypass vulnerability in the AI Scanner worker API endpoints that allows unauthenticated remote attackers to write arbitrary data to the database by sending requests to the /api/ai-scanner/status-webhook and /api/ai-scanner/callback endpoints. Attackers can exploit the lack of authentication checks to cause denial of service through storage exhaustion, corrupt scan history records, and pollute database fields with malicious data.	9.1	More Details
CVE-2026-41248	Clerk JavaScript is the official JavaScript repository for Clerk authentication. createRouteMatcher in @clerk/nextjs, @clerk/nuxt, and @clerk/astro can be bypassed by certain crafted requests, allowing them to skip middleware gating and reach downstream handlers. This vulnerability is fixed in @clerk/astro 1.5.7, 2.17.10, and 3.0.15; @clerk/nextjs 5.7.6, 6.39.2, and 7.2.1; @clerk/nuxt 1.13.28 and 2.2.2; and @clerk/shared 2.22.1, 3.47.4, anc 4.8.1	9.1	More Details
CVE-2026-41475	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to 1.4.3, an out-of-bounds read vulnerability in bacnet-stack's WritePropertyMultiple service decoder allows unauthenticated remote attackers to read past allocated buffer boundaries by sending a truncated WPM request. The vulnerability stems from wpm_decode_object_property() calling the deprecated decode_tag_number_and_value() function, which performs no bounds checking on the input buffer. A crafted BACnet/IP packet with a truncated property payload causes the decoder to read 1-7 bytes past the end of the buffer, leading to crashes or information disclosure on embedded BACnet devices. This vulnerability is fixed in 1.4.3.	9.1	More Details
CVE-2026-41428	Budibase is an open-source low-code platform. Prior to 3.35.4, the authenticated middleware uses unanchored regular expressions to match public (no-auth) endpoint patterns against ctx.request.url. Since ctx.request.url in Koa includes the query string, an attacker can access any protected endpoint by appending a public endpoint path as a query parameter. For example, POST /api/global/users/search?x=/api/system/status bypasses all authentication	9.1	More Details

	because the regex /api/system/status/ matches in the query string portion of the URL. This vulnerability is fixed in 3.35.4.		
CVE-2026-41415	PJSIP is a free and open source multimedia communication library written in C. In 2.16 and earlier, there is an out-of-bounds read when parsing a malformed Content-ID URI in SIP multipart message body. Insufficient length validation can cause reads beyond the intended buffer bounds. This vulnerability is fixed in 2.17.	9.1	More Details
CVE-2026-41328	Dgraph is an open source distributed GraphQL database. Prior to 25.3.3, a vulnerability has been found in Dgraph that gives an unauthenticated attacker full read access to every piece of data in the database. This affects Dgraph's default configuration where ACL is not enabled. The attack requires two HTTP POSTs to port 8080. The first sets up a schema predicate with @unique @index(exact) @lang via /alter (also unauthenticated in default config). The second sends a crafted JSON mutation to /mutate?commitNow=true where a JSON key contains the predicate name followed by @ and a DQL injection payload in the language tag position. The injection exploits the addQueryIfUnique function in edgraph/server.go, which constructs DQL queries using fmt.Sprintf with unsanitized predicateName that includes the raw pred.Lang value. The Lang field is extracted from JSON mutation keys by x.PredicateLang(), which splits on @, and is never validated by any function in the codebase. The attacker injects a closing parenthesis to escape the eq() function, adds an arbitrary named query block, and uses a # comment to neutralize trailing template syntax. The injected query executes server-side and its results are returned in the HTTP response. This vulnerability is fixed in 25.3.3.	9.1	More Details
CVE-2026-41327	Dgraph is an open source distributed GraphQL database. Prior to 25.3.3, a vulnerability has been found in Dgraph that gives an unauthenticated attacker full read access to every piece of data in the database. This affects Dgraph's default configuration where ACL is not enabled. The attack is a single HTTP POST to /mutate?commitNow=true containing a crafted cond field in an upsert mutation. The cond value is concatenated directly into a DQL query string via strings.Builder.WriteString after only a cosmetic strings.Replace transformation. No escaping, parameterization, or structural validation is applied. An attacker injects an additional DQL query block into the cond string, which the DQL parser accepts as a syntactically valid named query block. The injected query executes server-side and its results are returned in the HTTP response. This vulnerability is fixed in 25.3.3.	9.1	More Details
CVE-2026-41677	rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.9.0 to before 0.10.78, the *_from_pem_callback APIs did not validate the length returned by the user's callback. A password callback that returns a value larger than the buffer it was given can cause some versions of OpenSSL to over-read this buffer. OpenSSL 3.x is not affected by this. This vulnerability is fixed in 0.10.78.	9.1	More Details
CVE-2026-31636	In the Linux kernel, the following vulnerability has been resolved: rxrpc: fix RESPONSE authenticator parser OOB read rxgk_verify_authenticator() copies auth_len bytes into a temporary buffer and then passes p + auth_len as the parser limit to rxgk_do_verify_authenticator(). Since p is a __be32 *, that inflates the parser end pointer by a factor of four and lets malformed RESPONSE authenticators read past the kmalloc() buffer. Decoded from the original latest-net reproduction logs with scripts/decode_stacktrace.sh: BUG: KASAN: slab-out-of-bounds in rxgk_verify_response() Call Trace: dump_stack_lvl() [lib/dump_stack.c:123] print_report() [mm/kasan/report.c:379 mm/kasan/report.c:482] kasan_report() [mm/kasan/report.c:597] rxgk_verify_response() [net/rxrpc/rxgk.c:1103 net/rxrpc/rxgk.c:1167 net/rxrpc/rxgk.c:1274] rxrpc_process_connection() [net/rxrpc/conn_event.c:266 net/rxrpc/conn_event.c:364 net/rxrpc/conn_event.c:386] process_one_work() [kernel/workqueue.c:3281] worker_thread() [kernel/workqueue.c:3353 kernel/workqueue.c:3440] kthread() [kernel/kthread.c:436] ret_from_fork() [arch/x86/kernel/process.c:164] Allocated by task 54: rxgk_verify_response() [include/linux/slab.h:954 net/rxrpc/rxgk.c:1155 net/rxrpc/rxgk.c:1274] rxrpc_process_connection() [net/rxrpc/conn_event.c:266 net/rxrpc/conn_event.c:364 net/rxrpc/conn_event.c:386] Convert the byte count to __be32 units before constructing the parser limit.	9.1	More Details
CVE-2026-27843	A vulnerability exists in SenseLive X3050's web management interface that allows critical configuration parameters to be modified without sufficient authentication or server-side validation. By applying unsupported or disruptive values to recovery mechanisms and network settings, an attacker can induce a persistent lockout state. Because the device lacks a physical reset button, recovery requires specialized technical access via the console to perform a factory reset, resulting in a total denial-of-service for the gateway and its connected RS-485 downstream systems.	9.1	More Details
CVE-2026-41229	Froxlor is open source server administration software. Prior to version 2.3.6, `PhpHelper::parseArrayToString()` writes string values into single-quoted PHP string literals without escaping single quotes. When an admin with `change_serversettings` permission adds or updates a MySQL server via the API, the `privileged_user` parameter (which has no input validation) is written unescaped into `lib/userdata.inc.php`. Since this file is `require`d on every request via `Database::getDB()`, an attacker can inject arbitrary PHP code that executes as the web server user on every subsequent page load. Version 2.3.6 contains a patch.	9.1	More Details
CVE-2026-41167	Jellystat is a free and open source Statistics App for Jellyfin. Prior to version 1.1.10, multiple API endpoints in Jellystat build SQL queries by interpolating unsanitized request-body fields directly into raw SQL strings. An authenticated user can inject arbitrary SQL via `POST /api/getUserDetails` and `POST /api/getLibrary`, enabling full read of any table in the database - including `app_config`, which stores the Jellystat admin credentials, the Jellyfin API key, and the Jellyfin host URL. Because the vulnerable call site dispatches via `node-postgres`'s simple query protocol (no parameter array is passed), stacked queries are allowed, which escalates the injection from data disclosure to arbitrary command execution on the PostgreSQL host via `COPY ... TO PROGRAM`. Under the role shipped by the project's `docker-compose.yml` (a PostgreSQL superuser), no additional privileges are required to reach the RCE primitive. Version 1.1.10 contains a fix.	9.1	More Details
CVE-2026-33656	EspoCRM is an open source customer relationship management application. Prior to version 9.3.4, EspoCRM's built-in formula scripting engine allowing updating attachment's sourceId thus allowing an authenticated admin to overwrite the `sourceId` field on `Attachment` entities. Because `sourceId` is concatenated directly into a file path with no sanitization in `EspoUploadDir::getFilePath()`, an attacker can redirect any file read or write operation to an arbitrary path within the web server's `open_basedir` scope. Version 9.3.4 fixes the issue.	9.1	More Details
	The Create DB Tables plugin for WordPress is vulnerable to authorization bypass in all versions up to and including		

CVE-2026-4119	1.2.1. The plugin registers admin_post action hooks for creating tables (admin_post_add_table) and deleting tables (admin_post_delete_db_table) without implementing any capability checks via current_user_can() or nonce verification via wp_verify_nonce()/check_admin_referer(). The admin_post hook only requires the user to be logged in, meaning any authenticated user including Subscribers can access these endpoints. The cdbt_delete_db_table() function takes a user-supplied table name from $_POST['db_table'] and executes a DROP TABLE SQL query, allowing any authenticated attacker to delete any database table including critical WordPress core tables such as wp_users or wp_options. The cdbt_create_new_table() function similarly allows creating arbitrary tables. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary database tables and delete any existing database table, potentially destroying the entire WordPress installation.	9.1	More Details
CVE-2026-41386	OpenClaw before 2026.3.22 contains a privilege escalation vulnerability where bootstrap setup codes are not bound to intended device roles and scopes during pairing. Attackers can exploit this during first-use device pairing to escalate privileges beyond their intended role and scope.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-7055	A security vulnerability has been detected in Tenda F456 1.0.0.5. This issue affects the function fromVirtualSer of the file /goform/VirtualSer of the component httpd. The manipulation of the argument menufacturer/Go leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-40978	SQL injection vulnerability in Spring AI's `CosmosDBVectorStore` allows attackers to execute arbitrary SQL queries via crafted document IDs. Affected versions: Spring AI: 1.0.0 - 1.0.5 (fixed in 1.0.6), 1.1.0 - 1.1.4 (fixed in 1.1.5)	8.8	More Details
CVE-2026-6912	Improperly controlled modification of dynamically-determined object attributes in the Cognito User Pool configuration in AWS Ops Wheel before PR #165 allows remote authenticated users to escalate to deployment admin privileges and manage Cognito user accounts via a crafted UpdateUserAttributes API call that sets the custom:deployment_admin attribute. To remediate this issue, users should redeploy from the updated repository and ensure any forked or derivative code is patched to incorporate the new fixes.	8.8	More Details
CVE-2026-41378	OpenClaw before 2026.3.31 contains a privilege escalation vulnerability allowing paired nodes with role=node to dispatch node.event agent requests with unrestricted gateway-side tool access. Attackers with trusted paired node credentials can escalate privileges by leveraging unrestricted agent.request dispatch to achieve remote code execution on the gateway.	8.8	More Details
CVE-2026-40897	Math.js is an extensive math library for JavaScript and Node.js. From 13.1.1 to before 15.2.0, a vulnerability allowed executing arbitrary JavaScript via the expression parser of mathjs. You can be affected when you have an application where users can evaluate arbitrary expressions using the mathjs expression parser. This vulnerability is fixed in 15.2.0.	8.8	More Details
CVE-2026-6988	A flaw has been found in Tenda HG10 HG7_HG9_HG10re_300001138_en_xpon. This issue affects the function formRoute of the file /boaform/formRouting of the component Boa Service. This manipulation of the argument nextHop causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-7119	A vulnerability was detected in Tenda HG3 2.0. The impacted element is an unknown function of the file /boaform/formCountrystr. The manipulation of the argument countrystr results in os command injection. The attack may be performed from remote. The exploit is now public and may be used.	8.8	More Details
CVE-2026-31553	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix the descriptor address in __kvm_at_swap_desc() Using "(u64 __user *)hva + offset" to get the virtual addresses of S1/S2 descriptors looks really wrong, if offset is not zero. What we want to get for swapping is hva + offset, not hva + offset*8. ;-) Fix it.	8.8	More Details
CVE-2026-7019	A vulnerability was identified in Tenda F456 1.0.0.5. The impacted element is the function fromP2pListFilter of the file /goform/P2pListFilter. The manipulation of the argument menufacturer/Go leads to buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-41651	PackageKit is a a D-Bus abstraction layer that allows the user to manage packages in a secure way using a cross-distro, cross-architecture API. PackageKit between and including versions 1.0.2 and 1.3.4 is vulnerable to a time-of-check time-of-use (TOCTOU) race condition on transaction flags that allows unprivileged users to install packages as root and thus leads to a local privilege escalation. This is patched in version 1.3.5. A local unprivileged user can install arbitrary RPM packages as root, including executing RPM scriptlets, without authentication. The vulnerability is a TOCTOU race condition on `transaction->cached_transaction_flags` combined with a silent state-machine guard that discards illegal backward transitions while leaving corrupted flags in place. Three bugs exist in `src/pk-transaction.c`: 1. Unconditional flag overwrite (line 4036): `InstallFiles()` writes caller-supplied flags to `transaction->cached_transaction_flags` without checking whether the transaction has already been authorized/started. A second call blindly overwrites the flags even while the transaction is RUNNING. 2. Silent state-transition rejection (lines 873–882): `pk_transaction_set_state()` silently discards backward state transitions (e.g. `RUNNING` → `WAITING_FOR_AUTH`) but the flag overwrite at step 1 already happened. The transaction continues running with corrupted flags. 3. Late flag read at execution time (lines 2273–2277): The scheduler's idle callback reads cached_transaction_flags at dispatch time, not at authorization time. If flags were overwritten between authorization and execution, the backend sees the attacker's flags.	8.8	More Details
CVE-2026-41277	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, a Mass Assignment vulnerability in the DocumentStore creation endpoint allows authenticated users to control the primary key (id) and internal state fields of DocumentStore entities. Because the service uses repository.save() with a client-supplied primary key, the POST create endpoint behaves as an implicit UPSERT operation. This enables overwriting existing DocumentStore objects. In multi-workspace or multi-tenant deployments, this can lead to cross-workspace object takeover and broken object-level authorization (IDOR), allowing an attacker to reassign or modify DocumentStore objects belonging to other workspaces. This vulnerability is fixed in 3.1.0.	8.8	More Details

CVE-2026-6859	A flaw was found in InstructLab. The `linux_train.py` script hardcodes `trust_remote_code=True` when loading models from HuggingFace. This allows a remote attacker to achieve arbitrary Python code execution by convincing a user to run `ilab train/download/generate` with a specially crafted malicious model from the HuggingFace Hub. This vulnerability can lead to complete system compromise.	8.8	More Details
CVE-2026-31558	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Make kvm_get_vcpu_by_cpuid() more robust kvm_get_vcpu_by_cpuid() takes a cpuid parameter whose type is int, so cpuid can be negative. Let kvm_get_vcpu_by_cpuid() return NULL for this case so as to make it more robust. This fix an out-of-bounds access to kvm_arch::phyid_map::phys_map[].	8.8	More Details
CVE-2026-27172	The ConsulRegistry in the camel-consul component (class org.apache.camel.component.consul.ConsulRegistry and its inner ConsulRegistryUtils.deserialize method) read Java-serialized values from the Consul KV store and passed them to ObjectInputStream.readObject() without configuring an ObjectInputFilter. An attacker who can write to the Consul KV store backing a Camel ConsulRegistry instance could inject a malicious serialized Java object that is deserialized the next time Camel performs a lookup against that registry, leading to arbitrary code execution in the Camel process. The issue mirrors the class of vulnerability already addressed for other Camel components in CVE-2024-22369, CVE-2024-23114 and CVE-2026-25747, and was overlooked during the original remediation of those CVEs. This issue affects Apache Camel: from 3.0.0 before 4.14.6, from 4.15.0 before 4.18.1. Users are recommended to upgrade to version 4.19.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.1.	8.8	More Details
CVE-2026-40858	The camel-infinispan component's ProtoStream-based remote aggregation repository deserializes data read from a remote Infinispan cache using java.io.ObjectInputStream without applying any ObjectInputFilter. An attacker who can write to the Infinispan cache used by a Camel application can inject a crafted serialized Java object that, when read during normal aggregation repository operations such as get or recover, results in arbitrary code execution in the context of the application. This issue affects Apache Camel: from 4.0.0 before 4.14.7, from 4.15.0 before 4.18.2, from 4.19.0 before 4.20.0. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.7. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.2. The JIRA ticket: https://issues.apache.org/jira/browse/CAMEL-23322 refers to the various commits that resolved the issue, and have more details. This issue follows the same class of vulnerability previously addressed in CVE-2024-22369, CVE-2024-23114 and CVE-2026-25747.	8.8	More Details
CVE-2026-27785	Specific firmware versions of Milesight AIOT camera firmware contain hard-coded credentials.	8.8	More Details
CVE-2026-41138	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, there is a remote code execution vulnerability in AirtableAgent.ts caused by lack of input verification when using Pandas. The user's input is directly applied to the question parameter within the prompt template and it is reflected to the Python code without any sanitization. This vulnerability is fixed in 3.1.0.	8.8	More Details
CVE-2026-31433	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix potencial OOB in get_file_all_info() for compound requests When a compound request consists of QUERY_DIRECTORY + QUERY_INFO (FILE_ALL_INFORMATION) and the first command consumes nearly the entire max_trans_size, get_file_all_info() would blindly call smbConvertToUTF16() with PATH_MAX, causing out-of-bounds write beyond the response buffer. In get_file_all_info(), there was a missing validation check for the client-provided OutputBufferLength before copying the filename into FileName field of the smb2_file_all_info structure. If the filename length exceeds the available buffer space, it could lead to potential buffer overflows or memory corruption during smbConvertToUTF16 conversion. This calculating the actual free buffer size using smb2_calc_max_out_buf_len() and returning -EINVAL if the buffer is insufficient and updating smbConvertToUTF16 to use the actual filename length (clamped by PATH_MAX) to ensure a safe copy operation.	8.8	More Details
CVE-2026-31432	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix OOB write in QUERY_INFO for compound requests When a compound request such as READ + QUERY_INFO(Security) is received, and the first command (READ) consumes most of the response buffer, ksmbd could write beyond the allocated buffer while building a security descriptor. The root cause was that smb2_get_info_sec() checked buffer space using ppntsd_size from xattr, while build_sec_desc() often synthesized a significantly larger descriptor from POSIX ACLs. This patch introduces smb_acl_sec_desc_scratch_len() to accurately compute the final descriptor size beforehand, performs proper buffer checking with smb2_calc_max_out_buf_len(), and uses exact-sized allocation + iov pinning.	8.8	More Details
CVE-2026-41137	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, The CSVAgent allows providing a custom Pandas CSV read code. Due to lack of sanitization, an attacker can provide a command injection payload that will get interpolated and executed by the server. This vulnerability is fixed in 3.1.0.	8.8	More Details
CVE-2026-7101	A vulnerability has been found in Tenda F456 1.0.0.5. This affects the function fromWrlclientSet of the file /goform/WrlclientSet of the component httpd. The manipulation leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-24186	NVIDIA FLARE SDK contains a vulnerability in FOBS, where an attacker may cause deserialization of untrusted data by sending a malicious FOBS- encoded message. A successful exploit of this vulnerability might lead to code execution.	8.8	More Details
CVE-2026-41349	OpenClaw before 2026.3.28 contains an agentic consent bypass vulnerability allowing LLM agents to silently disable execution approval via config.patch parameter. Remote attackers can exploit this to bypass security controls and execute unauthorized operations without user consent.	8.8	More Details
CVE-2026-	ProjeQtor versions 7.0 through 12.4.3 contain a ZipSlip path traversal vulnerability in the plugin upload functionality that allows authenticated attackers with upload permissions to write files outside the intended extraction directory by crafting ZIP archives with directory traversal sequences. Attackers can exploit unvalidated archive extraction to write a PHP	8.8	More Details

41463	webshell to a web-accessible directory and achieve remote code execution with the privileges of the web server process.		
CVE-2026-31450	In the Linux kernel, the following vulnerability has been resolved: ext4: publish jinode after initialization ext4_inode_attach_jinode() publishes ei->jinode to concurrent users. It used to set ei->jinode before jbd2_journal_init_jbd_inode(), allowing a reader to observe a non-NULL jinode with i_vfs_inode still unset. The fast commit flush path can then pass this jinode to jbd2_wait_inode_data(), which dereferences i_vfs_inode->i_mapping and may crash. Below is the crash I observe: ``` BUG: unable to handle page fault for address: 000000010beb47f4 PGD 110e51067 P4D 110e51067 PUD 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 1 UID: 0 PID: 4850 Comm: fc_fsync_bench_ Not tainted 6.18.0-00764-g795a690c06a5 #1 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS Arch Linux 1.17.0-2-2 04/01/2014 RIP: 0010:xas_find_marked+0x3d/0x2e0 Code: e0 03 48 83 f8 02 0f 84 f0 01 00 00 48 8b 47 08 48 89 c3 48 39 c6 0f 82 fd 01 00 00 48 85 c9 74 3d 48 83 f9 03 77 63 4c 8b 0f <49> 8b 71 08 48 c7 47 18 00 00 00 00 48 89 f1 83 e1 03 48 83 f9 02 RSP: 0018:ffffbbee806e7bf0 EFLAGS: 00010246 RAX: 000000000010beb4 RBX: 000000000010beb4 RCX: 0000000000000003 RDX: 0000000000000001 RSI: 0000002000300000 RDI: ffffbbee806e7c10 RBP: 0000000000000001 R08: 0000002000300000 R09: 000000010beb47ec R10: ffff9ea494590090 R11: 0000000000000000 R12: 0000002000300000 R13: ffffbbee806e7c90 R14: ffff9ea494513788 R15: ffffbbee806e7c88 FS: 00007fc2f9e3e6c0(0000) GS:ffff9ea6b1444000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000010beb47f4 CR3: 0000000119ac5000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> filemap_get_folios_tag+0x87/0x2a0 __filemap_fdatawait_range+0x5f/0xd0 ? srso_alias_return_thunk+0x5/0xfbef5 ? __schedule+0x3e7/0x10c0 ? srso_alias_return_thunk+0x5/0xfbef5 ? srso_alias_return_thunk+0x5/0xfbef5 ? srso_alias_return_thunk+0x5/0xfbef5 ? preempt_count_sub+0x5f/0x80 ? srso_alias_return_thunk+0x5/0xfbef5 ? cap_safe_nice+0x37/0x70 ? srso_alias_return_thunk+0x5/0xfbef5 ? preempt_count_sub+0x5f/0x80 ? srso_alias_return_thunk+0x5/0xfbef5 filemap_fdatawait_range_keep_errors+0x12/0x40 ext4_fc_commit+0x697/0x8b0 ? ext4_file_write_iter+0x64b/0x950 ? srso_alias_return_thunk+0x5/0xfbef5 ? preempt_count_sub+0x5f/0x80 ? srso_alias_return_thunk+0x5/0xfbef5 ? vfs_write+0x356/0x480 ? srso_alias_return_thunk+0x5/0xfbef5 ? preempt_count_sub+0x5f/0x80 ext4_sync_file+0xf7/0x370 do_fsync+0x3b/0x80 ? syscall_trace_enter+0x108/0x1d0 __x64_sys_fdatasync+0x16/0x20 do_syscall_64+0x62/0x2c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e ... ``` Fix this by initializing the jbd2_inode first. Use smp_wmb() and WRITE_ONCE() to publish ei->jinode after initialization. Readers use READ_ONCE() to fetch the pointer.	8.8	More Details
CVE-2026-41421	SiYuan is an open-source personal knowledge management system. Prior to 3.6.5, SiYuan desktop renders notification messages as raw HTML inside an Electron renderer. The notification route POST /api/notification/pushMsg accepts a user-controlled msg value, forwards it through the backend broadcast layer, and the frontend inserts it into the DOM with insertAdjacentHTML(...) at message.ts. On desktop builds, this is not limited to ordinary XSS. Electron windows are created with nodeIntegration: true, contextIsolation: false, and webSecurity: false at main.js. As a result, JavaScript executed from the notification sink can directly access Node APIs and escalate to desktop code execution. This vulnerability is fixed in 3.6.5.	8.8	More Details
CVE-2026-41429	arduino-esp32 is an Arduino core for the ESP32, ESP32-S2, ESP32-S3, ESP32-C3, ESP32-C6 and ESP32-H2 microcontrollers. Prior to 3.3.8, there is a remotely reachable memory corruption issue in the NBNS packet handling path. When NetBIOS is enabled by calling NBNS.begin(...), the device listens on UDP port 137 and processes untrusted NBNS requests from the local network. The request parser trusts the attacker-controlled name_len field without enforcing a bound consistent with the fixed-size destination buffers used later in the flow. This vulnerability is fixed in 3.3.8.	8.8	More Details
CVE-2026-31435	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix read abandonment during retry Under certain circumstances, all the remaining subrequests from a read request will get abandoned during retry. The abandonment process expects the 'subreq' variable to be set to the place to start abandonment from, but it doesn't always have a useful value (it will be uninitialised on the first pass through the loop and it may point to a deleted subrequest on later passes). Fix the first jump to "abandon:" to set subreq to the start of the first subrequest expected to need retry (which, in this abandonment case, turned out unexpectedly to no longer have NEED_RETRY set). Also clear the subreq pointer after discarding superfluous retryable subrequests to cause an oops if we do try to access it.	8.8	More Details
CVE-2026-41476	Deskflow is a keyboard and mouse sharing app. Prior to 1.26.0.138, a remote memory-safety vulnerability in Deskflow's clipboard deserialization allows a connected peer to trigger an out-of-bounds read by sending a malformed clipboard update. The issue is in the implementation of src/lib/deskflow/IClipboard.cpp. This is reachable because ClipboardChunk::assemble() in src/lib/deskflow/ClipboardChunk.cpp validates only the outer clipboard transfer size. It does not validate the internal structure of the serialized clipboard blob, so malformed inner lengths reach IClipboard::unmarshall() unchanged. This vulnerability is fixed in 1.26.0.138.	8.8	More Details
CVE-2026-20766	An out-of-bounds memory access vulnerability exists in specific firmware versions of Milesight AIOT cameras.	8.8	More Details
CVE-2026-7151	A vulnerability was determined in Tenda HG3 2.0. Impacted is the function formUploadConfig of the file /boaform/formIPv6Routing. This manipulation of the argument destNet causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-6741	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Privilege Escalation in versions up to and including 5.4.1. This is due to a missing authorization check in the execute() method of the connect-customer-to-wp-user ability, which only requires the customer__edit capability granted to the latepoint_agent role by default, without verifying whether the target WordPress user ID belongs to a privileged account. This makes it possible for authenticated attackers with the latepoint_agent role to link any LatePoint customer record to an administrator's WordPress account and subsequently reset the administrator's password via the normal customer password-reset flow, resulting in full site takeover.	8.8	More Details
CVE-2026-7288	A vulnerability has been found in D-Link DIR-825M 1.1.12. This vulnerability affects the function sub_4151FC of the file /boafrm/formVpnConfigSetup. The manipulation of the argument submit-url leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE-2026-40466	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ. An authenticated attacker may bypass the fix in CVE-2026-34197 by adding a connector using an HTTP Discovery transport via BrokerView.addNetworkConnector or BrokerView.addConnector through Jolokia if the activemq-http module is on the classpath. A malicious HTTP endpoint can return a VM transport through the HTTP URI which will bypass the validation added in CVE-2026-34197. The attacker can then use the VM transport's brokerConfig parameter to load a remote Spring XML application context using ResourceXmlApplicationContext. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec(). This issue affects Apache ActiveMQ Broker: before 5.19.6, from 6.0.0 before 6.2.5; Apache ActiveMQ All: before 5.19.6, from 6.0.0 before 6.2.5; Apache ActiveMQ: before 5.19.6, from 6.0.0 before 6.2.5. Users are recommended to upgrade to version 5.19.6 or 6.2.5, which fixes the issue.	8.8	More Details
CVE-2026-41352	OpenClaw before 2026.3.31 contains a remote code execution vulnerability where a device-paired node can bypass the node scope gate authentication mechanism. Attackers with device pairing credentials can execute arbitrary node commands on the host system without proper node pairing validation.	8.8	More Details
CVE-2026-41044	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ, Apache ActiveMQ Broker, Apache ActiveMQ All. An authenticated attacker can use the admin web console page to construct a malicious broker name that bypasses name validation to include an xbean binding that can be later used by a VM transport to load a remote Spring XML application. The attacker can then use the DestinationView mbean to send a message to trigger a VM transport creation that will reference this malicious broker name which can lead to loading the malicious Spring XML context file. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec(). This issue affects Apache ActiveMQ: before 5.19.6, from 6.0.0 before 6.2.5; Apache ActiveMQ Broker: before 5.19.6, from 6.0.0 before 6.2.5; Apache ActiveMQ All: before 5.19.6, from 6.0.0 before 6.2.5. Users are recommended to upgrade to version 6.2.5 or 5.19.6, which fixes the issue.	8.8	More Details
CVE-2026-33318	Actual is a local-first personal finance tool. Prior to version 26.4.0, any authenticated user (including `BASIC` role) can escalate to `ADMIN` on servers migrated from password authentication to OpenID Connect. Three weaknesses combine: `POST /account/change-password` has no authorization check, allowing any session to overwrite the password hash; the inactive password `auth` row is never removed on migration; and the login endpoint accepts a client-supplied `loginMethod` that bypasses the server's active auth configuration. Together these allow an attacker to set a known password and authenticate as the anonymous admin account created during the multiuser migration. The three weaknesses form a single, sequential exploit chain — none produces privilege escalation on its own. Missing authorization on POST /change-password allows overwriting a password hash, but only matters if there is an orphaned row to target. Orphaned password row persisting after migration provides the target row, but is harmless without the ability to authenticate using it. Client-controlled loginMethod: "password" allows forcing password-based auth, but is useless without a known hash established by step 1. All three must be chained in sequence to achieve the impact. No single weakness independently results in privilege escalation. The single root cause is the missing authorization check on /change-password; the other two are preconditions that make it exploitable. Version 26.4.0 contains a fix.	8.8	More Details
CVE-2026-41404	OpenClaw before 2026.3.31 contains an incomplete scope-clearing vulnerability in trusted-proxy authentication mode that allows operator.admin privilege escalation. Attackers can exploit this by declaring operator scopes on non-Control-UI clients, allowing self-declared scopes to persist on identity-bearing authentication paths and escalate privileges.	8.8	More Details
CVE-2026-33208	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to version 8.2.6.4, the /config/ < service > /find-in-config endpoint in Roxy-WI fails to sanitize the user-supplied words parameter before embedding it into a shell command string that is subsequently executed on a remote managed server via SSH. An authenticated attacker can inject arbitrary shell metacharacters to break out of the intended grep command context and execute arbitrary OS commands with sudo privileges on the target server, resulting in full Remote Code Execution (RCE). Version 8.2.6.4 patches the issue.	8.8	More Details
CVE-2026-41325	Kirby is an open-source content management system. Kirby's user permissions control which user role is allowed to perform specific actions to content models in the CMS. These permissions are defined for each role in the user blueprint (`site/blueprints/users/...`). It is also possible to customize the permissions for each target model in the model blueprints (such as in `site/blueprints/pages/...`) using the `options` feature. The permissions and options together control the authorization of user actions. Kirby provides the `pages.create`, `files.create` and `users.create` permissions (among others). These permissions can again be set in the user blueprint and/or in the blueprint of the target model via `options`. Prior to versions 4.9.0 and 5.4.0, Kirby allowed to override the `options` during the creation of pages, files and users by injecting custom dynamic blueprint configuration into the model data. The injected `options` could include `'create' => true`, which then caused an override of the permissions and options configured by the site developer in the user and model blueprints. The problem has been patched in Kirby 4.9.0 and Kirby 5.4.0. The patched versions have updated the normalization code that is used during the creation of pages, files and users to include a filter for the `blueprint` property. This prevents the injection of dynamic blueprint configuration into the creation request.	8.8	More Details
CVE-2026-7289	A vulnerability was found in D-Link DIR-825M 1.1.12. This issue affects the function sub_414BA8 of the file /boafrm/formWanConfigSetup. The manipulation of the argument submit-url results in buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-69689	The Fan Control application V251 contains an improper privilege handling vulnerability in its Open File Dialog. The dialog processes user-supplied paths with elevated permissions, which can be exploited by a local attacker to perform actions with administrator-level privileges.	8.8	More Details
CVE-2026-38934	Cross Site Request Forgery vulnerability in diskoverdata diskover-community v.2.3.5. and before allows a remote attacker to escalate privileges and obtain sensitive information via the public/settings_process.php	8.8	More Details
CVE-2026-	A flaw has been found in Tenda F456 1.0.0.5. The impacted element is the function fromNatlimitof of the file /goform/Natlimit of the component httpd. Executing a manipulation can lead to buffer overflow. The attack may be	8.8	More

7100	launched remotely. The exploit has been published and may be used.		Details
CVE-2026-31570	In the Linux kernel, the following vulnerability has been resolved: can: gw: fix OOB heap access in cgw_csum_crc8_rel() cgw_csum_crc8_rel() correctly computes bounds-safe indices via calc_idx(): int from = calc_idx(crc8->from_idx, cf->len); int to = calc_idx(crc8->to_idx, cf->len); int res = calc_idx(crc8->result_idx, cf->len); if (from < 0 || to < 0 || res < 0) return; However, the loop and the result write then use the raw s8 fields directly instead of the computed variables: for (i = crc8->from_idx; ...) /* BUG: raw negative index */ cf->data[crc8->result_idx] = ...; /* BUG: raw negative index */ With from_idx = to_idx = result_idx = -64 on a 64-byte CAN FD frame, calc_idx(-64, 64) = 0 so the guard passes, but the loop iterates with i = -64, reading cf->data[-64], and the write goes to cf->data[-64]. This write might end up to 56 (7.0-rc) or 40 (<= 6.19) bytes before the start of the canfd_frame on the heap. The companion function cgw_csum_xor_rel() uses `from`/`to`/`res` correctly throughout; fix cgw_csum_crc8_rel() to match. Confirmed with KASAN on linux-7.0-rc2: BUG: KASAN: slab-out-of-bounds in cgw_csum_crc8_rel+0x515/0x5b0 Read of size 1 at addr ffff8880076619c8 by task poc_cgw_oob/62 To configure the can-gw crc8 checksums CAP_NET_ADMIN is needed.	8.8	More Details
CVE-2026-7029	A weakness has been identified in Tenda F456 1.0.0.5. The impacted element is the function fromaddressNat of the file /goform/addressNat. Executing a manipulation of the argument menufacturer/Go can lead to buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-7032	A flaw has been found in Tenda F456 1.0.0.5. Affected is the function SafeEmailFilter of the file /goform/SafeEmailFilter. This manipulation of the argument page causes buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-7034	A vulnerability was found in Tenda FH1202 1.2.0.14(408). Affected by this issue is the function WrlExtraSet of the file /goform/WrlExtraSet of the component httpd. Performing a manipulation of the argument Go results in stack-based buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-7035	A vulnerability was determined in Tenda FH1202 1.2.0.14. This affects the function fromWrlclientSet of the file /goform/WrlclientSet of the component httpd. Executing a manipulation of the argument Go can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-7082	A flaw has been found in Tenda F456 1.0.0.5. Affected by this vulnerability is the function formWrlExtraSet of the file /goform/WrlExtraSet of the component httpd. Executing a manipulation of the argument Go can lead to buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-7081	A vulnerability was detected in Tenda F456 1.0.0.5. Affected is the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer of the component httpd. Performing a manipulation of the argument dips results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7106	The Highland Software Custom Role Manager plugin for WordPress is vulnerable to Privilege Escalation in versions up to and including 1.0.0. This is due to insufficient authorization checks in the hscrm_save_user_roles() function, which is hooked to the personal_options_update action accessible by any authenticated user. This makes it possible for authenticated attackers, with Subscriber-level access or higher, to potentially modify user roles via the profile update form.	8.8	More Details
CVE-2026-31629	In the Linux kernel, the following vulnerability has been resolved: nfc: llcp: add missing return after LLCP_CLOSED checks In nfc_llcp_recv_hdlc() and nfc_llcp_recv_disc(), when the socket state is LLCP_CLOSED, the code correctly calls release_sock() and nfc_llcp_sock_put() but fails to return. Execution falls through to the remainder of the function, which calls release_sock() and nfc_llcp_sock_put() again. This results in a double release_sock() and a refcount underflow via double nfc_llcp_sock_put(), leading to a use-after-free. Add the missing return statements after the LLCP_CLOSED branches in both functions to prevent the fall-through.	8.8	More Details
CVE-2026-31622	In the Linux kernel, the following vulnerability has been resolved: NFC: digital: Bounds check NFC-A cascade depth in SDD response handler The NFC-A anti-collision cascade in digital_in_recv_sdd_res() appends 3 or 4 bytes to target->nfcid1 on each round, but the number of cascade rounds is controlled entirely by the peer device. The peer sets the cascade tag in the SDD_RES (deciding 3 vs 4 bytes) and the cascade-incomplete bit in the SEL_RES (deciding whether another round follows). ISO 14443-3 limits NFC-A to three cascade levels and target->nfcid1 is sized accordingly (NFC_NFCID1_MAXSIZE = 10), but nothing in the driver actually enforces this. This means a malicious peer can keep the cascade running, writing past the heap-allocated nfc_target with each round. Fix this by rejecting the response when the accumulated UID would exceed the buffer. Commit e329e71013c9 ("NFC: nci: Bounds check struct nfc_target arrays") fixed similar missing checks against the same field on the NCI path.	8.8	More Details
CVE-2026-7080	A security vulnerability has been detected in Tenda F456 1.0.0.5. This impacts the function fromPPTPUserSetting of the file /goform/PPTPUserSetting of the component httpd. Such manipulation of the argument delno leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-7079	A weakness has been identified in Tenda F456 1.0.0.5. This affects the function fromAdvSetWan of the file /goform/AdvSetWan of the component httpd. This manipulation of the argument wanmode causes buffer overflow. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-7078	A security flaw has been discovered in Tenda F456 1.0.0.5. The impacted element is the function fromSetIpBind of the file /goform/SetIpBind of the component httpd. The manipulation of the argument page results in buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-42422	OpenClaw before 2026.4.8 contains a role bypass vulnerability in the device.token.rotate function that allows minting tokens for unapproved roles. Attackers can bypass device role-upgrade pairing to preserve or mint roles and scopes that had not undergone intended approval.	8.8	More Details
CVE-2026-	A vulnerability was identified in D-Link DIR-825 3.00b32. This affects the function NMBD_process of the file sserver.c of the component nmbd. Such manipulation leads to buffer overflow. The attack can only be initiated within the local network. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the	8.8	More Details

7068	maintainer.		
CVE-2026-42426	OpenClaw before 2026.4.8 contains an improper authorization vulnerability where the node.pair.approve method accepts operator.write scope instead of the narrower operator.pairing scope, allowing unprivileged users to approve node pairing. Attackers with operator.write permissions can bypass pairing approval restrictions to gain unauthorized access to exec-capable nodes.	8.8	More Details
CVE-2026-41208	Paperclip is a Node.js server and React UI that orchestrates a team of AI agents to run a business. Versions of @paperclipai/server prior to 2026.416.0 contain a privilege escalation vulnerability that allows an attacker with an Agent API key to execute arbitrary OS commands on the Paperclip server host. An attacker with an agent credential can escalate privileges from the agent runtime to the Paperclip server host. The vulnerability occurs because agents are allowed to update their own adapterConfig via the /agents/:id API endpoint. The configuration field adapterConfig.workspaceStrategy.provisionCommand is later executed by the server runtime. As a result, an attacker controlling an agent credential can inject arbitrary shell commands which are executed by the Paperclip server during workspace provisioning. This breaks the intended trust boundary between agent runtime configuration and server host execution, allowing a compromised or malicious agent to escalate privileges and run commands on the host system. This vulnerability allows remote code execution on the server host. @paperclipai/server version 2026.416.0 fixes the issue.	8.8	More Details
CVE-2026-41133	pyLoad is a free and open-source download manager written in Python. Versions up to and including 0.5.0b3.dev97 cache `role` and `permission` in the session at login and continues to authorize requests using these cached values, even after an admin changes the user's role/permissions in the database. As a result, an already logged-in user can keep old (revoked) privileges until logout/session expiry, enabling continued privileged actions. This is a core authorization/session-consistency issue and is not resolved by toggling an optional security feature. Commit e95804fb0d06cbb07d2ba380fc494d9ff89b68c1 contains a fix for the issue.	8.8	More Details
CVE-2026-7053	A security flaw has been discovered in Tenda F456 1.0.0.5. This affects the function frmL7ProtForm of the file /goform/L7Prot of the component httpd. Performing a manipulation of the argument page results in buffer overflow. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-7057	A flaw has been found in Tenda F456 1.0.0.5. The affected element is an unknown function of the file /goform/setcfm of the component httpd. This manipulation of the argument funcname/funcpara1 causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-7056	A vulnerability was detected in Tenda F456 1.0.0.5. Impacted is the function fromSafeUrlFilter of the file /goform/SafeUrlFilter of the component httpd. The manipulation of the argument page results in buffer overflow. The attack may be performed from remote. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7054	A weakness has been identified in Tenda F456 1.0.0.5. This vulnerability affects the function fromPptpUserAdd of the file /goform/PPTPDClient of the component httpd. Executing a manipulation of the argument opttype/usernamewith can lead to buffer overflow. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-7033	A vulnerability has been found in Tenda F456 1.0.0.5. Affected by this vulnerability is the function fromSafeClientFilter of the file /goform/SafeClientFilter. Such manipulation of the argument menufacturer/Go leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-31588	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Use scratch field in MMIO fragment to hold small write values When exiting to userspace to service an emulated MMIO write, copy the to-be-written value to a scratch field in the MMIO fragment if the size of the data payload is 8 bytes or less, i.e. can fit in a single chunk, instead of pointing the fragment directly at the source value. This fixes a class of use-after-free bugs that occur when the emulator initiates a write using an on-stack, local variable as the source, the write splits a page boundary, *and* both pages are MMIO pages. Because KVM's ABI only allows for physically contiguous MMIO requests, accesses that split MMIO pages are separated into two fragments, and are sent to userspace one at a time. When KVM attempts to complete userspace MMIO in response to KVM_RUN after the first fragment, KVM will detect the second fragment and generate a second userspace exit, and reference the on-stack variable. The issue is most visible if the second KVM_RUN is performed by a separate task, in which case the stack of the initiating task can show up as truly freed data. == BUG: KASAN: use-after-free in complete_emulated_mmio+0x305/0x420 Read of size 1 at addr ffff888009c378d1 by task syz-executor417/984 CPU: 1 PID: 984 Comm: syz-executor417 Not tainted 5.10.0-182.0.0.95.h2627.eulerosv2r13.x86_64 #3 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.15.0-0-g2dd4b9b3f840-prebuilt.qemu.org 04/01/2014 Call Trace: dump_stack+0xbe/0xfd print_address_description.constprop.0+0x19/0x170 __kasan_report.cold+0x6c/0x84 kasan_report+0x3a/0x50 check_memory_region+0xfd/0x1f0 memcpy+0x20/0x60 complete_emulated_mmio+0x305/0x420 kvm_arch_vcpu_ioctl_run+0x63f/0x6d0 kvm_vcpu_ioctl+0x413/0xb20 __se_sys_ioctl+0x111/0x160 do_syscall_64+0x30/0x40 entry_SYSCALL_64_after_hwframe+0x67/0xd1 RIP: 0033:0x42477d Code: <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007faa8e6890e8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00000000004d7338 RCX: 000000000042477d RDX: 0000000000000000 RSI: 000000000000ae80 RDI: 0000000000000005 RBP: 00000000004d7330 R08: 00007fff28d546df R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 00000000004d733c R13: 0000000000000000 R14: 000000000040a200 R15: 00007fff28d54720 The buggy address belongs to the page: page:0000000029f6a428 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x9c37 flags: 0xfffffc0000000(node=0|zone=1|lastcpupid=0x1fffff) raw: 000fffffc0000000 0000000000000000 ffffea0000270dc8 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff888009c37780: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ffff888009c37800: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff >ffff888009c37880: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ^ ffff888009c37900: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ffff888009c37980: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff == The bug can also be reproduced with a targeted KVM-Unit-Test by hacking KVM to fill a large on-stack variable in complete_emulated_mmio(), i.e. by overwrite the data value with garbage. Limit the use of the scratch fields to 8-byte or	8.8	More Details

	smaller accesses, and to just writes, as larger accesses and reads are not affected thanks to implementation details in the emulator, but add a sanity check to ensure those details don't change in the future. Specifically, KVM never uses on-stack variables for accesses larger that 8 bytes, e.g. uses an operand in the emulator context, and *al ---truncated---		
CVE-2026-7031	A vulnerability was detected in Tenda F456 1.0.0.5. This impacts the function fromSafeMacFilter of the file /goform/SafeMacFilter. The manipulation of the argument page results in buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7030	A security vulnerability has been detected in Tenda F456 1.0.0.5. This affects the function fromRouteStatic of the file /goform/RouteStatic. The manipulation of the argument page leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-7099	A vulnerability was detected in Tenda F456 1.0.0.5. The affected element is the function formQuickIndex of the file /goform/QuickIndex of the component httpd. Performing a manipulation of the argument mit_linktype results in buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7098	A security vulnerability has been detected in Tenda F456 1.0.0.5. Impacted is the function fromDhcpListClient of the file /goform/DhcpListClient of the component httpd. Such manipulation of the argument page leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-40473	The camel-mina component's MinaConverter.toObjectInput(IoBuffer) type converter wraps an IoBuffer in a java.io.ObjectInputStream without applying any ObjectInputFilter or class-loading restrictions. When a Camel route uses camel-mina as a TCP or UDP consumer and requests conversion to ObjectInput (for example via getBody(ObjectInput.class) or @Body ObjectInput), an attacker sending a crafted serialized Java object over the network to the MINA consumer port can trigger arbitrary code execution in the context of the application during readObject(). This issue affects Apache Camel: from 3.0.0 before 4.14.6, from 4.15.0 before 4.18.2, from 4.19.0 before 4.20.0. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.2.	8.8	More Details
CVE-2026-7097	A weakness has been identified in Tenda F456 1.0.0.5. This issue affects the function fromwebExcptypemanFilter of the file /goform/webExcptypemanFilter of the component httpd. This manipulation of the argument page causes buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-7096	A security flaw has been discovered in Tenda HG3 2.0 300003070. This vulnerability affects the function formgponConf of the file /boaform/admin/formgponConf. The manipulation of the argument fmgpon_loid results in os command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-7160	A vulnerability was determined in Tenda HG3 2.0. This vulnerability affects the function formTracert of the file /boaform/formTracert. Executing a manipulation of the argument datasize can lead to command injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-41241	pretalx is a conference planning tool. Prior to 2026.1.0, The organiser search in the pretalx backend rendered submission titles, speaker display names, and user names/emails into the result dropdown using innerHTML string interpolation. Any user who controls one of those fields (which includes any registered user whose display name is looked up by an administrator) could include HTML or JavaScript that would execute in an organiser's browser when the organiser's search query matched the malicious record. This vulnerability is fixed in 2026.1.0.	8.7	More Details
CVE-2026-41468	Beghelli Sicuro24 SicuroWeb embeds AngularJS 1.5.2, an end-of-life component containing known sandbox escape primitives. When combined with template injection present in the same application, these primitives allow attackers to escape the AngularJS sandbox and achieve arbitrary JavaScript execution in operator browser sessions, enabling session hijacking, DOM manipulation, and persistent browser compromise. Network-adjacent attackers can deliver the complete injection and escape chain via MITM in plaintext HTTP deployments without active user interaction.	8.7	More Details
CVE-2026-33317	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. In versions 3.13.0 through 4.10.0, missing checks in `entry_get_attribute_value()` in `ta/pkcs11/src/object.c` can lead to out-of-bounds read from the PKCS#11 TA heap or a crash. When chained with the OOB read, the PKCS#11 TA function `PKCS11_CMD_GET_ATTRIBUTE_VALUE` or `entry_get_attribute_value()` can, with a bad template parameter, be tricked into reading at most 7 bytes beyond the end of the template buffer and writing beyond the end of the template buffer with the content of an attribute value of a PKCS#11 object. Commits e031c4e562023fd9f199e39fd2e85797e4cbdca9, 16926d5a46934c46e6656246b4fc18385a246900, and 149e8d7ecc4ef8bb00ab4a37fd2ccede6d79e1ca contain patches and are anticipated to be part of version 4.11.0.	8.7	More Details
CVE-2026-40967	In Spring AI, various FilterExpressionConverter implementations accept a filter expression object and translate them to specific vector store query languages. In several cases, keys and values are not properly escaped, leading to the ability to alter the query. Affected versions: Spring AI: 1.0.0 - 1.0.5 (fixed in 1.0.6), 1.1.0 - 1.1.4 (fixed in 1.1.5)	8.6	More Details
CVE-2026-5367	A flaw was found in OVN (Open Virtual Network). A remote attacker, by sending crafted DHCPv6 (Dynamic Host Configuration Protocol for IPv6) SOLICIT packets with an inflated Client ID length, could cause the ovn-controller to read beyond the bounds of a packet. This out-of-bounds read can lead to the disclosure of sensitive information stored in heap memory, which is then returned to the attacker's virtual machine port.	8.6	More Details
CVE-2026-26150	Server-side request forgery (ssrf) in Microsoft Purview allows an unauthorized attacker to elevate privileges over a network.	8.6	More Details
CVE-2026-	Xerte Online Toolkits versions 3.15 and earlier contain a missing authentication vulnerability in the elFinder connector endpoint at /editor/elfinder/php/connector.php where an HTTP redirect to unauthenticated callers does not call exit() or die(), allowing PHP execution to continue and process the full request server-side. Unauthenticated attackers can perform file operations on project media directories including creating directories, uploading files, renaming files, duplicating files,	8.6	More Details

34413	overwriting files, and deleting files, which can be chained with path traversal and extension blocklist vulnerabilities to achieve remote code execution and arbitrary file read.		
CVE-2026-24222	NVIDIA NeMoClaw contains a vulnerability in the sandbox environment initialization component, where a remote attacker could cause improper access control by sending prompt-injected content that causes the agent to read and exfiltrate host environment variables not properly restricted during sandbox creation. A successful exploit of this vulnerability might lead to information disclosure.	8.6	More Details
CVE-2026-31611	In the Linux kernel, the following vulnerability has been resolved: ksmbd: require 3 sub-authorities before reading sub_auth[2] parse_dacl() compares each ACE SID against sid_unix_NFS_mode and on match reads sid.sub_auth[2] as the file mode. If sid_unix_NFS_mode is the prefix S-1-5-88-3 with num_subauth = 2 then compare_sids() compares only min(num_subauth, 2) sub-authorities so a client SID with num_subauth = 2 and sub_auth = {88, 3} will match. If num_subauth = 2 and the ACE is placed at the very end of the security descriptor, sub_auth[2] will be 4 bytes past end_of_acl. The out-of-band bytes will then be masked to the low 9 bits and applied as the file's POSIX mode, probably not something that is good to have happen. Fix this up by forcing the SID to actually carry a third sub-authority before reading it at all.	8.6	More Details
CVE-2026-41455	WeKan before 8.35 contains a server-side request forgery vulnerability in webhook integration URL handling where the url schema field accepts any string without protocol restriction or destination validation. Attackers who can create or modify integrations can set webhook URLs to internal network addresses, causing the server to issue HTTP POST requests to attacker-controlled internal targets with full board event payloads, and can additionally exploit response handling to overwrite arbitrary comment text without authorization checks.	8.5	More Details
CVE-2026-35548	An issue was discovered in guardsix (formerly Logpoint) ODBC Enrichment Plugins before 5.2.1 (5.2.1 is used in guardsix 7.9.0.0). A logic flaw allowed stored database credentials to be reused after modification of the target Host, IP address, or Port. When editing an existing Enrichment Source, previously stored credentials were retained even if the connection endpoint was changed. An authenticated Operator user could redirect the database connection to unintended internal systems, resulting in SSRF and potential misuse of valid stored credentials.	8.5	More Details
CVE-2026-41914	OpenClaw before 2026.4.8 contains a server-side request forgery vulnerability in QQ Bot media download paths that bypass SSRF protection. Attackers can exploit unprotected media fetch endpoints to access internal resources and bypass allowlist policies.	8.5	More Details
CVE-2026-41371	OpenClaw before 2026.3.28 contains a privilege escalation vulnerability in chat.send that allows write-scoped gateway callers to trigger admin-only session reset operations. Attackers can rotate target sessions, archive prior transcript state, and force new session IDs without requiring admin scope by exploiting improper authorization checks in the chat.send path.	8.5	More Details
CVE-2026-41230	Froxlor is open source server administration software. Prior to version 2.3.6, `DomainZones::add()` accepts arbitrary DNS record types without a whitelist and does not sanitize newline characters in the `content` field. When a DNS type not covered by the if/elseif validation chain is submitted (e.g., `NAPTR`, `PTR`, `HINFO`), content validation is entirely bypassed. Embedded newline characters in the content survive `trim()` processing, are stored in the database, and are written directly into BIND zone files via `DnsEntry::__toString()`. An authenticated customer can inject arbitrary DNS records and BIND directives (`$INCLUDE`, `$ORIGIN`, `$GENERATE`) into their domain's zone file. Version 2.3.6 fixes the issue.	8.5	More Details
CVE-2026-41461	SocialEngine versions 7.8.0 and prior contain a blind server-side request forgery vulnerability in the /core/link/preview endpoint where user-supplied input passed via the uri request parameter is not sanitized before being used to construct outbound HTTP requests. Authenticated remote attackers can supply arbitrary URLs including internal network addresses and loopback addresses to cause the server to issue HTTP requests to attacker-controlled destinations, enabling internal network enumeration and access to services not intended to be externally reachable.	8.5	More Details
CVE-2026-5398	The implementation of TIOCNOTTY failed to clear a back-pointer from the structure representing the controlling terminal to the calling process' session. If the invoking process then exits, the terminal structure may end up containing a pointer to freed memory. A malicious process can abuse the dangling pointer to grant itself root privileges.	8.4	More Details
CVE-2026-41433	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. From 0.4.0 to before 0.8.0, a flaw in the Java agent injection path allows a local attacker controlling a Java workload to overwrite arbitrary host files when Java injection is enabled and OBI is running with elevated privileges. The injector trusted TMPDIR from the target process and used unsafe file creation semantics, enabling both filesystem boundary escape and symlink-based file clobbering. This vulnerability is fixed in 0.8.0.	8.4	More Details
CVE-2018-25265	LanSpy 2.0.1.159 contains a local buffer overflow vulnerability in the scan section that allows local attackers to execute arbitrary code by exploiting structured exception handling mechanisms. Attackers can craft malicious payloads using egghunter techniques to locate and execute shellcode, triggering code execution through SEH chain manipulation and controlled jumps.	8.4	More Details
CVE-2018-25259	Terminal Services Manager 3.1 contains a stack-based buffer overflow vulnerability in the computer names field that allows local attackers to execute arbitrary code by triggering structured exception handling. Attackers can craft a malicious input file with shellcode and jump instructions that overwrite the SEH handler pointer to execute calc.exe or other payloads when imported through the add computers wizard.	8.4	More Details
CVE-2018-25283	iSmartViewPro 1.5 contains a structured exception handling (SEH) buffer overflow vulnerability in the 'Save Path for Snapshot and Record file' field that allows local attackers to execute arbitrary code. Attackers can input a crafted payload exceeding 260 bytes through the System Setup interface to overwrite SEH records and execute shellcode with application privileges.	8.4	More Details
CVE-2018-25268	LanSpy 2.0.1.159 contains a local buffer overflow vulnerability that allows attackers to overwrite the instruction pointer by supplying oversized input to the scan field. Attackers can craft a payload with 688 bytes of padding followed by 4 bytes of controlled data to crash the application or potentially achieve code execution.	8.4	More Details

CVE-2018-25261	Iperius Backup 5.8.1 contains a local buffer overflow vulnerability in the structured exception handling (SEH) mechanism that allows local attackers to execute arbitrary code by supplying a malicious file path. Attackers can create a backup job with a crafted payload in the external file location field that triggers a buffer overflow when the backup job executes, enabling code execution with application privileges.	8.4	More Details
CVE-2018-25263	Faleemi Desktop Software 1.8.2 contains a local buffer overflow vulnerability in the Device alias field that allows local attackers to trigger a structured exception handler (SEH) overwrite. Attackers can craft a malicious payload and paste it into the Device alias field within the Managing Log interface to execute arbitrary code with calculator proof-of-concept execution.	8.4	More Details
CVE-2018-25260	MAGIX Music Editor 3.1 contains a buffer overflow vulnerability in the FreeDB Proxy Options dialog that allows local attackers to execute arbitrary code by exploiting structured exception handling. Attackers can craft a malicious payload, paste it into the Server field via the CD menu's FreeDB Proxy Options, and trigger code execution when settings are accepted.	8.4	More Details
CVE-2026-41271	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, a Server-Side Request Forgery (SSRF) vulnerability exists in FlowiseAI's POST/GET API Chain components that allows unauthenticated attackers to force the server to make arbitrary HTTP requests to internal and external systems. By injecting malicious prompt templates, attackers can bypass the intended API documentation constraints and redirect requests to sensitive internal services, potentially leading to internal network reconnaissance and data exfiltration. This vulnerability is fixed in 3.1.0.	8.3	More Details
CVE-2026-41454	WeKan before 8.35 contains a missing authorization vulnerability in the Integration REST API endpoints that allows authenticated board members to perform administrative actions without proper privilege verification. Attackers can enumerate integrations including webhook URLs, create new integrations, modify or delete existing integrations, and manage integration activities by exploiting insufficient authorization checks in the JsonRoutes REST handlers.	8.3	More Details
CVE-2026-40937	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-alpha.94, all four notification target admin API endpoints in `rustfs/src/admin/handlers/event.rs` use a `check_permissions` helper that validates authentication only (access key + session token), without performing any admin-action authorization via `validate_admin_request`. Every other admin handler in the codebase correctly calls `validate_admin_request` with a specific `AdminAction`. This is the only admin handler file that skips authorization. A non-admin user can overwrite a shared admin-defined notification target by name, causing subsequent bucket events to be delivered to an attacker-controlled endpoint. This enables cross-user event interception and audit evasion. 1.0.0-alpha.94 contains a patch.	8.3	More Details
CVE-2026-6921	Race in GPU in Google Chrome on Windows prior to 147.0.7727.117 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-38651	Authentication Bypass vulnerability exists in Netmaker versions prior to 1.5.0. The VerifyHostToken function in logic/jwts.go fails to validate the JWT signature when verifying host tokens. An attacker can forge a JWT signed with any arbitrary key and use it to impersonate any host in the network, gaining access to sensitive information	8.2	More Details
CVE-2026-40022	When authentication is enabled on the Apache Camel embedded HTTP server or embedded management server (camel-platform-http-main) and a non-root context path such as /api or /admin is configured via camel.server.path or camel.management.path, the BasicAuthenticationConfigurer and JWTAuthenticationConfigurer classes derive the authentication path from properties.getPath() when camel.server.authenticationPath / camel.management.authenticationPath is not explicitly set. Combined with the Vert.x sub-router mounting model - the sub-router is mounted at _path_* and the authentication handler is registered inside the sub-router at the resolved path - this causes the authentication handler to match only the exact configured context path, not its subpaths. Unauthenticated requests to subpaths such as /api/_route_ or /admin/observe/info therefore reach protected business routes and management endpoints without being challenged for credentials. The /observe/info endpoint can disclose runtime metadata such as the user, working directory, home directory, process ID, JVM and operating system information. This issue affects Apache Camel: from 4.14.1 before 4.14.6, from 4.18.0 before 4.18.2. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, they are suggested to upgrade to 4.14.6. If users are on the 4.18.x LTS releases stream, they are suggested to upgrade to 4.18.2.	8.2	More Details
CVE-2026-41309	Open Source Social Network (OSSN) is open-source social networking software developed in PHP. Versions prior to 9.0 are vulnerable to resource exhaustion. An attacker can upload a specially crafted image with extreme pixel dimensions (e.g., 10000×10000 pixels). While the compressed file size on disk may be small, the server attempts to allocate significant memory and CPU cycles during the decompression and resizing process, leading to a Denial of Service (DoS) condition. It is highly recommended to upgrade to OSSN 9.0. This version introduces stricter validation of image dimensions and improved resource management during the processing phase. Those who cannot upgrade immediately can mitigate the risk by adjusting their `php.ini` settings to strictly limit `memory_limit` and `max_execution_time` and/or implementing a client-side and server-side check on image headers to reject files exceeding reasonable pixel dimensions (e.g., 4000×4000 pixels) before processing begins.	8.2	More Details
CVE-2026-41273	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, Flowise contains an authentication bypass vulnerability that allows an unauthenticated attacker to obtain OAuth 2.0 access tokens associated with a public chatflow. By accessing a public chatflow configuration endpoint, an attacker can retrieve internal workflow data, including OAuth credential identifiers, which can then be used to refresh and obtain valid OAuth 2.0 access tokens without authentication. This vulnerability is fixed in 3.1.0.	8.2	More Details
CVE-2026-31476	In the Linux kernel, the following vulnerability has been resolved: ksmbd: do not expire session on binding failure When a multichannel session binding request fails (e.g. wrong password), the error path unconditionally sets sess->state = SMB2_SESSION_EXPIRED. However, during binding, sess points to the target session looked up via ksmbd_session_lookup_slowpath() -- which belongs to another connection's user. This allows a remote attacker to invalidate any active session by simply sending a binding request with a wrong password (DoS). Fix this by skipping session expiration when the failed request was a binding attempt, since the session does not belong to the current connection. The reference	8.2	More Details

	taken by ksmbd_session_lookup_slowpath() is still correctly released via ksmbd_user_session_put().		
CVE-2026-41394	OpenClaw before 2026.3.31 contains an authentication bypass vulnerability where unauthenticated plugin-auth HTTP routes receive operator runtime write scopes. Attackers can access these routes without authentication to perform privileged runtime actions intended for authorized operators.	8.2	More Details
CVE-2026-41604	Out-of-bounds Read vulnerability in Apache Thrift. This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	8.2	More Details
CVE-2026-40344	MinIO is a high-performance object storage system. Starting in RELEASE.2023-05-18T00-05-36Z and prior to RELEASE.2026-04-11T03-20-12Z, an authentication bypass vulnerability in MinIO's Snowball auto-extract handler (`PutObjectExtractHandler`) allows any user who knows a valid access key to write arbitrary objects to any bucket without knowing the secret key or providing a valid cryptographic signature. Any MinIO deployment is impacted. The attack requires only a valid access key (the well-known default `minioadmin`, or any key with WRITE permission on a bucket) and a target bucket name. When `authTypeStreamingUnsignedTrailer` support was added, the new auth type was handled in `PutObjectHandler` and `PutObjectPartHandler` but was never added to `PutObjectExtractHandler`. The snowball auto-extract handler's `switch rAuthType` block has no case for `authTypeStreamingUnsignedTrailer`, so execution falls through with zero signature verification. The `isPutActionAllowed` call before the switch extracts the access key and checks IAM permissions, but does not verify the cryptographic signature. An attacker sends a PUT request with `X-Amz-Content-Sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER`, `X-Amz-Meta-Snowball-Auto-Extract: true`, and an `Authorization` header containing a valid access key with a completely fabricated signature. The request is accepted and the tar payload is extracted into the bucket. Users of the open-source minio/minio project should upgrade to MinIO AIStor RELEASE.2026-04-11T03-20-12Z or later. If upgrading is not immediately possible, block unsigned-trailer requests at the load balancer. Reject any request containing X-Amz-Content-Sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER at the reverse proxy or WAF layer. Clients can use STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER (the signed variant) instead. Alternatively, restrict WRITE permissions. Limit s3:PutObject grants to trusted principals. While this reduces the attack surface, it does not eliminate the vulnerability since any user with WRITE permission can exploit it with only their access key.	8.2	More Details
CVE-2026-5944	An improper access control vulnerability exists in the Cisco Intersight Device Connector for Nutanix Prism Central. The service exposes an API passthrough endpoint on TCP port 7373 that is accessible within the network scope of the deployment environment without authentication. An unauthenticated attacker with network access can exploit this vulnerability by sending crafted requests to the exposed endpoint to enumerate cluster metadata, including virtual machine information and cluster configuration details. While the API primarily supports read-only operations, it also allows certain cluster maintenance workflows to be invoked. Although this vulnerability does not allow persistent modification of system configurations or access to credentials or sensitive user data, successful exploitation may result in disruption of active workloads, leading to loss of service availability within the affected environment.	8.2	More Details
CVE-2026-41059	OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Versions 7.5.0 through 7.15.1 have a configuration-dependent authentication bypass. Deployments are affected when all of the following are true: Use of `skip_auth_routes` or the legacy `skip_auth_regex`; use of patterns that can be widened by attacker-controlled suffixes, such as `^/foo/.*/bar$` causing potential exposure of `/foo/secret`; and protected upstream applications that interpret `#` as a fragment delimiter or otherwise route the request to the protected base path. In deployments that rely on these settings, an unauthenticated attacker can send a crafted request containing a number sign in the path, including the browser-safe encoded form `%23`, so that OAuth2 Proxy matches a public allowlist rule while the backend serves a protected resource. Deployments that do not use these skip-auth options, or that only allow exact public paths with tightly scoped method and path rules, are not affected. A fix has been implemented in version 7.15.2 to normalize request paths more conservatively before skip-auth matching so fragment content does not influence allowlist decisions. Users who cannot upgrade immediately can reduce exposure by tightening or removing `skip_auth_routes` and `skip_auth_regex` rules, especially patterns that use broad wildcards across path segments. Recommended mitigations include replacing broad rules with exact, anchored public paths and explicit HTTP methods; rejecting requests whose path contains `%23` or `#` at the ingress, load balancer, or WAF level; and/or avoiding placing sensitive application paths behind broad `skip_auth_routes` rules.	8.2	More Details
CVE-2026-31631	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix buffer overread in rxgk_do_verify_authenticator() Fix rxgk_do_verify_authenticator() to check the buffer size before checking the nonce.	8.2	More Details
CVE-2026-41145	MinIO is a high-performance object storage system. Starting in RELEASE.2023-05-18T00-05-36Z and prior to RELEASE.2026-04-11T03-20-12Z, an authentication bypass vulnerability in MinIO's `STREAMING-UNSIGNED-PAYLOAD-TRAILER` code path allows any user who knows a valid access key to write arbitrary objects to any bucket without knowing the secret key or providing a valid cryptographic signature. Any MinIO deployment is impacted. The attack requires only a valid access key (the well-known default `minioadmin`, or any key with WRITE permission on a bucket) and a target bucket name. `PutObjectHandler` and `PutObjectPartHandler` call `newUnsignedV4ChunkedReader` with a signature verification gate based solely on the presence of the `Authorization` header. Meanwhile, `isPutActionAllowed` extracts credentials from either the `Authorization` header or the `X-Amz-Credential` query parameter, and trusts whichever it finds. An attacker omits the `Authorization` header and supplies credentials exclusively via the query string. The signature gate evaluates to `false`, `doesSignatureMatch` is never called, and the request proceeds with the permissions of the impersonated access key. This affects `PutObjectHandler` (standard and tables/warehouse bucket paths) and `PutObjectPartHandler` (multipart uploads). Users of the open-source `minio/minio` project should upgrade to MinIO AIStor `RELEASE.2026-04-11T03-20-12Z` or later. If upgrading is not immediately possible, block unsigned-trailer requests at the load balancer. Reject any request containing `X-Amz-Content-Sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER` at the reverse proxy or WAF layer. Clients can use `STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER` (the signed variant) instead. Alternatively, restrict WRITE permissions. Limit `s3:PutObject` grants to trusted principals. While this reduces the attack surface, it does not eliminate the vulnerability since any user with WRITE permission can exploit it with only their access key.	8.2	More Details
	In the Linux kernel, the following vulnerability has been resolved: scsi: ibmvfc: Fix OOB access in ibmvfc_discover_targets_done() A malicious or compromised VIO server can return a num_written value in the discover		

CVE-2026-31464	targets MAD response that exceeds max_targets. This value is stored directly in vhost->num_targets without validation, and is then used as the loop bound in ibmvfc_alloc_targets() to index into disc_buf[], which is only allocated for max_targets entries. Indices at or beyond max_targets access kernel memory outside the DMA-coherent allocation. The out-of-bounds data is subsequently embedded in Implicit Logout and PLOGI MADs that are sent back to the VIO server, leaking kernel memory. Fix by clamping num_written to max_targets before storing it.	8.1	More Details
CVE-2026-4922	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.0 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed an unauthenticated user to execute GraphQL mutations on behalf of authenticated users due to insufficient CSRF protection.	8.1	More Details
CVE-2026-34587	Kirby is an open-source content management system. Prior to versions 4.9.0 and 5.4.0, Kirby's user permissions control which user role is allowed to perform specific actions to content models in the CMS. These permissions are defined for each role in the user blueprint (`site/blueprints/users/...`). It is also possible to customize the permissions for each target model in the model blueprints (such as in `site/blueprints/pages/...`) using the `options` feature. The permissions and options together control the authorization of user actions. For pages, Kirby provides the `pages.create` and `pages.changeStatus` permissions (among others). In affected releases, Kirby checked these permissions independently and only for the respective action. However the `changeStatus` permission didn't take effect on page creation. New pages are created as drafts by default and need to be published by changing the page status of an existing page draft. This is ensured when the page is created via the Kirby Panel. However the REST API allows to override the `isDraft` flag when creating a new page. This allowed authenticated attackers with the `pages.create` permission to immediately create published pages, bypassing the normal editorial workflow. The problem has been patched in Kirby 4.9.0 and Kirby 5.4.0. Kirby has updated the `Options` logic to no longer double-resolve queries in option values coming from `OptionsQuery` or `OptionsApi` sources. Kirby now only resolves queries that are directly configured in the blueprints.	8.1	More Details
CVE-2026-40623	A vulnerability in SenseLive X3050's web management interface allows critical system and network configuration parameters to be modified without sufficient validation and safety controls. Due to inadequate enforcement of constraints on sensitive functions, parameters such as IP addressing, watchdog timers, reconnect intervals, and service ports can be set to unsupported or unsafe values. These configuration changes directly affect core device behaviour and recovery mechanisms. The lack of proper validation and safeguards allows critical system functions to be altered in a manner that can destabilize device operation or render the device persistently unavailable.	8.1	More Details
CVE-2026-6786	Memory safety bugs present in Firefox ESR 140.9, Thunderbird ESR 140.9, Firefox 149 and Thunderbird 149. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	8.1	More Details
CVE-2026-31613	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix OOB reads parsing symlink error response When a CREATE returns STATUS_STOPPED_ON_SYMLINK, smb2_check_message() returns success without any length validation, leaving the symlink parsers as the only defense against an untrusted server. symlink_data() walks SMB 3.1.1 error contexts with the loop test "p < end", but reads p->ErrorId at offset 4 and p->ErrorDataLength at offset 0. When the server-controlled ErrorDataLength advances p to within 1-7 bytes of end, the next iteration will read past it. When the matching context is found, sym->SymLinkErrorTag is read at offset 4 from p->ErrorContextData with no check that the symlink header itself fits. smb2_parse_symlink_response() then bounds-checks the substitute name using SMB2_SYMLINK_STRUCT_SIZE as the offset of PathBuffer from iov_base. That value is computed as sizeof(smb2_err_rsp) + sizeof(smb2_symlink_err_rsp), which is correct only when ErrorContextCount == 0. With at least one error context the symlink data sits 8 bytes deeper, and each skipped non-matching context shifts it further by 8 + ALIGN(ErrorDataLength, 8). The check is too short, allowing the substitute name read to run past iov_len. The out-of-bound heap bytes are UTF-16-decoded into the symlink target and returned to userspace via readlink(2). Fix this all up by making the loops test require the full context header to fit, rejecting sym if its header runs past end, and bound the substitute name against the actual position of sym->PathBuffer rather than a fixed offset. Because sub_offs and sub_len are 16bits, the pointer math will not overflow here with the new greater-than.	8.1	More Details
CVE-2026-41246	Contour is a Kubernetes ingress controller using Envoy proxy. From v1.19.0 to before v1.33.4, v1.32.5, and v1.31.6, Contour's Cookie Rewriting feature is vulnerable to Lua code injection. An attacker with RBAC permissions to create or modify HTTPProxy resources can craft a malicious value in spec.routes[].cookieRewritePolicies[].pathRewrite.value or spec.routes[].services[].cookieRewritePolicies[].pathRewrite.value that results in arbitrary code execution in the Envoy proxy. The cookie rewriting feature is internally implemented using Envoy's HTTP Lua filter. User-controlled values are interpolated into Lua source code using Go text/template without sufficient sanitization. The injected code only executes when processing traffic on the attacker's own route, which they already control. However, since Envoy runs as shared infrastructure, the injected code can also read Envoy's xDS client credentials from the filesystem or cause denial of service for other tenants sharing the Envoy instance. This vulnerability is fixed in v1.33.4, v1.32.5, and v1.31.6.	8.1	More Details
CVE-2026-39462	A vulnerability exists in SenseLive X3050’s web management interface in which password updates are not reliably applied due to improper handling of credential changes on the backend. After the device undergoes a factory restore using the SenseLive Config 2.0 tool, the interface may indicate that the password update was successful; however, the system may continue to accept the previous or default credentials, demonstrating that the password-change process is not consistently enforced. Even after a factory reset, attempted password changes may fail to propagate correctly.	8.1	More Details
CVE-2026-6023	In Progress® Telerik® UI for AJAX versions 2024.4.1114 through 2026.1.421, the RadFilter control is vulnerable to insecure deserialization when restoring filter state if the state is exposed to the client. If an attacker tampers with this state, a server-side remote code execution is possible.	8.1	More Details
CVE-2026-6785	Memory safety bugs present in Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird ESR 140.9, Firefox 149 and Thunderbird 149. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	8.1	More Details
CVE-	A vulnerability in SenseLive X3050's web management interface allows state-changing operations to be triggered without proper Cross-Site Request Forgery (CSRF) protections. Because the application does not enforce server-side validation of		More

2026-27841	request origin or implement CSRF tokens, a malicious external webpage could cause a user's browser to submit unauthorized configuration requests to the device.	8.1	Details
CVE-2026-31513	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix stack-out-of-bounds read in l2cap_ecred_conn_req Syzbot reported a KASAN stack-out-of-bounds read in l2cap_build_cmd() that is triggered by a malformed Enhanced Credit Based Connection Request. The vulnerability stems from l2cap_ecred_conn_req(). The function allocates a local stack buffer (`pdu`) designed to hold a maximum of 5 Source Channel IDs (SCIDs), totaling 18 bytes. When an attacker sends a request with more than 5 SCIDs, the function calculates `rsp_len` based on this unvalidated `cmd_len` before checking if the number of SCIDs exceeds L2CAP_ECRED_MAX_CID. If the SCID count is too high, the function correctly jumps to the `response` label to reject the packet, but `rsp_len` retains the attacker's oversized value. Consequently, l2cap_send_cmd() is instructed to read past the end of the 18-byte `pdu` buffer, triggering a KASAN panic. Fix this by moving the assignment of `rsp_len` to after the `num_scid` boundary check. If the packet is rejected, `rsp_len` will safely remain 0, and the error response will only read the 8-byte base header from the stack.	8.1	More Details
CVE-2026-23902	Incorrect Authorization vulnerability in Apache DolphinScheduler allows authenticated users with system login permissions to use tenants that are not defined on the platform during workflow execution. This issue affects Apache DolphinScheduler versions prior to 3.4.1. Users are recommended to upgrade to version 3.4.1, which fixes this issue.	8.1	More Details
CVE-2026-41353	OpenClaw before 2026.3.22 contains an access control bypass vulnerability in the allowProfiles feature that allows attackers to circumvent profile restrictions through persistent profile mutation and runtime profile selection. Remote attackers can exploit this by manipulating browser proxy profiles at runtime to access restricted profiles and bypass intended access controls.	8.1	More Details
CVE-2026-5364	The Drag and Drop File Upload for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file upload in versions up to, and including, 1.1.3. This is due to the plugin extracting the file extension before sanitization occurs and allowing the file type parameter to be controlled by the attacker rather than being restricted to administrator-configured values, which when combined with the fact that validation occurs on the unsanitized extension while the file is saved with a sanitized extension, allows special characters like '$' to be stripped during the save process. This makes it possible for unauthenticated attackers to upload arbitrary PHP files and potentially achieve remote code execution, however, an .htaccess file and name randomization is in place which restricts real-world exploitability.	8.1	More Details
CVE-2026-41267	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, an improper mass assignment (JSON injection) vulnerability in the account registration endpoint of Flowise Cloud allows unauthenticated attackers to inject server-managed fields and nested objects during account creation. This enables client-controlled manipulation of ownership metadata, timestamps, organization association, and role mappings, breaking trust boundaries in a multi-tenant environment. This vulnerability is fixed in 3.1.0.	8.1	More Details
CVE-2026-41383	OpenClaw before 2026.4.2 contains an arbitrary directory deletion vulnerability in mirror mode that allows attackers to delete remote directories by influencing remoteWorkspaceDir and remoteAgentWorkspaceDir configuration values. Attackers can manipulate these OpenShell config paths to cause mirror sync operations to delete unintended remote directory contents and replace them with uploaded workspace data.	8.1	More Details
CVE-2026-27760	OpenCATS prior to commit 3002a29 contains a PHP code injection vulnerability in the installer AJAX endpoint that allows unauthenticated attackers to execute arbitrary code by injecting PHP statements into the databaseConnectivity action parameter. Attackers can break out of the define() string context in config.php using a single quote and statement separator to inject malicious PHP code that persists and executes on every subsequent page load when the installation wizard remains incomplete.	8.1	More Details
CVE-2026-41175	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.20 and 6.13.0, manipulating query parameters on Control Panel and REST API endpoints, or arguments in GraphQL queries, could result in the loss of content, assets, and user accounts. The Control Panel requires authentication with minimal permissions in order to exploit. e.g. "view entries" permission to delete entries, or "view users" permission to delete users, etc. The REST and GraphQL API exploits do not require any permissions, however neither are enabled by default. In order to be exploited, they would need to be explicitly enabled with no authentication configured, and the specific resources enabled too. Sites that enable the REST or GraphQL API without authentication should treat patching as critical priority. This has been fixed in 5.73.20 and 6.13.0.	8.1	More Details
CVE-2026-41316	ERB is a templating system for Ruby. Ruby 2.7.0 (before ERB 2.2.0 was published on rubygems.org) introduced an `@_init` instance variable guard in `ERB#result` and `ERB#run` to prevent code execution when an ERB object is reconstructed via `Marshal.load` (deserialization). However, three other public methods that also evaluate `@src` via `eval()` were not given the same guard: `ERB#def_method`, `ERB#def_module`, and `ERB#def_class`. An attacker who can trigger `Marshal.load` on untrusted data in a Ruby application that has `erb` loaded can use `ERB#def_module` (zero-arg, default parameters) as a code execution sink, bypassing the `@_init` protection entirely. ERB 4.0.3.1, 4.0.4.1, 6.0.1.1, and 6.0.4 patch the issue.	8.1	More Details
CVE-2026-41364	OpenClaw before 2026.3.31 contains a symlink following vulnerability in SSH sandbox tar upload that allows remote attackers to write arbitrary files. Attackers can exploit this by uploading tar archives containing symlinks to escape the sandbox and overwrite files on the remote host.	8.1	More Details
CVE-2026-42431	OpenClaw before 2026.4.8 contains a security bypass vulnerability in node.invoke(browser.proxy) that allows mutation of persistent browser profiles. Attackers can exploit this path to circumvent the browser.request persistent profile-mutation guard and modify browser configurations.	8.1	More Details
CVE-2026-41323	Kyverno is a policy engine designed for cloud native platform engineering teams. Prior to versions 1.18.0-rc1, 1.17.2-rc1, and 1.16.4, Kyverno's apiCall feature in ClusterPolicy automatically attaches the admission controller's ServiceAccount token to outgoing HTTP requests. The service URL has no validation — it can point anywhere, including attacker-controlled servers. Since the admission controller SA has permissions to patch webhook configurations, a stolen token leads to full cluster compromise. Versions 1.18.0-rc1, 1.17.2-rc1, and 1.16.4 patch the issue.	8.1	More Details
CVE-	mod_sql in ProFTPD before 1.3.10rc1 allows remote attackers to execute arbitrary code via a username, in scenarios where		

2026-42167	there is logging of USER requests with an expansion such as %U, and the SQL backend allows commands (e.g., COPY TO PROGRAM).	8.1	More Details
CVE-2026-26354	Dell PowerProtect Data Domain with Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain a stack-based Buffer Overflow vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution.	8.1	More Details
CVE-2026-5262	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.1.0 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that under certain conditions could have allowed an unauthenticated user to access tokens in the Storybook development environment due to improper input validation.	8.0	More Details
CVE-2026-5816	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.10 before 18.10.4 and 18.11 before 18.11.1 that could have allowed an unauthenticated user to execute arbitrary JavaScript in a user's browser session due to improper path validation under certain conditions.	8.0	More Details
CVE-2026-32172	Uncontrolled search path element in Microsoft Power Apps allows an unauthorized attacker to execute code over a network.	8.0	More Details
CVE-2026-7069	A security flaw has been discovered in D-Link DIR-825 up to 3.00b32. This impacts the function AddPortMapping of the file upnpsoap.c of the component miniupnpd. Performing a manipulation of the argument NewPortMappingDescription results in buffer overflow. The attack needs to be approached within the local network. The exploit has been released to the public and may be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	8.0	More Details
CVE-2026-31511	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix dangling pointer on mgmt_add_adv_patterns_monitor_complete This fixes the condition checking so mgmt_pending_valid is executed whenever status != -ECANCELED otherwise calling mgmt_pending_free(cmd) would kfree(cmd) without unlinking it from the list first, leaving a dangling pointer. Any subsequent list traversal (e.g., mgmt_pending_foreach during __mgmt_power_off, or another mgmt_pending_valid call) would dereference freed memory.	7.8	More Details
CVE-2026-41387	OpenClaw before 2026.3.22 contains an incomplete host environment variable sanitization vulnerability in host-env-security-policy.json and host-env-security.ts that allows package-manager environment overrides. Attackers can exploit approved exec requests to redirect package resolution or runtime bootstrap to attacker-controlled infrastructure and execute trojanized content.	7.8	More Details
CVE-2026-31650	In the Linux kernel, the following vulnerability has been resolved: mmc: vub300: fix use-after-free on disconnect The vub300 driver maintains an explicit reference count for the controller and its driver data and the last reference can in theory be dropped after the driver has been unbound. This specifically means that the controller allocation must not be device managed as that can lead to use-after-free. Note that the lifetime is currently also incorrectly tied the parent USB device rather than interface, which can lead to memory leaks if the driver is unbound without its device being physically disconnected (e.g. on probe deferral). Fix both issues by reverting to non-managed allocation of the controller.	7.8	More Details
CVE-2026-31578	In the Linux kernel, the following vulnerability has been resolved: media: as102: fix to not free memory after the device is registered in as102_usb_probe() In as102_usb driver, the following race condition occurs: ``` CPU0 CPU1 as102_usb_probe() kzalloc(); // alloc as102_dev_t .... usb_register_dev(); fd = sys_open("/path/to/dev"); // open as102 fd .... usb_deregister_dev(); .... kfree(); // free as102_dev_t .... sys_close(fd); as102_release() // UAF!! as102_usb_release() kfree(); // DFB!! ``` When a USB character device registered with usb_register_dev() is later unregistered (via usb_deregister_dev() or disconnect), the device node is removed so new open() calls fail. However, file descriptors that are already open do not go away immediately: they remain valid until the last reference is dropped and the driver's .release() is invoked. In as102, as102_usb_probe() calls usb_register_dev() and then, on an error path, does usb_deregister_dev() and frees as102_dev_t right away. If userspace raced a successful open() before the deregistration, that open FD will later hit as102_release() --> as102_usb_release() and access or free as102_dev_t again, occur a race to use-after-free and double-free vuln. The fix is to never kfree(as102_dev_t) directly once usb_register_dev() has succeeded. After deregistration, defer freeing memory to .release(). In other words, let release() perform the last kfree when the final open FD is closed.	7.8	More Details
CVE-2026-40048	The Camel-PQC FileBasedKeyLifecycleManager class deserializes the contents of `<keyId>.key` files in the configured key directory using java.io.ObjectInputStream without applying any ObjectInputFilter or class-loading restrictions. The cast to `java.security.KeyPair` is evaluated only after `readObject()` has already returned, so any `readObject()` side effects in the deserialized object run before the type check. An attacker who can write to the key directory used by a Camel application — for example through a path traversal into the directory, misconfigured filesystem permissions on the volume where keys are stored, a compromised key provisioning pipeline, or a symlink attack — can place a crafted serialized Java object that, when deserialized during normal key lifecycle operations, results in arbitrary code execution in the context of the application. This issue affects Apache Camel: from 4.19.0 before 4.20.0, from 4.18.0 before 4.18.2. Users are recommended to upgrade to version 4.20.0, which fixes the issue by replacing java.io.ObjectInputStream-based key and metadata storage with standard PKCS#8 (private key) / X.509 SubjectPublicKeyInfo (public key) Base64 JSON encoding. For users on the 4.18.x LTS releases stream, upgrade to 4.18.2.	7.8	More Details
CVE-2026-31506	In the Linux kernel, the following vulnerability has been resolved: net: bcmasp: fix double free of WoL irq We do not need to free wol_irq since it was instantiated with devm_request_irq(). So devres will free for us.	7.8	More Details
CVE-2026-31627	In the Linux kernel, the following vulnerability has been resolved: i2c: s3c24xx: check the size of the SMBUS message before using it The first byte of an i2c SMBUS message is the size, and it should be verified to ensure that it is in the range of 0..I2C_SMBUS_BLOCK_MAX before processing it. This is the same logic that was added in commit a6e04f05ce0b ("i2c: tegra: check msg length in SMBUS block read") to the i2c tegra driver.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: bcache: fix cached_dev.sb_bio use-after-free and crash In		

CVE-2026-31580	our production environment, we have received multiple crash reports regarding libceph, which have caught our attention: ``` [6888366.280350] Call Trace: [6888366.280452] blk_update_request+0x14e/0x370 [6888366.280561] blk_mq_end_request+0x1a/0x130 [6888366.280671] rbd_img_handle_request+0x1a0/0x1b0 [rbd] [6888366.280792] rbd_obj_handle_request+0x32/0x40 [rbd] [6888366.280903] __complete_request+0x22/0x70 [libceph] [6888366.281032] osd_dispatch+0x15e/0xb40 [libceph] [6888366.281164] ? inet_recvmsg+0x5b/0xd0 [6888366.281272] ? ceph_tcp_recvmsg+0x6f/0xa0 [libceph] [6888366.281405] ceph_con_process_message+0x79/0x140 [libceph] [6888366.281534] ceph_con_v1_try_read+0x5d7/0xf30 [libceph] [6888366.281661] ceph_con_workfn+0x329/0x680 [libceph] ``` After analyzing the coredump file, we found that the address of dc->sb_bio has been freed. We know that cached_dev is only freed when it is stopped. Since sb_bio is a part of struct cached_dev, rather than an alloc every time. If the device is stopped while writing to the superblock, the released address will be accessed at endio. This patch hopes to wait for sb_write to complete in cached_dev_free. It should be noted that we analyzed the cause of the problem, then tell all details to the QWEN and adopted the modifications it made.	7.8	More Details
CVE-2026-31541	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix trace_marker copy link list updates When the "copy_trace_marker" option is enabled for an instance, anything written into /sys/kernel/tracing/trace_marker is also copied into that instances buffer. When the option is set, that instance's trace_array descriptor is added to the marker_copies link list. This list is protected by RCU, as all iterations uses an RCU protected list traversal. When the instance is deleted, all the flags that were enabled are cleared. This also clears the copy_trace_marker flag and removes the trace_array descriptor from the list. The issue is after the flags are called, a direct call to update_marker_trace() is performed to clear the flag. This function returns true if the state of the flag changed and false otherwise. If it returns true here, synchronize_rcu() is called to make sure all readers see that its removed from the list. But since the flag was already cleared, the state does not change and the synchronization is never called, leaving a possible UAF bug. Move the clearing of all flags below the updating of the copy_trace_marker option which then makes sure the synchronization is performed. Also use the flag for checking the state in update_marker_trace() instead of looking at if the list is empty.	7.8	More Details
CVE-2026-31516	In the Linux kernel, the following vulnerability has been resolved: xfrm: prevent policy_hthresh.work from racing with netns teardown A XFRM_MSG_NEWSPDINFO request can queue the per-net work item policy_hthresh.work onto the system workqueue. The queued callback, xfrm_hash_rebuild(), retrieves the enclosing struct net via container_of(). If the net namespace is torn down before that work runs, the associated struct net may already have been freed, and xfrm_hash_rebuild() may then dereference stale memory. xfrm_policy_fini() already flushes policy_hash_work during teardown, but it does not synchronize policy_hthresh.work. Synchronize policy_hthresh.work in xfrm_policy_fini() as well, so the queued work cannot outlive the net namespace teardown and access a freed struct net.	7.8	More Details
CVE-2026-31683	In the Linux kernel, the following vulnerability has been resolved: batman-adv: avoid OGM aggregation when skb tailroom is insufficient When OGM aggregation state is toggled at runtime, an existing forwarded packet may have been allocated with only packet_len bytes, while a later packet can still be selected for aggregation. Appending in this case can hit skb_put overflow conditions. Reject aggregation when the target skb tailroom cannot accommodate the new packet. The caller then falls back to creating a new forward packet instead of appending.	7.8	More Details
CVE-2026-31508	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: Avoid releasing netdev before teardown completes The patch cited in the Fixes tag below changed the teardown code for OVS ports to no longer unconditionally take the RTNL. After this change, the netdev_destroy() callback can proceed immediately to the call_rcu() invocation if the IFF_OVS_DATAPATH flag is already cleared on the netdev. The ovs_netdev_detach_dev() function clears the flag before completing the unregistration, and if it gets preempted after clearing the flag (as can happen on an -rt kernel), netdev_destroy() can complete and the device can be freed before the unregistration completes. This leads to a splat like: [998.393867] Oops: general protection fault, probably for non-canonical address 0xff00000001000239: 0000 [#1] SMP PTI [998.393877] CPU: 42 UID: 0 PID: 55177 Comm: ip Kdump: loaded Not tainted 6.12.0-211.1.1.el10_2.x86_64+rt #1 PREEMPT_RT [998.393886] Hardware name: Dell Inc. PowerEdge R740/0JMK61, BIOS 2.24.0 03/27/2025 [998.393889] RIP: 0010:dev_set_promiscuity+0x8d/0xa0 [998.393901] Code: 00 00 75 d8 48 8b 53 08 48 83 ba b0 02 00 00 00 75 ca 48 83 c4 08 5b c3 cc cc cc cc 48 83 bf 48 09 00 00 00 75 91 48 8b 47 08 <48> 83 b8 b0 02 00 00 00 74 97 eb 81 0f 1f 80 00 00 00 00 90 90 90 [998.393906] RSP: 0018:ffffce5864a5f6a0 EFLAGS: 00010246 [998.393912] RAX: ff00000000ffff89 RBX: ffff894d0adf5a05 RCX: 0000000000000000 [998.393917] RDX: 0000000000000000 RSI: 00000000ffffffff RDI: ffff894d0adf5a05 [998.393921] RBP: ffff894d19252000 R08: ffff894d19252000 R09: 0000000000000000 [998.393924] R10: ffff894d19252000 R11: ffff894d192521b8 R12: 0000000000000006 [998.393927] R13: ffffce5864a5f738 R14: 00000000ffffffe2 R15: 0000000000000000 [998.393931] FS: 00007fad61971800(0000) GS:ffff894cc0140000(0000) knlGS:0000000000000000 [998.393936] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [998.393940] CR2: 000055df0a2a6e40 CR3: 000000011c7fe003 CR4: 00000000007726f0 [998.393944] PKRU: 55555554 [998.393946] Call Trace: [998.393949] <TASK> [998.393952] ? show_trace_log_lvl+0x1b0/0x2f0 [998.393961] ? show_trace_log_lvl+0x1b0/0x2f0 [998.393975] ? dp_device_event+0x41/0x80 [openvswitch] [998.394009] ? __die_body.cold+0x8/0x12 [998.394016] ? die_addr+0x3c/0x60 [998.394027] ? exc_general_protection+0x16d/0x390 [998.394042] ? asm_exc_general_protection+0x26/0x30 [998.394058] ? dev_set_promiscuity+0x8d/0xa0 [998.394066] ? ovs_netdev_detach_dev+0x3a/0x80 [openvswitch] [998.394092] dp_device_event+0x41/0x80 [openvswitch] [998.394102] notifier_call_chain+0x5a/0xd0 [998.394106] unregister_netdevice_many_notify+0x51b/0xa60 [998.394110] rtnl_dellink+0x169/0x3e0 [998.394121] ? rt_mutex_slowlock.constprop.0+0x95/0xd0 [998.394125] rtnetlink_rcv_msg+0x142/0x3f0 [998.394128] ? avc_has_perm_noaudit+0x69/0xf0 [998.394130] ? __pfx_rtnetlink_rcv_msg+0x10/0x10 [998.394132] netlink_rcv_skb+0x50/0x100 [998.394138] netlink_unicast+0x292/0x3f0 [998.394141] netlink_sendmsg+0x21b/0x470 [998.394145] ____sys_sendmsg+0x39d/0x3d0 [998.394149] ___sys_sendmsg+0x9a/0xe0 [998.394156] __sys_sendmsg+0x7a/0xd0 [998.394160] do_syscall_64+0x7f/0x170 [998.394162] entry_SYSCALL_64_after_hwframe+0x76/0x7e [998.394165] RIP: 0033:0x7fad61bf4724 [998.394188] Code: 89 02 b8 ff ff ff ff eb bb 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 f3 0f 1e fa 80 3d c5 e9 0c 00 00 74 13 b8 2e 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 48 83 ec 28 89 54 24 1c 48 89 [998.394189] RSP: 002b:00007ffd7e2f7cb8 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [998.394191] RAX: ffffffffffffffda RBX: 0000000000000001 RCX: 00007fad61bf4724 [998.394193] RDX: 0000000000000000 RSI: 00007ffd7e2f7d20 RDI: 0000000000000003 [998.394194] RBP: 00007ffd7e2f7d90 R08: 0000000000000010 R09: 000000000000003f [998.394195] R10: 000055df11558010 R11: 0000000000000202 R12: 00007ffd7e2 ---truncated---	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: fix use-after-free in encoder		

CVE-2026-31584	release path The fops_vcodec_release() function frees the context structure (ctx) without first cancelling any pending or running work in ctx->encode_work. This creates a race window where the workqueue handler (mtk_venc_worker) may still be accessing the context memory after it has been freed. Race condition: CPU 0 (release path) CPU 1 (workqueue) ---------- ---------- fops_vcodec_release() v4l2_m2m_ctx_release() v4l2_m2m_cancel_job() // waits for m2m job "done" mtk_venc_worker() v4l2_m2m_job_finish() // m2m job "done" // BUT worker still running! // post-job_finish access: other ctx dereferences // UAF if ctx already freed // returns (job "done") kfree(ctx) // ctx freed Root cause: The v4l2_m2m_ctx_release() only waits for the m2m job lifecycle (via TRANS_RUNNING flag), not the workqueue lifecycle. After v4l2_m2m_job_finish() is called, the m2m framework considers the job complete and v4l2_m2m_ctx_release() returns, but the worker function continues executing and may still access ctx. The work is queued during encode operations via: queue_work(ctx->dev->encode_workqueue, &ctx->encode_work) The worker function accesses ctx->m2m_ctx, ctx->dev, and other ctx fields even after calling v4l2_m2m_job_finish(). This vulnerability was confirmed with KASAN by running an instrumented test module that widens the post-job_finish race window. KASAN detected: BUG: KASAN: slab-use-after-free in mtk_venc_worker+0x159/0x180 Read of size 4 at addr ffff88800326e000 by task kworker/u8:0/12 Workqueue: mtk_vcodec_enc_wq mtk_venc_worker Allocated by task 47: __kasan_kmalloc+0x7f/0x90 fops_vcodec_open+0x85/0x1a0 Freed by task 47: __kasan_slab_free+0x43/0x70 kfree+0xee/0x3a0 fops_vcodec_release+0xb7/0x190 Fix this by calling cancel_work_sync(&ctx->encode_work) before kfree(ctx). This ensures the workqueue handler is both cancelled (if pending) and synchronized (waits for any running handler to complete) before the context is freed. Placement rationale: The fix is placed after v4l2_ctrl_handler_free() and before list_del_init(&ctx->list). At this point, all m2m operations are done (v4l2_m2m_ctx_release() has returned), and we need to ensure the workqueue is synchronized before removing ctx from the list and freeing it. Note: The open error path does NOT need cancel_work_sync() because INIT_WORK() only initializes the work structure - it does not schedule it. Work is only scheduled later during device_run() operations.	7.8	More Details
CVE-2026-31583	In the Linux kernel, the following vulnerability has been resolved: media: em28xx: fix use-after-free in em28xx_v4l2_open() em28xx_v4l2_open() reads dev->v4l2 without holding dev->lock, creating a race with em28xx_v4l2_init()'s error path and em28xx_v4l2_fini(), both of which free the em28xx_v4l2 struct and set dev->v4l2 to NULL under dev->lock. This race leads to two issues: - use-after-free in v4l2_fh_init() when accessing vdev->ctrl_handler, since the video_device is embedded in the freed em28xx_v4l2 struct. - NULL pointer dereference in em28xx_resolution_set() when accessing v4l2->norm, since dev->v4l2 has been set to NULL. Fix this by moving the mutex_lock() before the dev->v4l2 read and adding a NULL check for dev->v4l2 under the lock.	7.8	More Details
CVE-2026-31582	In the Linux kernel, the following vulnerability has been resolved: hwmon: (powerz) Fix use-after-free on USB disconnect After powerz_disconnect() frees the URB and releases the mutex, a subsequent powerz_read() call can acquire the mutex and call powerz_read_data(), which dereferences the freed URB pointer. Fix by: - Setting priv->urb to NULL in powerz_disconnect() so that powerz_read_data() can detect the disconnected state. - Adding a !priv->urb check at the start of powerz_read_data() to return -ENODEV on a disconnected device. - Moving usb_set_intfdata() before hwmon registration so the disconnect handler can always find the priv pointer.	7.8	More Details
CVE-2026-31507	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix double-free of smc_spd_priv when tee() duplicates splice pipe buffer smc_rx_splice() allocates one smc_spd_priv per pipe_buffer and stores the pointer in pipe_buffer.private. The pipe_buf_operations for these buffers used .get = generic_pipe_buf_get, which only increments the page reference count when tee(2) duplicates a pipe buffer. The smc_spd_priv pointer itself was not handled, so after tee() both the original and the cloned pipe_buffer share the same smc_spd_priv *. When both pipes are subsequently released, smc_rx_pipe_buf_release() is called twice against the same object: 1st call: kfree(priv) sock_put(sk) smc_rx_update_cons() [correct] 2nd call: kfree(priv) sock_put(sk) smc_rx_update_cons() [UAF] KASAN reports a slab-use-after-free in smc_rx_pipe_buf_release(), which then escalates to a NULL-pointer dereference and kernel panic via smc_rx_update_consumer() when it chases the freed priv->smc pointer: BUG: KASAN: slab-use-after-free in smc_rx_pipe_buf_release+0x78/0x2a0 Read of size 8 at addr ffff888004a45740 by task smc_splice_tee_/74 Call Trace: <TASK> dump_stack_lvl+0x53/0x70 print_report+0xce/0x650 kasan_report+0xc6/0x100 smc_rx_pipe_buf_release+0x78/0x2a0 free_pipe_info+0xd4/0x130 pipe_release+0x142/0x160 __fput+0x1c6/0x490 __x64_sys_close+0x4f/0x90 do_syscall_64+0xa6/0x1a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> BUG: kernel NULL pointer dereference, address: 0000000000000020 RIP: 0010:smc_rx_update_consumer+0x8d/0x350 Call Trace: <TASK> smc_rx_pipe_buf_release+0x121/0x2a0 free_pipe_info+0xd4/0x130 pipe_release+0x142/0x160 __fput+0x1c6/0x490 __x64_sys_close+0x4f/0x90 do_syscall_64+0xa6/0x1a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Kernel panic - not syncing: Fatal exception Beyond the memory-safety problem, duplicating an SMC splice buffer is semantically questionable: smc_rx_update_cons() would advance the consumer cursor twice for the same data, corrupting receive-window accounting. A refcount on smc_spd_priv could fix the double-free, but the cursor-accounting issue would still need to be addressed separately. The .get callback is invoked by both tee(2) and splice_pipe_to_pipe() for partial transfers; both will now return -EFAULT. Users who need to duplicate SMC socket data must use a copy-based read path.	7.8	More Details
CVE-2026-31525	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix undefined behavior in interpreter sdiv/smod for INT_MIN The BPF interpreter's signed 32-bit division and modulo handlers use the kernel abs() macro on s32 operands. The abs() macro documentation (include/linux/math.h) explicitly states the result is undefined when the input is the type minimum. When DST contains S32_MIN (0x80000000), abs((s32)DST) triggers undefined behavior and returns S32_MIN unchanged on arm64/x86. This value is then sign-extended to u64 as 0xFFFFFFFF80000000, causing do_div() to compute the wrong result. The verifier's abstract interpretation (scalar32_min_max_sdiv) computes the mathematically correct result for range tracking, creating a verifier/interpreter mismatch that can be exploited for out-of-bounds map value access. Introduce abs_s32() which handles S32_MIN correctly by casting to u32 before negating, avoiding signed overflow entirely. Replace all 8 abs((s32)...) call sites in the interpreter's sdiv32/smod32 handlers. s32 is the only affected case -- the s64 division/modulo handlers do not use abs().	7.8	More Details
CVE-2026-31581	In the Linux kernel, the following vulnerability has been resolved: ALSA: 6fire: fix use-after-free on disconnect In usb6fire_chip_abort(), the chip struct is allocated as the card's private data (via snd_card_new with sizeof(struct sfire_chip)). When snd_card_free_when_closed() is called and no file handles are open, the card and embedded chip are freed synchronously. The subsequent chip->card = NULL write then hits freed slab memory. Call trace: usb6fire_chip_abort sound/usb/6fire/chip.c:59 [inline] usb6fire_chip_disconnect+0x348/0x358 sound/usb/6fire/chip.c:182 usb_unbind_interface+0x1a8/0x88c drivers/usb/core/driver.c:458 ... hub_event+0x1a04/0x4518 drivers/usb/core/hub.c:5953 Fix by moving the card lifecycle out of usb6fire_chip_abort() and into	7.8	More Details

	usb6fire_chip_disconnect(). The card pointer is saved in a local before any teardown, snd_card_disconnect() is called first to prevent new opens, URBs are aborted while chip is still valid, and snd_card_free_when_closed() is called last so chip is never accessed after the card may be freed.		
CVE-2026-31665	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_ct: fix use-after-free in timeout object destroy nft_ct_timeout_obj_destroy() frees the timeout object with kfree() immediately after nf_ct_untimeout(), without waiting for an RCU grace period. Concurrent packet processing on other CPUs may still hold RCU-protected references to the timeout object obtained via rcu_dereference() in nf_ct_timeout_data(). Add an rcu_head to struct nf_ct_timeout and use kfree_rcu() to defer freeing until after an RCU grace period, matching the approach already used in nfnetlink_cttimeout.c. KASAN report: BUG: KASAN: slab-use-after-free in nf_conntrack_tcp_packet+0x1381/0x29d0 Read of size 4 at addr ffff8881035fe19c by task exploit/80 Call Trace: nf_conntrack_tcp_packet+0x1381/0x29d0 nf_conntrack_in+0x612/0x8b0 nf_hook_slow+0x70/0x100 __ip_local_out+0x1b2/0x210 tcp_sendmsg_locked+0x722/0x1580 __sys_sendto+0x2d8/0x320 Allocated by task 75: nft_ct_timeout_obj_init+0xf6/0x290 nft_obj_init+0x107/0x1b0 nf_tables_newobj+0x680/0x9c0 nfnetlink_rcv_batch+0xc29/0xe00 Freed by task 26: nft_obj_destroy+0x3f/0xa0 nf_tables_trans_destroy_work+0x51c/0x5c0 process_one_work+0x2c4/0x5a0	7.8	More Details
CVE-2026-31527	In the Linux kernel, the following vulnerability has been resolved: driver core: platform: use generic driver_override infrastructure When a driver is probed through __driver_attach(), the bus' match() callback is called without the device lock held, thus accessing the driver_override field without a lock, which can cause a UAF. Fix this by using the driver-core driver_override infrastructure taking care of proper locking internally. Note that calling match() from __driver_attach() without the device lock held is intentional. [1]	7.8	More Details
CVE-2026-31528	In the Linux kernel, the following vulnerability has been resolved: perf: Make sure to use pmu_ctx->pmu for groups Oliver reported that x86_pmu_del() ended up doing an out-of-bound memory access when group_sched_in() fails and needs to roll back. This *should* be handled by the transaction callbacks, but he found that when the group leader is a software event, the transaction handlers of the wrong PMU are used. Despite the move_group case in perf_event_open() and group_sched_in() using pmu_ctx->pmu. Turns out, inherit uses event->pmu to clone the events, effectively undoing the move_group case for all inherited contexts. Fix this by also making inherit use pmu_ctx->pmu, ensuring all inherited counters end up in the same pmu context. Similarly, __perf_event_read() should use equally use pmu_ctx->pmu for the group case.	7.8	More Details
CVE-2026-5940	Calling a function that triggers a UI refresh after removing comments via a script may access an invalidated object, leading to program crashes.	7.8	More Details
CVE-2026-5941	Parsing logic flaws cause non-signature data to be misidentified as valid signatures when processing malformed form field hierarchies, leading to invalid memory writes and program crashes during internal data structure construction.	7.8	More Details
CVE-2026-31641	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix RxGK token loading to check bounds rxrpc_preparse_xdr_yfs_rxgk() reads the raw key length and ticket length from the XDR token as u32 values and passes each through round_up(x, 4) before using the rounded value for validation and allocation. When the raw length is >= 0xfffffffd, round_up() wraps to 0, so the bounds check and kzalloc both use 0 while the subsequent memcpy still copies the original ~4 GiB value, producing a heap buffer overflow reachable from an unprivileged add_key() call. Fix this by: (1) Rejecting raw key lengths above AFSTOKEN_GK_KEY_MAX and raw ticket lengths above AFSTOKEN_GK_TOKEN_MAX before rounding, consistent with the caps that the RxKAD path already enforces via AFSTOKEN_RK_TIX_MAX. (2) Sizing the flexible-array allocation from the validated raw key length via struct_size_t() instead of the rounded value. (3) Caching the raw lengths so that the later field assignments and memcpy calls do not re-read from the token, eliminating a class of TOCTOU re-parse. The control path (valid token with lengths within bounds) is unaffected.	7.8	More Details
CVE-2026-31431	In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. There is no benefit in operating in-place in algif_aead since the source and destination come from different mappings. Get rid of all the complexity added for in-place operation and just copy the AD directly.	7.8	More Details
CVE-2026-31566	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix fence put before wait in amdgpu_amdkfd_submit_ib amdgpu_amdkfd_submit_ib() submits a GPU job and gets a fence from amdgpu_ib_schedule(). This fence is used to wait for job completion. Currently, the code drops the fence reference using dma_fence_put() before calling dma_fence_wait(). If dma_fence_put() releases the last reference, the fence may be freed before dma_fence_wait() is called. This can lead to a use-after-free. Fix this by waiting on the fence first and releasing the reference only after dma_fence_wait() completes. Fixes the below: drivers/gpu/drm/amd/amdgpu/amdgpu_amdkfd.c:697 amdgpu_amdkfd_submit_ib() warn: passing freed memory 'f' (line 696) (cherry picked from commit 8b9e5259adc385b61a6590a13b82ae0ac2bd3482)	7.8	More Details
CVE-2026-5943	Document structural anomalies caused inconsistencies between page element relationships and internal index states. When scripts triggered document modifications, object reference validity was not properly maintained, leading to a crash when accessing an invalid pointer during page information queries.	7.8	More Details
CVE-2026-31663	In the Linux kernel, the following vulnerability has been resolved: xfrm: hold dev ref until after transport_finish NF_HOOK After async crypto completes, xfrm_input_resume() calls dev_put() immediately on re-entry before the skb reaches transport_finish. The skb->dev pointer is then used inside NF_HOOK and its okfn, which can race with device teardown. Remove the dev_put from the async resumption entry and instead drop the reference after the NF_HOOK call in transport_finish, using a saved device pointer since NF_HOOK may consume the skb. This covers NF_DROP, NF_QUEUE and NF_STOLEN paths that skip the okfn. For non-transport exits (decaps, gro, drop) and secondary async return points, release the reference inline when async is set.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: iavf: fix out-of-bounds writes in iavf_get_ethtool_stats() iavf incorrectly uses real_num_tx_queues for ETH_SS_STATS. Since the value could change in runtime, we should use		

CVE-2026-31505	num_tx_queues instead. Moreover iavf_get_ethtool_stats() uses num_active_queues while iavf_get_sset_count() and iavf_get_stat_strings() use real_num_tx_queues, which triggers out-of-bounds writes when we do "ethtool -L" and "ethtool -S" simultaneously [1]. For example when we change channels from 1 to 8, Thread 3 could be scheduled before Thread 2, and out-of-bounds writes could be triggered in Thread 3: Thread 1 (ethtool -L) Thread 2 (work) Thread 3 (ethtool -S) iavf_set_channels() ... iavf_alloc_queues() -> num_active_queues = 8 iavf_schedule_finish_config() iavf_get_sset_count() real_num_tx_queues: 1 -> buffer for 1 queue iavf_get_ethtool_stats() num_active_queues: 8 -> out-of-bounds! iavf_finish_config() -> real_num_tx_queues = 8 Use immutable num_tx_queues in all related functions to avoid the issue. [1] BUG: KASAN: vmalloc-out-of-bounds in iavf_add_one_ethtool_stat+0x200/0x270 Write of size 8 at addr ffffc900031c9080 by task ethtool/5800 CPU: 1 UID: 0 PID: 5800 Comm: ethtool Not tainted 6.19.0-enjuk-08403-g8137e3db7f1c #241 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x6f/0xb0 print_report+0x170/0x4f3 kasan_report+0xe1/0x180 iavf_add_one_ethtool_stat+0x200/0x270 iavf_get_ethtool_stats+0x14c/0x2e0 __dev_ethtool+0x3d0c/0x5830 dev_ethtool+0x12d/0x270 dev_ioctl+0x53c/0xe30 sock_do_ioctl+0x1a9/0x270 sock_ioctl+0x3d4/0x5e0 __x64_sys_ioctl+0x137/0x1c0 do_syscall_64+0xf3/0x690 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f7da0e6e36d ... </TASK> The buggy address belongs to a 1-page vmalloc region starting at 0xffffc900031c9000 allocated at __dev_ethtool+0x3cc9/0x5830 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:0000000000000000 index:0xffff88813a013de0 pfn:0x13a013 flags: 0x200000000000000(node=0|zone=2) raw: 0200000000000000 0000000000000000 dead000000000122 0000000000000000 raw: ffff88813a013de0 0000000000000000 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffffc900031c8f80: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc900031c9000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >ffffc900031c9080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ ffffc900031c9100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc900031c9180: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8	7.8	More Details
CVE-2026-31644	In the Linux kernel, the following vulnerability has been resolved: net: lan966x: fix use-after-free and leak in lan966x_fdma_reload() When lan966x_fdma_reload() fails to allocate new RX buffers, the restore path restarts DMA using old descriptors whose pages were already freed via lan966x_fdma_rx_free_pages(). Since page_pool_put_full_page() can release pages back to the buddy allocator, the hardware may DMA into memory now owned by other kernel subsystems. Additionally, on the restore path, the newly created page pool (if allocation partially succeeded) is overwritten without being destroyed, leaking it. Fix both issues by deferring the release of old pages until after the new allocation succeeds. Save the old page array before the allocation so old pages can be freed on the success path. On the failure path, the old descriptors, pages and page pool are all still valid, making the restore safe. Also ensure the restore path re-enables NAPI and wakes the netdev, matching the success path.	7.8	More Details
CVE-2026-31648	In the Linux kernel, the following vulnerability has been resolved: mm: filemap: fix nr_pages calculation overflow in filemap_map_pages() When running stress-ng on my Arm64 machine with v7.0-rc3 kernel, I encountered some very strange crash issues showing up as "Bad page state": " [734.496287] BUG: Bad page state in process stress-ng-env pfn:415735fb [734.496427] page: refcount:0 mapcount:1 mapping:0000000000000000 index:0x4cf316 pfn:0x415735fb [734.496434] flags: 0x57fffe000000800(owner_2|node=1|zone=2|lastcpupid=0x3ffff) [734.496439] raw: 057fffe000000800 0000000000000000 dead000000000122 0000000000000000 [734.496440] raw: 00000000004cf316 0000000000000000 0000000000000000 0000000000000000 [734.496442] page dumped because: nonzero mapcount " After analyzing this page's state, it is hard to understand why the mapcount is not 0 while the refcount is 0, since this page is not where the issue first occurred. By enabling the CONFIG_DEBUG_VM config, I can reproduce the crash as well and captured the first warning where the issue appears: " [734.469226] page: refcount:33 mapcount:0 mapping:00000000bef2d187 index:0x81a0 pfn:0x415735c0 [734.469304] head: order:5 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0 [734.469315] memcg:ffff000807a8ec00 [734.469320] aops:ext4_da_aops ino:100b6f dentry name(?):"stress-ng-mmaptorture-9397-0-2736200540" [734.469335] flags: 0x57fffe400000069(locked|uptodate|lru|head|node=1|zone=2|lastcpupid=0x3ffff) ..... [734.469364] page dumped because: VM_WARN_ON_FOLIO((_Generic((page + nr_pages - 1), const struct page *: (const struct folio *)_compound_head(page + nr_pages - 1), struct page *: (struct folio *)_compound_head(page + nr_pages - 1))) != folio) [734.469390] ------------[cut here]------------ [734.469393] WARNING: ./include/linux/rmap.h:351 at folio_add_file_rmap_ptes+0x3b8/0x468, CPU#90: stress-ng-mlock/9430 [734.469551] folio_add_file_rmap_ptes+0x3b8/0x468 (P) [734.469555] set_pte_range+0xd8/0x2f8 [734.469566] filemap_map_folio_range+0x190/0x400 [734.469579] filemap_map_pages+0x348/0x638 [734.469583] do_fault_around+0x140/0x198 ..... [734.469640] el0t_64_sync+0x184/0x188 " The code that triggers the warning is: "VM_WARN_ON_FOLIO(page_folio(page + nr_pages - 1) != folio, folio)", which indicates that set_pte_range() tried to map beyond the large folio's size. By adding more debug information, I found that 'nr_pages' had overflowed in filemap_map_pages(), causing set_pte_range() to establish mappings for a range exceeding the folio size, potentially corrupting fields of pages that do not belong to this folio (e.g., page->_mapcount). After above analysis, I think the possible race is as follows: CPU 0 CPU 1 filemap_map_pages() ext4_setattr() //get and lock folio with old inode->i_size next_uptodate_folio() ..... //shrink the inode->i_size i_size_write(inode, attr->ia_size); //calculate the end_pgoff with the new inode->i_size file_end = DIV_ROUND_UP(i_size_read(mapping->host), PAGE_SIZE) - 1; end_pgoff = min(end_pgoff, file_end); ..... //nr_pages can be overflowed, cause xas.xa_index > end_pgoff end = folio_next_index(folio) - 1; nr_pages = min(end, end_pgoff) - xas.xa_index + 1; ..... //map large folio filemap_map_folio_range() ..... //truncate folios truncate_pagecache(inode, inode->i_size); To fix this issue, move the 'end_pgoff' calculation before next_uptodate_folio(), so the retrieved folio stays consistent with the file end to avoid ---truncated---	7.8	More Details
CVE-2026-31666	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix incorrect return value after changing leaf in lookup_extent_data_ref() After commit 1618aa3c2e01 ("btrfs: simplify return variables in lookup_extent_data_ref()"), the err and ret variables were merged into a single ret variable. However, when btrfs_next_leaf() returns 0 (success), ret is overwritten from -ENOENT to 0. If the first key in the next leaf does not match (different objectid or type), the function returns 0 instead of -ENOENT, making the caller believe the lookup succeeded when it did not. This can lead to operations on the wrong extent tree item, potentially causing extent tree corruption. Fix this by returning -ENOENT directly when the key does not match, instead of relying on the ret variable.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: rxrpc: proc: size address buffers for %pISpc output The AF_RXRPC procfs helpers format local and remote socket addresses into fixed 50-byte stack buffers with "%pISpc". That is too small for the longest current-tree IPv6-with-port form the formatter can produce. In lib/vsprintf.c, the compressed IPv6 path uses a dotted-quad tail not only for v4mapped addresses, but also for ISATAP addresses via ipv6_addr_is_isatap(). As a		

CVE-2026-31630	result, a case such as [ffff:ffff:ffff:ffff:0:5efe:255.255.255.255]:65535 is possible with the current formatter. That is 50 visible characters, so 51 bytes including the trailing NUL, which does not fit in the existing char[50] buffers used by net/rxrpc/proc.c. Size the buffers from the formatter's maximum textual form and switch the call sites to scnprintf(). Changes since v1: - correct the changelog to cite the actual maximum current-tree case explicitly - frame the proof around the ISATAP formatting path instead of the earlier mapped-v4 example	7.8	More Details
CVE-2026-41336	OpenClaw before 2026.3.31 allows workspace .env files to override the OPENCLAW_BUNDLED_HOOKS_DIR environment variable, enabling loading of attacker-controlled hook code. Attackers can replace trusted default-on bundled hooks from untrusted workspaces to execute arbitrary code.	7.8	More Details
CVE-2026-31576	In the Linux kernel, the following vulnerability has been resolved: media: hackrf: fix to not free memory after the device is registered in hackrf_probe() In hackrf driver, the following race condition occurs: ``` CPU0 CPU1 hackrf_probe() kzalloc(); // alloc hackrf_dev .... v4l2_device_register(); .... fd = sys_open("/path/to/dev"); // open hackrf fd .... v4l2_device_unregister(); .... kfree(); // free hackrf_dev .... sys_ioctl(fd, ...); v4l2_ioctl(); video_is_registered() // UAF!! .... sys_close(fd); v4l2_release() // UAF!! hackrf_video_release() kfree(); // DFB!! ``` When a V4L2 or video device is unregistered, the device node is removed so new open() calls are blocked. However, file descriptors that are already open-and any in-flight I/O-do not terminate immediately; they remain valid until the last reference is dropped and the driver's release() is invoked. Therefore, freeing device memory on the error path after hackrf_probe() has registered dev it will lead to a race to use-after-free vuln, since those already-open handles haven't been released yet. And since release() free memory too, race to use-after-free and double-free vuln occur. To prevent this, if device is registered from probe(), it should be modified to free memory only through release() rather than calling kfree() directly.	7.8	More Details
CVE-2026-31554	In the Linux kernel, the following vulnerability has been resolved: futex: Require sys_futex_requeue() to have identical flags Nicholas reported that his LLM found it was possible to create a UaF when sys_futex_requeue() is used with different flags. The initial motivation for allowing different flags was the variable sized futex, but since that hasn't been merged (yet), simply mandate the flags are identical, as is the case for the old style sys_futex() requeue operations.	7.8	More Details
CVE-2026-31530	In the Linux kernel, the following vulnerability has been resolved: cxl/port: Fix use after free of parent_port in cxl_detach_ep() cxl_detach_ep() is called during bottom-up removal when all CXL memory devices beneath a switch port have been removed. For each port in the hierarchy it locks both the port and its parent, removes the endpoint, and if the port is now empty, marks it dead and unregisters the port by calling delete_switch_port(). There are two places during this work where the parent_port may be used after freeing: First, a concurrent detach may have already processed a port by the time a second worker finds it via bus_find_device(). Without pinning parent_port, it may already be freed when we discover port->dead and attempt to unlock the parent_port. In a production kernel that's a silent memory corruption, with lock debug, it looks like this: []DEBUG_LOCKS_WARN_ON(__owner_task(owner) != get_current()) []WARNING: kernel/locking/mutex.c:949 at __mutex_unlock_slowpath+0x1ee/0x310 []Call Trace: []mutex_unlock+0xd/0x20 []cxl_detach_ep+0x180/0x400 [cxl_core] []devm_action_release+0x10/0x20 []devres_release_all+0xa8/0xe0 []device_unbind_cleanup+0xd/0xa0 []really_probe+0x1a6/0x3e0 Second, delete_switch_port() releases three devm actions registered against parent_port. The last of those is unregister_port() and it calls device_unregister() on the child port, which can cascade. If parent_port is now also empty the device core may unregister and free it too. So by the time delete_switch_port() returns, parent_port may be free, and the subsequent device_unlock(&parent_port->dev) operates on freed memory. The kernel log looks same as above, with a different offset in cxl_detach_ep(). Both of these issues stem from the absence of a lifetime guarantee between a child port and its parent port. Establish a lifetime rule for ports: child ports hold a reference to their parent device until release. Take the reference when the port is allocated and drop it when released. This ensures the parent is valid for the full lifetime of the child and eliminates the use after free window in cxl_detach_ep(). This is easily reproduced with a reload of cxl_acpi in QEMU with CXL devices present.	7.8	More Details
CVE-2026-31548	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: cancel pmsr_free_wk in cfg80211_pmsr_wdev_down When the nl80211 socket that originated a PMSR request is closed, cfg80211_release_pmsr() sets the request's nl_portid to zero and schedules pmsr_free_wk to process the abort asynchronously. If the interface is concurrently torn down before that work runs, cfg80211_pmsr_wdev_down() calls cfg80211_pmsr_process_abort() directly. However, the already- scheduled pmsr_free_wk work item remains pending and may run after the interface has been removed from the driver. This could cause the driver's abort_pmsr callback to operate on a torn-down interface, leading to undefined behavior and potential crashes. Cancel pmsr_free_wk synchronously in cfg80211_pmsr_wdev_down() before calling cfg80211_pmsr_process_abort(). This ensures any pending or in-progress work is drained before interface teardown proceeds, preventing the work from invoking the driver abort callback after the interface is gone.	7.8	More Details
CVE-2026-31667	In the Linux kernel, the following vulnerability has been resolved: Input: uinput - fix circular locking dependency with ff-core A lockdep circular locking dependency warning can be triggered reproducibly when using a force-feedback gamepad with uinput (for example, playing ELDEN RING under Wine with a Flydigi Vader 5 controller): ff->mutex -> udev->mutex -> input_mutex -> dev->mutex -> ff->mutex The cycle is caused by four lock acquisition paths: 1. ff upload: input_ff_upload() holds ff->mutex and calls uinput_dev_upload_effect() -> uinput_request_submit() -> uinput_request_send(), which acquires udev->mutex. 2. device create: uinput_ioctl_handler() holds udev->mutex and calls uinput_create_device() -> input_register_device(), which acquires input_mutex. 3. device register: input_register_device() holds input_mutex and calls kbd_connect() -> input_register_handle(), which acquires dev->mutex. 4. evdev release: evdev_release() calls input_flush_device() under dev->mutex, which calls input_ff_flush() acquiring ff->mutex. Fix this by introducing a new state_lock spinlock to protect udev->state and udev->dev access in uinput_request_send() instead of acquiring udev->mutex. The function only needs to atomically check device state and queue an input event into the ring buffer via uinput_dev_event() -- both operations are safe under a spinlock (ktime_get_ts64() and wake_up_interruptible() do not sleep). This breaks the ff->mutex -> udev->mutex link since a spinlock is a leaf in the lock ordering and cannot form cycles with mutexes. To keep state transitions visible to uinput_request_send(), protect writes to udev->state in uinput_create_device() and uinput_destroy_device() with the same state_lock spinlock. Additionally, move init_completion(&request->done) from uinput_request_send() to uinput_request_submit() before uinput_request_reserve_slot(). Once the slot is allocated, uinput_flush_requests() may call complete() on it at any time from the destroy path, so the completion must be initialised before the request becomes visible. Lock ordering after the fix: ff->mutex -> state_lock (spinlock, leaf) udev->mutex -> state_lock (spinlock, leaf) udev->mutex -> input_mutex -> dev->mutex -> ff->mutex (no back-edge)	7.8	More Details

CVE-2026-31490	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pf: Fix use-after-free in migration restore When an error is returned from xe_sriov_pf_migration_restore_produce(), the data pointer is not set to NULL, which can trigger use-after-free in subsequent .write() calls. Set the pointer to NULL upon error to fix the problem. (cherry picked from commit 4f53d8c6d23527d734fe3531d08e15cb170a0819)	7.8	More Details
CVE-2026-31504	In the Linux kernel, the following vulnerability has been resolved: net: fix fanout UAF in packet_release() via NETDEV_UP race `packet_release()` has a race window where `NETDEV_UP` can re-register a socket into a fanout group's `arr[]` array. The re-registration is not cleaned up by `fanout_release()`, leaving a dangling pointer in the fanout array. `packet_release()` does NOT zero `po->num` in its `bind_lock` section. After releasing `bind_lock`, `po->num` is still non-zero and `po->ifindex` still matches the bound device. A concurrent `packet_notifier(NETDEV_UP)` that already found the socket in `sklist` can re-register the hook. For fanout sockets, this re-registration calls `__fanout_link(sk, po)` which adds the socket back into `f->arr[]` and increments `f->num_members`, but does NOT increment `f->sk_ref`. The fix sets `po->num` to zero in `packet_release` while `bind_lock` is held to prevent NETDEV_UP from linking, preventing the race window. This bug was found following an additional audit with Claude Code based on CVE-2025-38617.	7.8	More Details
CVE-2026-31454	In the Linux kernel, the following vulnerability has been resolved: xfs: save ailp before dropping the AIL lock in push callbacks In xfs_inode_item_push() and xfs_qm_dquot_logitem_push(), the AIL lock is dropped to perform buffer IO. Once the cluster buffer no longer protects the log item from reclaim, the log item may be freed by background reclaim or the dquot shrinker. The subsequent spin_lock() call dereferences lip->li_ailp, which is a use-after-free. Fix this by saving the ailp pointer in a local variable while the AIL lock is held and the log item is guaranteed to be valid.	7.8	More Details
CVE-2026-31475	In the Linux kernel, the following vulnerability has been resolved: ASoC: sma1307: fix double free of devm_kzalloc() memory A previous change added NULL checks and cleanup for allocation failures in sma1307_setting_loaded(). However, the cleanup for mode_set entries is wrong. Those entries are allocated with devm_kzalloc(), so they are device-managed resources and must not be freed with kfree(). Manually freeing them in the error path can lead to a double free when devres later releases the same memory. Drop the manual kfree() loop and let devres handle the cleanup.	7.8	More Details
CVE-2026-31474	In the Linux kernel, the following vulnerability has been resolved: can: isotp: fix tx.buf use-after-free in isotp_sendmsg() isotp_sendmsg() uses only cmpxchg() on so->tx.state to serialize access to so->tx.buf. isotp_release() waits for ISOTP_IDLE via wait_event_interruptible() and then calls kfree(so->tx.buf). If a signal interrupts the wait_event_interruptible() inside close() while tx.state is ISOTP_SENDING, the loop exits early and release proceeds to force ISOTP_SHUTDOWN and continues to kfree(so->tx.buf) while sendmsg may still be reading so->tx.buf for the final CAN frame in isotp_fill_dataframe(). The so->tx.buf can be allocated once when the standard tx.buf length needs to be extended. Move the kfree() of this potentially extended tx.buf to sk_destruct time when either isotp_sendmsg() and isotp_release() are done.	7.8	More Details
CVE-2026-31473	In the Linux kernel, the following vulnerability has been resolved: media: mc, v4l2: serialize REINIT and REQBUFS with req_queue_mutex MEDIA_REQUEST_IOC_REINIT can run concurrently with VIDIOC_REQBUFS(0) queue teardown paths. This can race request object cleanup against vb2 queue cancellation and lead to use-after-free reports. We already serialize request queueing against STREAMON/OFF with req_queue_mutex. Extend that serialization to REQBUFS, and also take the same mutex in media_request_ioctl_reinit() so REINIT is in the same exclusion domain. This keeps request cleanup and queue cancellation from running in parallel for request-capable devices.	7.8	More Details
CVE-2026-31532	In the Linux kernel, the following vulnerability has been resolved: can: raw: fix ro->uniq use-after-free in raw_rcv() raw_release() unregisters raw CAN receive filters via can_rx_unregister(), but receiver deletion is deferred with call_rcu(). This leaves a window where raw_rcv() may still be running in an RCU read-side critical section after raw_release() frees ro->uniq, leading to a use-after-free of the percpu uniq storage. Move free_percpu(ro->uniq) out of raw_release() and into a raw-specific socket destructor. can_rx_unregister() takes an extra reference to the socket and only drops it from the RCU callback, so freeing uniq from sk_destruct ensures the percpu area is not released until the relevant callbacks have drained. [mkl: applied manually]	7.8	More Details
CVE-2026-31471	In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: only publish mode_data after clone setup iptfs_clone_state() stores x->mode_data before allocating the reorder window. If that allocation fails, the code frees the cloned state and returns -ENOMEM, leaving x->mode_data pointing at freed memory. The xfrm clone unwind later runs destroy_state() through x->mode_data, so the failed clone path tears down IPTFS state that clone_state() already freed. Keep the cloned IPTFS state private until all allocations succeed so failed clones leave x->mode_data unset. The destroy path already handles a NULL mode_data pointer.	7.8	More Details
CVE-2026-31469	In the Linux kernel, the following vulnerability has been resolved: virtio_net: Fix UAF on dst_ops when IFF_XMIT_DST_RELEASE is cleared and napi_tx is false A UAF issue occurs when the virtio_net driver is configured with napi_tx=N and the device's IFF_XMIT_DST_RELEASE flag is cleared (e.g., during the configuration of tc route filter rules). When IFF_XMIT_DST_RELEASE is removed from the net_device, the network stack expects the driver to hold the reference to skb->dst until the packet is fully transmitted and freed. In virtio_net with napi_tx=N, skbs may remain in the virtio transmit ring for an extended period. If the network namespace is destroyed while these skbs are still pending, the corresponding dst_ops structure has freed. When a subsequent packet is transmitted, free_old_xmit() is triggered to clean up old skbs. It then calls dst_release() on the skb associated with the stale dst_entry. Since the dst_ops (referenced by the dst_entry) has already been freed, a UAF kernel paging request occurs. fix it by adds skb_dst_drop(skb) in start_xmit to explicitly release the dst reference before the skb is queued in virtio_net. Call Trace: Unable to handle kernel paging request at virtual address ffff80007e150000 CPU: 2 UID: 0 PID: 6236 Comm: ping Kdump: loaded Not tainted 7.0.0-rc1+ #6 PREEMPT ... percpu_counter_add_batch+0x3c/0x158 lib/percpu_counter.c:98 (P) dst_release+0xe0/0x110 net/core/dst.c:177 skb_release_head_state+0xe8/0x108 net/core/skbuff.c:1177 sk_skb_reason_drop+0x54/0x2d8 net/core/skbuff.c:1255 dev_kfree_skb_any_reason+0x64/0x78 net/core/dev.c:3469 napi_consume_skb+0x1c4/0x3a0 net/core/skbuff.c:1527 __free_old_xmit+0x164/0x230 drivers/net/virtio_net.c:611 [virtio_net] free_old_xmit drivers/net/virtio_net.c:1081 [virtio_net] start_xmit+0x7c/0x530 drivers/net/virtio_net.c:3329 [virtio_net] ... Reproduction Steps: NETDEV="enp3s0" config_qdisc_route_filter() { tc qdisc del dev $NETDEV root tc qdisc add dev $NETDEV root handle 1: prio tc filter add dev $NETDEV parent 1:0 \ protocol ip prio 100 route to 100 flowid 1:1 ip route add 192.168.1.100/32 dev $NETDEV realm 100 } test_ns() { ip netns add testns ip link set $NETDEV netns testns ip netns exec testns ifconfig $NETDEV 10.0.32.46/24 ip netns exec testns ping -c 1 10.0.32.1 ip netns del testns } config_qdisc_route_filter test_ns sleep 2 test_ns	7.8	More Details

CVE-2026-31468	In the Linux kernel, the following vulnerability has been resolved: vfio/pci: Fix double free in dma-buf feature The error path through vfio_pci_core_feature_dma_buf() ignores its own advice to only use dma_buf_put() after dma_buf_export(), instead falling through the entire unwind chain. In the unlikely event that we encounter file descriptor exhaustion, this can result in an unbalanced refcount on the vfio device and double free of allocated objects. Avoid this by moving the "put" directly into the error path and return the errno rather than entering the unwind chain.	7.8	More Details
CVE-2026-7279	AVACAST developed by eMPIA Technology, has a DLL Hijacking vulnerability, allowing authenticated local attackers to place a malicious DLL in a specific directory, resulting in arbitrary code execution with system privileges when the system loads the DLL.	7.8	More Details
CVE-2026-31597	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix use-after-free in ocfs2_fault() when VM_FAULT_RETRY filemap_fault() may drop the mmap_lock before returning VM_FAULT_RETRY, as documented in mm/filemap.c: "If our return value has VM_FAULT_RETRY set, it's because the mmap_lock may be dropped before doing I/O or by lock_folio_maybe_drop_mmap()." When this happens, a concurrent munmap() can call remove_vma() and free the vm_area_struct via RCU. The saved 'vma' pointer in ocfs2_fault() then becomes a dangling pointer, and the subsequent trace_ocfs2_fault() call dereferences it -- a use-after-free. Fix this by saving ip_blkno as a plain integer before calling filemap_fault(), and removing vma from the trace event. Since ip_blkno is copied by value before the lock can be dropped, it remains valid regardless of what happens to the vma or inode afterward.	7.8	More Details
CVE-2026-31453	In the Linux kernel, the following vulnerability has been resolved: xfs: avoid dereferencing log items after push callbacks After xfsaild_push_item() calls iop_push(), the log item may have been freed if the AIL lock was dropped during the push. Background inode reclaim or the dquot shrinker can free the log item while the AIL lock is not held, and the tracepoints in the switch statement dereference the log item after iop_push() returns. Fix this by capturing the log item type, flags, and LSN before calling xfsaild_push_item(), and introducing a new xfs_ail_push_class trace event class that takes these pre-captured values and the ailp pointer instead of the log item pointer.	7.8	More Details
CVE-2026-35368	A vulnerability exists in the chroot utility of uutils coreutils when using the --userspec option. The utility resolves the user specification via getpwnam() after entering the chroot but before dropping root privileges. On glibc-based systems, this can trigger the Name Service Switch (NSS) to load shared libraries (e.g., libnss_*.so.2) from the new root directory. If the NEWROOT is writable by an attacker, they can inject a malicious NSS module to execute arbitrary code as root, facilitating a full container escape or privilege escalation.	7.8	More Details
CVE-2026-31449	In the Linux kernel, the following vulnerability has been resolved: ext4: validate p_idx bounds in ext4_ext_correct_indexes ext4_ext_correct_indexes() walks up the extent tree correcting index entries when the first extent in a leaf is modified. Before accessing path[k].p_idx->ei_block, there is no validation that p_idx falls within the valid range of index entries for that level. If the on-disk extent header contains a corrupted or crafted eh_entries value, p_idx can point past the end of the allocated buffer, causing a slab-out-of-bounds read. Fix this by validating path[k].p_idx against EXT_LAST_INDEX() at both access sites: before the while loop and inside it. Return -EFSCORRUPTED if the index pointer is out of range, consistent with how other bounds violations are handled in the ext4 extent tree code.	7.8	More Details
CVE-2026-31447	In the Linux kernel, the following vulnerability has been resolved: ext4: reject mount if bigalloc with s_first_data_block != 0 bigalloc with s_first_data_block != 0 is not supported, reject mounting it.	7.8	More Details
CVE-2026-31446	In the Linux kernel, the following vulnerability has been resolved: ext4: fix use-after-free in update_super_work when racing with umount Commit b98535d09179 ("ext4: fix bug_on in start_this_handle during umount filesystem") moved ext4_unregister_sysfs() before flushing s_sb_upd_work to prevent new error work from being queued via /proc/fs/ext4/xx/mb_groups reads during unmount. However, this introduced a use-after-free because update_super_work calls ext4_notify_error_sysfs() -> sysfs_notify() which accesses the kobject's kernfs_node after it has been freed by kobject_del() in ext4_unregister_sysfs(): update_super_work ext4_put_super ---------- ---------- ext4_unregister_sysfs(sb) kobject_del(&sbi->s_kobj) __kobject_del() sysfs_remove_dir() kobj->sd = NULL sysfs_put(sd) kernfs_put() // RCU free ext4_notify_error_sysfs(sbi) sysfs_notify(&sbi->s_kobj) kn = kobj->sd // stale pointer kernfs_get(kn) // UAF on freed kernfs_node ext4_journal_destroy() flush_work(&sbi->s_sb_upd_work) Instead of reordering the teardown sequence, fix this by making ext4_notify_error_sysfs() detect that sysfs has already been torn down by checking s_kobj.state_in_sysfs, and skipping the sysfs_notify() call in that case. A dedicated mutex (s_error_notify_mutex) serializes ext4_notify_error_sysfs() against kobject_del() in ext4_unregister_sysfs() to prevent TOCTOU races where the kobject could be deleted between the state_in_sysfs check and the sysfs_notify() call.	7.8	More Details
CVE-2026-31442	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix possible invalid memory access after FLR In the case that the first Function Level Reset (FLR) concludes correctly, but in the second FLR the scratch area for the saved configuration cannot be allocated, it's possible for a invalid memory access to happen. Always set the deallocated scratch area to NULL after FLR completes.	7.8	More Details
CVE-2026-41477	Deskflow is a keyboard and mouse sharing app. In 1.20.0, 1.26.0.134, and earlier, Deskflow daemon runs as SYSTEM and exposes an IPC named pipe with WorldAccessOption enabled. The daemon processes privileged commands without authentication, allowing any local unprivileged user to execute arbitrary commands as SYSTEM. Affects both stable v1.20.0 + and Continuous v1.26.0.134 prerelease.	7.8	More Details
CVE-2026-42432	OpenClaw before 2026.4.8 contains a privilege escalation vulnerability allowing previously paired nodes to reconnect with exec-capable commands without operator.admin scope requirement. Attackers can bypass re-pairing authentication to execute privileged commands on the local assistant system.	7.8	More Details
CVE-2026-41396	OpenClaw before 2026.3.31 allows workspace .env files to override the OPENCLAW_BUNDLED_PLUGINS_DIR environment variable, compromising plugin trust verification. Attackers with control over workspace configuration can inject malicious plugins by overriding the bundled plugin trust root directory.	7.8	More Details
CVE-2026-	OpenClaw before 2026.3.24 contains an environment variable injection vulnerability in the CLI backend runner that allows attackers to inject malicious environment variables through workspace configuration. Attackers can craft malicious workspace configs to inject arbitrary environment variables into the backend process spawning, enabling code execution or	7.8	More Details

41384	sensitive data exposure.		
CVE-2026-31602	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Limit PTP to a single page Commit 391e69143d0a increased CT_PTP_NUM from 1 to 4 to support 256 playback streams, but the additional pages are not used by the card correctly. The CT20K2 hardware already has multiple VMEM_PTPAL registers, but using them separately would require refactoring the entire virtual memory allocation logic. ct_vm_map() always uses PTEs in vm->ptp[0].area regardless of CT_PTP_NUM. On AMD64 systems, a single PTP covers 512 PTEs (2M). When aggregate memory allocations exceed this limit, ct_vm_map() tries to access beyond the allocated space and causes a page fault: BUG: unable to handle page fault for address: ffffd4ae8a10a000 Oops: Oops: 0002 [#1] SMP PTI RIP: 0010:ct_vm_map+0x17c/0x280 [snd_ctxfi] Call Trace: atc_pcm_playback_prepare+0x225/0x3b0 ct_pcm_playback_prepare+0x38/0x60 snd_pcm_do_prepare+0x2f/0x50 snd_pcm_action_single+0x36/0x90 snd_pcm_action_nonatomic+0xbf/0xd0 snd_pcm_ioctl+0x28/0x40 __x64_sys_ioctl+0x97/0xe0 do_syscall_64+0x81/0x610 entry_SYSCALL_64_after_hwframe+0x76/0x7e Revert CT_PTP_NUM to 1. The 256 SRC_RESOURCE_NUM and playback_count remain unchanged.	7.8	More Details
CVE-2026-6846	A flaw was found in binutils. A heap-buffer-overflow vulnerability exists when processing a specially crafted XCOFF (Extended Common Object File Format) object file during linking. A local attacker could trick a user into processing this malicious file, which could lead to arbitrary code execution, allowing the attacker to run unauthorized commands, or cause a denial of service, making the system unavailable.	7.8	More Details
CVE-2026-31479	In the Linux kernel, the following vulnerability has been resolved: drm/xe: always keep track of remap prev/next During 3D workload, user is reporting hitting: [413.361679] WARNING: drivers/gpu/drm/xe/xe_vm.c:1217 at vm_bind_ioctl_ops_unwind+0x1e2/0x2e0 [xe], CPU#7: vkd3d_queue/9925 [413.361944] CPU: 7 UID: 1000 PID: 9925 Comm: vkd3d_queue Kdump: loaded Not tainted 7.0.0-070000rc3-generic #202603090038 PREEMPT(lazy) [413.361949] RIP: 0010:vm_bind_ioctl_ops_unwind+0x1e2/0x2e0 [xe] [413.362074] RSP: 0018:ffffd4c25c3df930 EFLAGS: 00010282 [413.362077] RAX: 0000000000000000 RBX: ffff8f3ee817ed10 RCX: 0000000000000000 [413.362078] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 [413.362079] RBP: ffffd4c25c3df980 R08: 0000000000000000 R09: 0000000000000000 [413.362081] R10: 0000000000000000 R11: 0000000000000000 R12: ffff8f41fbf99380 [413.362082] R13: ffff8f3ee817e968 R14: 00000000ffffffef R15: ffff8f43d00bd380 [413.362083] FS: 00000001040ff6c0(0000) GS:ffff8f4696d89000(0000) knlGS:00000000330b0000 [413.362085] CS: 0010 DS: 002b ES: 002b CR0: 0000000080050033 [413.362086] CR2: 00007ddfc4747000 CR3: 00000002e6262005 CR4: 0000000000f72ef0 [413.362088] PKRU: 55555554 [413.362089] Call Trace: [413.362092] <TASK> [413.362096] xe_vm_bind_ioctl+0xa9a/0xc60 [xe] Which seems to hint that the vma we are re-inserting for the ops unwind is either invalid or overlapping with something already inserted in the vm. It shouldn't be invalid since this is a re-insertion, so must have worked before. Leaving the likely culprit as something already placed where we want to insert the vma. Following from that, for the case where we do something like a rebind in the middle of a vma, and one or both mapped ends are already compatible, we skip doing the rebind of those vma and set next/prev to NULL. As well as then adjust the original unmap va range, to avoid unmapping the ends. However, if we trigger the unwind path, we end up with three va, with the two ends never being removed and the original va range in the middle still being the shrunken size. If this occurs, one failure mode is when another unwind op needs to interact with that range, which can happen with a vector of binds. For example, if we need to re-insert something in place of the original va. In this case the va is still the shrunken version, so when removing it and then doing a re-insert it can overlap with the ends, which were never removed, triggering a warning like above, plus leaving the vm in a bad state. With that, we need two things here: 1) Stop nuking the prev/next tracking for the skip cases. Instead relying on checking for skip prev/next, where needed. That way on the unwind path, we now correctly remove both ends. 2) Undo the unmap va shrinkage, on the unwind path. With the two ends now removed the unmap va should expand back to the original size again, before re-insertion. v2: - Update the explanation in the commit message, based on an actual IGT of triggering this issue, rather than conjecture. - Also undo the unmap shrinkage, for the skip case. With the two ends now removed, the original unmap va range should expand back to the original range. v3: - Track the old start/range separately. vma_size/start() uses the va info directly. (cherry picked from commit aec6969f75afbf4e01fd5fb5850ed3e9c27043ac)	7.8	More Details
CVE-2026-31502	In the Linux kernel, the following vulnerability has been resolved: team: fix header_ops type confusion with non-Ethernet ports Similar to commit 950803f72547 ("bonding: fix type confusion in bond_setup_by_slave()") team has the same class of header_ops type confusion. For non-Ethernet ports, team_setup_by_port() copies port_dev->header_ops directly. When the team device later calls dev_hard_header() or dev_parse_header(), these callbacks can run with the team net_device instead of the real lower device, so netdev_priv(dev) is interpreted as the wrong private type and can crash. The syzbot report shows a crash in bond_header_create(), but the root cause is in team: the topology is gre -> bond -> team, and team calls the inherited header_ops with its own net_device instead of the lower device, so bond_header_create() receives a team device and interprets netdev_priv() as bonding private data, causing a type confusion crash. Fix this by introducing team header_ops wrappers for create/parse, selecting a team port under RCU, and calling the lower device callbacks with port->dev, so each callback always sees the correct net_device context. Also pass the selected lower device to the lower parse callback, so recursion is bounded in stacked non-Ethernet topologies and parse callbacks always run with the correct device context.	7.8	More Details
CVE-2026-31675	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_netem: fix out-of-bounds access in packet corruption In netem_enqueue(), the packet corruption logic uses get_random_u32_below(skb_headlen(skb)) to select an index for modifying skb->data. When an AF_PACKET TX_RING sends fully non-linear packets over an IPIP tunnel, skb_headlen(skb) evaluates to 0. Passing 0 to get_random_u32_below() takes the variable-ceil slow path which returns an unconstrained 32-bit random integer. Using this unconstrained value as an offset into skb->data results in an out-of-bounds memory access. Fix this by verifying skb_headlen(skb) is non-zero before attempting to corrupt the linear data area. Fully non-linear packets will silently bypass the corruption logic.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel: serialize btintel_hw_error() with hci_req_sync_lock btintel_hw_error() issues two __hci_cmd_sync() calls (HCI_OP_RESET and Intel exception-info retrieval) without holding hci_req_sync_lock(). This lets it race against hci_dev_do_close() -> btintel_shutdown_combined(), which also runs __hci_cmd_sync() under the same lock. When both paths manipulate hdev->req_status/req_rsp concurrently, the close path may free the response skb first, and the still-running hw_error path hits a slab-use-after-free in kfree_skb(). Wrap the whole recovery sequence in hci_req_sync_lock/unlock so it is serialized with every other synchronous HCI command issuer. Below is the data race report and the kasan report: BUG: data-race in __hci_cmd_sync_sk / btintel_shutdown_combined read		

CVE-2026-31500	of hdev->req_rsp at net/bluetooth/hci_sync.c:199 by task kworker/u17:1/83: __hci_cmd_sync_sk+0x12f2/0x1c30 net/bluetooth/hci_sync.c:200 __hci_cmd_sync+0x55/0x80 net/bluetooth/hci_sync.c:223 btintel_hw_error+0x114/0x670 drivers/bluetooth/btintel.c:254 hci_error_reset+0x348/0xa30 net/bluetooth/hci_core.c:1030 write/free by task ioctl/22580: btintel_shutdown_combined+0xd0/0x360 drivers/bluetooth/btintel.c:3648 hci_dev_close_sync+0x9ae/0x2c10 net/bluetooth/hci_sync.c:5246 hci_dev_do_close+0x232/0x460 net/bluetooth/hci_core.c:526 BUG: KASAN: slab-use-after-free in sk_skb_reason_drop+0x43/0x380 net/core/skbuff.c:1202 Read of size 4 at addr ffff888144a738dc by task kworker/u17:1/83: __hci_cmd_sync_sk+0x12f2/0x1c30 net/bluetooth/hci_sync.c:200 __hci_cmd_sync+0x55/0x80 net/bluetooth/hci_sync.c:223 btintel_hw_error+0x186/0x670 drivers/bluetooth/btintel.c:260	7.8	More Details
CVE-2026-31680	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: flowlabel: defer exclusive option free until RCU teardown `ip6fl_seq_show()` walks the global flowlabel hash under the seq-file RCU read-side lock and prints `fl->opt->opt_nflen` when an option block is present. Exclusive flowlabels currently free `fl->opt` as soon as `fl->users` drops to zero in `fl_release()`. However, the surrounding `struct ip6_flowlabel` remains visible in the global hash table until later garbage collection removes it and `fl_free_rcu()` finally tears it down. A concurrent `/proc/net/ip6_flowlabel` reader can therefore race that early `kfree()` and dereference freed option state, triggering a crash in `ip6fl_seq_show()`. Fix this by keeping `fl->opt` alive until `fl_free_rcu()`. That matches the lifetime already required for the enclosing flowlabel while readers can still reach it under RCU.	7.8	More Details
CVE-2026-31586	In the Linux kernel, the following vulnerability has been resolved: mm: blk-cgroup: fix use-after-free in cgwb_release_workfn() cgwb_release_workfn() calls css_put(wb->blkcg_css) and then later accesses wb->blkcg_css again via blkcg_unpin_online(). If css_put() drops the last reference, the blkcg can be freed asynchronously (css_free_rwork_fn -> blkcg_css_free -> kfree) before blkcg_unpin_online() dereferences the pointer to access blkcg->online_pin, resulting in a use-after-free: BUG: KASAN: slab-use-after-free in blkcg_unpin_online (./include/linux/instrumented.h:112 ./include/linux/atomic/atomic-instrumented.h:400 ./include/linux/refcount.h:389 ./include/linux/refcount.h:432 ./include/linux/refcount.h:450 block/blk-cgroup.c:1367) Write of size 4 at addr ff11000117aa6160 by task kworker/71:1/531 Workqueue: cgwb_release cgwb_release_workfn Call Trace: <TASK> blkcg_unpin_online (./include/linux/instrumented.h:112 ./include/linux/atomic/atomic-instrumented.h:400 ./include/linux/refcount.h:389 ./include/linux/refcount.h:432 ./include/linux/refcount.h:450 block/blk-cgroup.c:1367) cgwb_release_workfn (mm/backing-dev.c:629) process_scheduled_works (kernel/workqueue.c:3278 kernel/workqueue.c:3385) Freed by task 1016: kfree (./include/linux/kasan.h:235 mm/slub.c:2689 mm/slub.c:6246 mm/slub.c:6561) css_free_rwork_fn (kernel/cgroup/cgroup.c:5542) process_scheduled_works (kernel/workqueue.c:3302 kernel/workqueue.c:3385) ** Stack based on commit 66672af7a095 ("Add linux-next specific files for 20260410") I am seeing this crash sporadically in Meta fleet across multiple kernel versions. A full reproducer is available at: https://github.com/leitao/debug/blob/main/reproducers/repro_blkcg_uaf.sh (The race window is narrow. To make it easily reproducible, inject a msleep(100) between css_put() and blkcg_unpin_online() in cgwb_release_workfn(). With that delay and a KASAN-enabled kernel, the reproducer triggers the splat reliably in less than a second.) Fix this by moving blkcg_unpin_online() before css_put(), so the cgwb's CSS reference keeps the blkcg alive while blkcg_unpin_online() accesses it.	7.8	More Details
CVE-2026-34003	A flaw was found in the X.Org X server's XKB key types request validation. A local attacker could send a specially crafted request to the X server, leading to an out-of-bounds memory access vulnerability. This could result in the disclosure of sensitive information or cause the server to crash, leading to a Denial of Service (DoS). In certain configurations, higher impact outcomes may be possible.	7.8	More Details
CVE-2026-31678	In the Linux kernel, the following vulnerability has been resolved: openvswitch: defer tunnel netdev_put to RCU release ovs_netdev_tunnel_destroy() may run after NETDEV_UNREGISTER already detached the device. Dropping the netdev reference in destroy can race with concurrent readers that still observe vport->dev. Do not release vport->dev in ovs_netdev_tunnel_destroy(). Instead, let vport_netdev_free() drop the reference from the RCU callback, matching the non-tunnel destroy path and avoiding additional synchronization under RTNL.	7.8	More Details
CVE-2026-34001	A flaw was found in the X.Org X server. This use-after-free vulnerability occurs in the XSYNC fence triggering logic, specifically within the miSyncTriggerFence() function. An attacker with access to the X11 server can exploit this without user interaction, leading to a server crash and potentially enabling memory corruption. This could result in a denial of service or further compromise of the system.	7.8	More Details
CVE-2026-31494	In the Linux kernel, the following vulnerability has been resolved: net: macb: use the current queue number for stats There's a potential mismatch between the memory reserved for statistics and the amount of memory written. gem_get_sset_count() correctly computes the number of stats based on the active queues, whereas gem_get_ethtool_stats() indiscriminately copies data using the maximum number of queues, and in the case the number of active queues is less than MACB_MAX_QUEUES, this results in a OOB write as observed in the KASAN splat. == BUG: KASAN: vmalloc-out-of-bounds in gem_get_ethtool_stats+0x54/0x78 [macb] Write of size 760 at addr ffff80008080b000 by task ethtool/1027 CPU: [...] Tainted: [E]=UNSIGNED_MODULE Hardware name: raspberrypi rpi/rpi, BIOS 2025.10 10/01/2025 Call trace: show_stack+0x20/0x38 (C) dump_stack_lvl+0x80/0xf8 print_report+0x384/0x5e0 kasan_report+0xa0/0xf0 kasan_check_range+0xe8/0x190 __asan_memcpy+0x54/0x98 gem_get_ethtool_stats+0x54/0x78 [macb 926c13f3af83b0c6fe64badb21ec87d5e93fcf65] dev_ethtool+0x1220/0x38c0 dev_ioctl+0x4ac/0xca8 sock_do_ioctl+0x170/0x1d8 sock_ioctl+0x484/0x5d8 __arm64_sys_ioctl+0x12c/0x1b8 invoke_syscall+0xd4/0x258 el0_svc_common.constprop.0+0xb4/0x240 do_el0_svc+0x48/0x68 el0_svc+0x40/0xf8 el0t_64_sync_handler+0xa0/0xe8 el0t_64_sync+0x1b0/0x1b8 The buggy address belongs to a 1-page vmalloc region starting at 0xffff80008080b000 allocated at dev_ethtool+0x11f0/0x38c0 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:0000000000000000 index:0xffff00000a333000 pfn:0xa333 flags: 0x7fffc000000000(node=0|zone=0|lastcpupid=0x1ffff) raw: 007fffc000000000 0000000000000000 dead000000000122 0000000000000000 raw: ffff00000a333000 0000000000000000 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff80008080b080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff80008080b100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >ffff80008080b180: 00 00 00 00 00 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ ffff80008080b200: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffff80008080b280: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8	7.8	More Details

	========== Fix it by making sure the copied size only considers the active number of queues.		
CVE-2026-31493	In the Linux kernel, the following vulnerability has been resolved: RDMA/efa: Fix use of completion ctx after free On admin queue completion handling, if the admin command completed with error we print data from the completion context. The issue is that we already freed the completion context in polling/interrupts handler which means we print data from context in an unknown state (it might be already used again). Change the admin submission flow so alloc/dealloc of the context will be symmetric and dealloc will be called after any potential use of the context.	7.8	More Details
CVE-2026-33999	A flaw was found in the X.Org X server. This integer underflow vulnerability, specifically in the XKB compatibility map handling, allows an attacker with local or remote X11 server access to trigger a buffer read overrun. This can lead to memory-safety violations and potentially a denial of service (DoS) or other severe impacts.	7.8	More Details
CVE-2026-31656	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: fix refcount underflow in intel_engine_park_heartbeat A use-after-free / refcount underflow is possible when the heartbeat worker and intel_engine_park_heartbeat() race to release the same engine->heartbeat.systole request. The heartbeat worker reads engine->heartbeat.systole and calls i915_request_put() on it when the request is complete, but clears the pointer in a separate, non-atomic step. Concurrently, a request retirement on another CPU can drop the engine wakeref to zero, triggering __engine_park() -> intel_engine_park_heartbeat(). If the heartbeat timer is pending at that point, cancel_delayed_work() returns true and intel_engine_park_heartbeat() reads the stale non-NULL systole pointer and calls i915_request_put() on it again, causing a refcount underflow: ``` <4> [487.221889] Workqueue: i915-unordered engine_retire [i915] <4> [487.222640] RIP: 0010:refcount_warn_saturate+0x68/0xb0 ... <4> [487.222707] Call Trace: <4> [487.222711] <TASK> <4> [487.222716] intel_engine_park_heartbeat.part.0+0x6f/0x80 [i915] <4> [487.223115] intel_engine_park_heartbeat+0x25/0x40 [i915] <4> [487.223566] __engine_park+0xb9/0x650 [i915] <4> [487.223973] ___intel_wakeref_put_last+0x2e/0xb0 [i915] <4> [487.224408] __intel_wakeref_put_last+0x72/0x90 [i915] <4> [487.224797] intel_context_exit_engine+0x7c/0x80 [i915] <4> [487.225238] intel_context_exit+0xf1/0x1b0 [i915] <4> [487.225695] i915_request_retire.part.0+0x1b9/0x530 [i915] <4> [487.226178] i915_request_retire+0x1c/0x40 [i915] <4> [487.226625] engine_retire+0x122/0x180 [i915] <4> [487.227037] process_one_work+0x239/0x760 <4> [487.227060] worker_thread+0x200/0x3f0 <4> [487.227068] ? __pfx_worker_thread+0x10/0x10 <4> [487.227075] kthread+0x10d/0x150 <4> [487.227083] ? __pfx_kthread+0x10/0x10 <4> [487.227092] ret_from_fork+0x3d4/0x480 <4> [487.227099] ? __pfx_kthread+0x10/0x10 <4> [487.227107] ret_from_fork_asm+0x1a/0x30 <4> [487.227141] </TASK> ``` Fix this by replacing the non-atomic pointer read + separate clear with xchg() in both racing paths. xchg() is a single indivisible hardware instruction that atomically reads the old pointer and writes NULL. This guarantees only one of the two concurrent callers obtains the non-NULL pointer and performs the put, the other gets NULL and skips it. (cherry picked from commit 13238dc0ee4f9ab8dafa2cca7295736191ae2f42)	7.8	More Details
CVE-2026-31587	In the Linux kernel, the following vulnerability has been resolved: ASoC: qcom: q6apm: move component registration to unmanaged version q6apm component registers dais dynamically from ASoC toplology, which are allocated using device managed version apis. Allocating both component and dynamic dais using managed version could lead to incorrect free ordering, dai will be freed while component still holding references to it. Fix this issue by moving component to unmanged version so that the dai pointers are only freeded after the component is removed. ========== BUG: KASAN: slab-use-after-free in snd_soc_del_component_unlocked+0x3d4/0x400 [snd_soc_core] Read of size 8 at addr ffff00084493a6e8 by task kworker/u48:0/3426 Tainted: [W]=WARN Hardware name: LENOVO 21N2ZC5PUS/21N2ZC5PUS, BIOS N42ET57W (1.31) 08/08/2024 Workqueue: pdr_notifier_wq pdr_notifier_work [pdr_interface] Call trace: show_stack+0x28/0x7c (C) dump_stack_lvl+0x60/0x80 print_report+0x160/0x4b4 kasan_report+0xac/0xfc __asan_report_load8_noabort+0x20/0x34 snd_soc_del_component_unlocked+0x3d4/0x400 [snd_soc_core] snd_soc_unregister_component_by_driver+0x50/0x88 [snd_soc_core] devm_component_release+0x30/0x5c [snd_soc_core] devres_release_all+0x13c/0x210 device_unbind_cleanup+0x20/0x190 device_release_driver_internal+0x350/0x468 device_release_driver+0x18/0x30 bus_remove_device+0x1a0/0x35c device_del+0x314/0x7f0 device_unregister+0x20/0xbc apr_remove_device+0x5c/0x7c [apr] device_for_each_child+0xd8/0x160 apr_pd_status+0x7c/0xa8 [apr] pdr_notifier_work+0x114/0x240 [pdr_interface] process_one_work+0x500/0xb70 worker_thread+0x630/0xfb0 kthread+0x370/0x6c0 ret_from_fork+0x10/0x20 Allocated by task 77: kasan_save_stack+0x40/0x68 kasan_save_track+0x20/0x40 kasan_save_alloc_info+0x44/0x58 __kasan_kmalloc+0xbc/0xdc __kmalloc_node_track_caller_noprof+0x1f4/0x620 devm_kmalloc+0x7c/0x1c8 snd_soc_register_dai+0x50/0x4f0 [snd_soc_core] soc_tplg_pcm_elems_load+0x55c/0x1eb8 [snd_soc_core] snd_soc_tplg_component_load+0x4f8/0xb60 [snd_soc_core] audioreach_tplg_init+0x124/0x1fc [snd_q6apm] q6apm_audio_probe+0x10/0x1c [snd_q6apm] snd_soc_component_probe+0x5c/0x118 [snd_soc_core] soc_probe_component+0x44c/0xaf0 [snd_soc_core] snd_soc_bind_card+0xad0/0x2370 [snd_soc_core] snd_soc_register_card+0x3b0/0x4c0 [snd_soc_core] devm_snd_soc_register_card+0x50/0xc8 [snd_soc_core] x1e80100_platform_probe+0x208/0x368 [snd_soc_x1e80100] platform_probe+0xc0/0x188 really_probe+0x188/0x804 __driver_probe_device+0x158/0x358 driver_probe_device+0x60/0x190 __device_attach_driver+0x16c/0x2a8 bus_for_each_drv+0x100/0x194 __device_attach+0x174/0x380 device_initial_probe+0x14/0x20 bus_probe_device+0x124/0x154 deferred_probe_work_func+0x140/0x220 process_one_work+0x500/0xb70 worker_thread+0x630/0xfb0 kthread+0x370/0x6c0 ret_from_fork+0x10/0x20 Freed by task 3426: kasan_save_stack+0x40/0x68 kasan_save_track+0x20/0x40 __kasan_save_free_info+0x4c/0x80 __kasan_slab_free+0x78/0xa0 kfree+0x100/0x4a4 devres_release_all+0x144/0x210 device_unbind_cleanup+0x20/0x190 device_release_driver_internal+0x350/0x468 device_release_driver+0x18/0x30 bus_remove_device+0x1a0/0x35c device_del+0x314/0x7f0 device_unregister+0x20/0xbc apr_remove_device+0x5c/0x7c [apr] device_for_each_child+0xd8/0x160 apr_pd_status+0x7c/0xa8 [apr] pdr_notifier_work+0x114/0x240 [pdr_interface] process_one_work+0x500/0xb70 worker_thread+0x630/0xfb0 kthread+0x370/0x6c0 ret_from_fork+0x10/0x20	7.8	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: mm/damon/stat: deallocate damon_call() failure leaking damon_ctx damon_stat_start() always allocates the module's damon_ctx object (damon_stat_context). Meanwhile, if damon_call() in the function fails, the damon_ctx object is not deallocated. Hence, if the damon_call() is failed, and the user writes Y to “enabled” again, the previously allocated damon_ctx object is leaked. This cannot simply be fixed by deallocating the damon_ctx object when damon_call() fails. That's because damon_call() failure doesn't guarantee the		More

2026-31652	kdamond main function, which accesses the damon_ctx object, is completely finished. In other words, if damon_stat_start() deallocates the damon_ctx object after damon_call() failure, the not-yet-terminated kdamond could access the freed memory (use-after-free). Fix the leak while avoiding the use-after-free by keeping returning damon_stat_start() without deallocating the damon_ctx object after damon_call() failure, but deallocating it when the function is invoked again and the kdamond is completely terminated. If the kdamond is not yet terminated, simply return -EAGAIN, as the kdamond will soon be terminated. The issue was discovered [1] by sashiko.	7.8	Details
CVE-2026-31489	In the Linux kernel, the following vulnerability has been resolved: spi: meson-spicc: Fix double-put in remove path meson_spicc_probe() registers the controller with devm_spi_register_controller(), so teardown already drops the controller reference via devm cleanup. Calling spi_controller_put() again in meson_spicc_remove() causes a double-put.	7.8	More Details
CVE-2026-31488	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Do not skip unrelated mode changes in DSC validation Starting with commit 17ce8a6907f7 ("drm/amd/display: Add dsc pre-validation in atomic check"), amdgpu resets the CRTC state mode_changed flag to false when recomputing the DSC configuration results in no timing change for a particular stream. However, this is incorrect in scenarios where a change in MST/DSC configuration happens in the same KMS commit as another (unrelated) mode change. For example, the integrated panel of a laptop may be configured differently (e.g., HDR enabled/disabled) depending on whether external screens are attached. In this case, plugging in external DP-MST screens may result in the mode_changed flag being dropped incorrectly for the integrated panel if its DSC configuration did not change during precomputation in pre_validate_dsc(). At this point, however, dm_update_crtc_state() has already created new streams for CRTCs with DSC-independent mode changes. In turn, amdgpu_dm_commit_streams() will never release the old stream, resulting in a memory leak. amdgpu_dm_atomic_commit_tail() will never acquire a reference to the new stream either, which manifests as a use-after-free when the stream gets disabled later on: BUG: KASAN: use-after-free in dc_stream_release+0x25/0x90 [amdgpu] Write of size 4 at addr ffff88813d836524 by task kworker/9:9/29977 Workqueue: events drm_mode_rmfb_work_fn Call Trace: <TASK> dump_stack_lvl+0x6e/0xa0 print_address_description.constprop.0+0x88/0x320 ? dc_stream_release+0x25/0x90 [amdgpu] print_report+0xfc/0x1ff ? srso_alias_return_thunk+0x5/0xfbef5 ? __virt_addr_valid+0x225/0x4e0 ? dc_stream_release+0x25/0x90 [amdgpu] kasan_report+0xe1/0x180 ? dc_stream_release+0x25/0x90 [amdgpu] kasan_check_range+0x125/0x200 dc_stream_release+0x25/0x90 [amdgpu] dc_state_destruct+0x14d/0x5c0 [amdgpu] dc_state_release.part.0+0x4e/0x130 [amdgpu] dm_atomic_destroy_state+0x3f/0x70 [amdgpu] drm_atomic_state_default_clear+0x8ee/0xf30 ? drm_mode_object_put.part.0+0xb1/0x130 __drm_atomic_state_free+0x15c/0x2d0 atomic_remove_fb+0x67e/0x980 Since there is no reliable way of figuring out whether a CRTC has unrelated mode changes pending at the time of DSC validation, remember the value of the mode_changed flag from before the point where a CRTC was marked as potentially affected by a change in DSC configuration. Reset the mode_changed flag to this earlier value instead in pre_validate_dsc(). (cherry picked from commit cc7c7121ae082b7b82891baa7280f1ff2608f22b)	7.8	More Details
CVE-2026-7039	A security vulnerability has been detected in tufantunc ssh-mcp up to 1.5.0. The affected element is the function shell.write of the file src/index.ts. Such manipulation of the argument Description leads to command injection. The attack must be carried out locally. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.8	More Details
CVE-2026-31485	In the Linux kernel, the following vulnerability has been resolved: spi: spi-fsl-lpspi: fix teardown order issue (UAF) There is a teardown order issue in the driver. The SPI controller is registered using devm_spi_register_controller(), which delays unregistration of the SPI controller until after the fsl_lpspi_remove() function returns. As the fsl_lpspi_remove() function synchronously tears down the DMA channels, a running SPI transfer triggers the following NULL pointer dereference due to use after free: | fsl_lpspi 42550000.spi: I/O Error in DMA RX | Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [...] | Call trace: | fsl_lpspi_dma_transfer+0x260/0x340 [spi_fsl_lpspi] | fsl_lpspi_transfer_one+0x198/0x448 [spi_fsl_lpspi] | spi_transfer_one_message+0x49c/0x7c8 | __spi_pump_transfer_message+0x120/0x420 | __spi_sync+0x2c4/0x520 | spi_sync+0x34/0x60 | spidev_message+0x20c/0x378 [spidev] | spidev_ioctl+0x398/0x750 [spidev] [...] Switch from devm_spi_register_controller() to spi_register_controller() in fsl_lpspi_probe() and add the corresponding spi_unregister_controller() in fsl_lpspi_remove().	7.8	More Details
CVE-2026-31673	In the Linux kernel, the following vulnerability has been resolved: af_unix: read UNIX_DIAG_VFS data under unix_state_lock Exact UNIX diag lookups hold a reference to the socket, but not to u->path. Meanwhile, unix_release_sock() clears u->path under unix_state_lock() and drops the path reference after unlocking. Read the inode and device numbers for UNIX_DIAG_VFS while holding unix_state_lock(), then emit the netlink attribute after dropping the lock. This keeps the VFS data stable while the reply is being built.	7.8	More Details
CVE-2026-42171	NSIS (Nullsoft Scriptable Install System) 3.06.1 before 3.12 sometimes uses the Low IL temp directory when executing as SYSTEM, allowing local attackers to gain privileges (if they can cause my_GetTempFileName to return 0, as shown in the references).	7.8	More Details
CVE-2026-40517	radare2 prior to 6.1.4 contains a command injection vulnerability in the PDB parser's print_gvars() function that allows attackers to execute arbitrary commands by crafting a malicious PDB file with newline characters in symbol names. Attackers can inject arbitrary radare2 commands through unsanitized symbol name interpolation in the flag rename command, which are then executed when a user runs the idp command against the malicious PDB file, enabling arbitrary OS command execution through radare2's shell execution operator.	7.8	More Details
CVE-2026-42379	Insertion of Sensitive Information Into Sent Data vulnerability in WPDeveloper Templately allows Retrieve Embedded Sensitive Data.This issue affects Templately: from n/a through 3.6.1.	7.7	More Details
CVE-2026-40886	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. From 3.6.5 to 4.0.4, an unchecked array index in the pod informer's podGCFromPod() function causes a controller-wide panic when a workflow pod carries a malformed workflows.argoproj.io/pod-gc-strategy annotation. Because the panic occurs inside an informer goroutine (outside the controller's recover() scope), it crashes the entire controller process. The poisoned pod persists across restarts, causing a crash loop that halts all workflow processing until the pod is manually deleted. This vulnerability is fixed in 4.0.5 and 3.7.14.	7.7	More Details

CVE-2026-41485	Kyverno is a policy engine designed for cloud native platform engineering teams. Prior to versions 1.17.2 and 1.16.4, an unchecked type assertion in the `forEach` mutation handler allows any user with permission to create a `Policy` or `ClusterPolicy` to crash the cluster-wide background controller into a persistent CrashLoopBackOff. The same bug also causes the admission controller to drop connections and block all matching resource operations. The crash loop persists until the policy is deleted. The vulnerability is confined to the legacy engine, and CEL-based policies are unaffected. Versions 1.17.2 and 1.16.4 fix the issue.	7.7	More Details
CVE-2026-41649	Outline is a service that allows for collaborative documentation. The `shares.create` API endpoint starting in version 0.86.0 and prior to version 1.7.0 has an insecure direct object reference.. When both `collectionId` and `documentId` are provided in the request, the authorization logic only checks access to the collection, completely ignoring the document. This allows an authenticated attacker to generate a valid public share link for any document on the platform, including documents belonging to other workspaces. The full document contents can then be retrieved via the `documents.info` endpoint. Version 1.7.0 contains a patch.	7.7	More Details
CVE-2026-41068	Kyverno is a policy engine designed for cloud native platform engineering teams. The patch for CVE-2026-22039 fixed cross-namespace privilege escalation in Kyverno's `apiCall` context by validating the `URLPath` field. However, the ConfigMap context loader has the identical vulnerability — the `configMap.namespace` field accepts any namespace with zero validation, allowing a namespace admin to read ConfigMaps from any namespace using Kyverno's privileged service account. This is a complete RBAC bypass in multi-tenant Kubernetes clusters. An updated fix is available in version 1.17.2.	7.7	More Details
CVE-2026-31952	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Versions 1.7 through 4.4.0 have an SQL injection vulnerability in the API routes inside the CMS responsible for Filtering DataSets. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the API filter parameter. Exploitation of the vulnerability is possible on behalf of an authorized user who has either of the `Access to DataSet Feature` privilege or the `Access to the Layout Feature` privilege. Users should upgrade to version 4.4.1 which fixes this issue. Customers who host their CMS with Xibo Signage have been patched if they are using 4.4, 4.3, 3.3, 2.3 or 1.8. Upgrading to a fixed version is necessary to remediate. Patches are available for earlier versions of Xibo CMS that are out of support, namely 3.3, 2.3, and 1.8.	7.6	More Details
CVE-2026-40882	OpenRemote is an open-source internet-of-things platform. Prior to version 1.22.0, the Velbus asset import path parses attacker-controlled XML without explicit XXE hardening. An authenticated user who can call the import endpoint may trigger XML external entity processing, which can lead to server-side file disclosure and SSRF. The target file must be less than 1023 characters. Version 1.22.0 fixes the issue.	7.6	More Details
CVE-2026-41419	4ga Boards is a boards system for realtime project management. Prior to 3.3.5, a path traversal vulnerability allows an authenticated user with board import privileges to make the server ingest arbitrary host files as board attachments during BOARDS archive import. Once imported, the file can be downloaded through the normal application interface, resulting in unauthorized local file disclosure. This vulnerability is fixed in 3.3.5.	7.6	More Details
CVE-2026-41912	OpenClaw before 2026.4.8 contains a server-side request forgery policy bypass vulnerability allowing attackers to trigger navigations bypassing normal SSRF checks. Attackers can exploit browser interactions to bypass SSRF protections and access restricted resources.	7.6	More Details
CVE-2025-69428	An issue in Pro-Bit before v1.77.4 allows unauthenticated attackers to directly access sensitive directory and its subdirectories.	7.5	More Details
CVE-2026-31467	In the Linux kernel, the following vulnerability has been resolved: erofs: add GFP_NOIO in the bio completion if needed The bio completion path in the process context (e.g. dm-verity) will directly call into decompression rather than trigger another workqueue context for minimal scheduling latencies, which can then call vm_map_ram() with GFP_KERNEL. Due to insufficient memory, vm_map_ram() may generate memory swapping I/O, which can cause submit_bio_wait to deadlock in some scenarios. Trimmed down the call stack, as follows: f2fs_submit_read_io submit_bio //bio_list is initialized. mmc_blk_mq_recovery z_erofs_endio vm_map_ram __pte_alloc_kernel __alloc_pages_direct_reclaim shrink_folio_list __swap_writepage submit_bio_wait //bio_list is non-NULL, hang!!! Use memalloc_noio_{save,restore}() to wrap up this path.	7.5	More Details
CVE-2026-41502	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to 1.4.3, an off-by-one out-of-bounds read vulnerability in bacnet-stack's ReadPropertyMultiple service decoder allows unauthenticated remote attackers to read one byte past an allocated buffer boundary by sending a crafted RPM request with a truncated object identifier. The vulnerability is in rpm_decode_object_id(), which checks apdu_len < 5 but then accesses all 6 byte positions (indices 0-5) — consuming 1 byte for the context tag, 4 bytes for the object ID, then reading apdu[5] for the opening tag check. A 5-byte input passes the length check but causes a 1-byte OOB read, leading to crashes on embedded BACnet devices. The vulnerability exists in src/bacnet/rpm.c and affects any deployment that enables the ReadPropertyMultiple confirmed service handler (enabled by default in the reference server). This vulnerability is fixed in 1.4.3.	7.5	More Details
CVE-2026-32870	Kirby is an open-source content management system. Kirby's `Xml::value()` method has special handling for `<![CDATA[ ]]>` blocks. If the input value is already valid `CDATA`, it is not escaped a second time but allowed to pass through. However, prior to versions 4.9.0 and 5.4.0, it was possible to trick this check into allowing values that only contained a valid `CDATA` block but also contained other structured data outside of the `CDATA` block. This structured data would then also be allowed to pass through, circumventing the value protection. The `Xml::value()` method is used in `Xml::tag()`, `Xml::create()` and in the `Xml` data handler (e.g. `Data::encode($string, 'xml')`). Both the vulnerable methods and the data handler are not used in the Kirby core. However they may be used in site or plugin code, e.g. to create XML strings from input data. If those generated files are passed to another implementation that assigns specific meaning to the XML schema, manipulation of this system's behavior is possible. Kirby sites that don't use XML generation in site or plugin code are not affected. The problem has been patched in Kirby 4.9.0 and Kirby 5.4.0. In all of the mentioned releases, Kirby has added additional checks that only allow unchanged `CDATA` passthrough if the entire string is made up of valid `CDATA` blocks and no structured data. This protects all uses of the method against the described vulnerability.	7.5	More Details
CVE-2026-	An unsecured configuration interface on affected devices allows unauthenticated remote attackers to access sensitive	7.5	More

3323	information, including hashed credentials and access codes.		Details
CVE-2026-41231	Froxlor is open source server administration software. Prior to version 2.3.6, `DataDump.add()` constructs the export destination path from user-supplied input without passing the `$fixed_homedir` parameter to `FileDir::makeCorrectDir()`, bypassing the symlink validation that was added to all other customer-facing path operations (likely as the fix for CVE-2023-6069). When the ExportCron runs as root, it executes `chown -R` on the resolved symlink target, allowing a customer to take ownership of arbitrary directories on the system. Version 2.3.6 contains an updated fix.	7.5	More Details
CVE-2026-41399	OpenClaw before 2026.3.28 accepts unbounded concurrent unauthenticated WebSocket upgrades without pre-authentication budget allocation. Unauthenticated network attackers can exhaust socket and worker capacity to disrupt WebSocket availability for legitimate clients.	7.5	More Details
CVE-2026-42423	OpenClaw before 2026.4.8 contains an approval-timeout fallback mechanism that bypasses strictInlineEval explicit-approval requirements on gateway and node exec hosts. Attackers can exploit this timeout fallback to execute inline eval commands that should require explicit user approval, circumventing the intended security boundary.	7.5	More Details
CVE-2026-41503	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to 1.4.3, an out-of-bounds read vulnerability in bacnet-stack's ReadPropertyMultiple service property decoder allows unauthenticated remote attackers to read past allocated buffer boundaries by sending an RPM request with a truncated property list. The vulnerability stems from rpm_decode_object_property() calling the deprecated decode_tag_number_and_value() function at src/bacnet/rpm.c:344, which accepts no buffer length parameter and reads blindly from whatever pointer it receives. A crafted BACnet/IP packet with a 1-byte property payload containing an extended tag marker (0xF9) causes the decoder to read 1 byte past the end of the buffer, leading to crashes on embedded BACnet devices. The vulnerability exists in src/bacnet/rpm.c and affects any deployment that enables the ReadPropertyMultiple confirmed service handler (enabled by default in the reference server). This vulnerability is fixed in 1.4.3.	7.5	More Details
CVE-2026-41564	CryptX versions before 0.088 for Perl do not reseed the Crypt::PK PRNG state after forking. The Crypt::PK::RSA, Crypt::PK::DSA, Crypt::PK::DH, Crypt::PK::ECC, Crypt::PK::Ed25519 and Crypt::PK::X25519 modules seed a per-object PRNG state in their constructors and reuse it without fork detection. A Crypt::PK::* object created before `fork()` shares byte-identical PRNG state with every child process, and any randomized operation they perform can produce identical output, including key generation. Two ECDSA or DSA signatures from different processes are enough to recover the signing private key through nonce-reuse key recovery. This affects preforking services such as the Starman web server, where a Crypt::PK::* object loaded at startup is inherited by every worker process.	7.5	More Details
CVE-2026-6903	The LabOne Web Server, backing the LabOne User Interface, contains insufficient input validation in its file access functionality. An unauthenticated attacker could exploit this vulnerability to read arbitrary files on the host system that are accessible to the operating system user running the LabOne software. Additionally, the Web Server does not sufficiently restrict cross-origin requests, which could allow a remote attacker to trigger file access from a victim's browser by directing the victim to a malicious website. The vulnerability is only exploitable when the LabOne Web Server is running. Installations using only the LabOne APIs without starting the Web Server are not exposed.	7.5	More Details
CVE-2026-31612	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate EaNameLength in smb2_get_ea() smb2_get_ea() reads ea_req->EaNameLength from the client request and passes it directly to strncmp() as the comparison length without verifying that the length of the name really is the size of the input buffer received. Fix this up by properly checking the size of the name based on the value received and the overall size of the request, to prevent a later strncmp() call to use the length as a "trusted" size of the buffer. Without this check, uninitialized heap values might be slowly leaked to the client.	7.5	More Details
CVE-2026-33524	Zserio is a framework for serializing structured data with a compact and efficient way with low overhead. Prior to 2.18.1, a crafted payload as small as 4-5 bytes can force memory allocations of up to 16 GB, crashing any process with an OOM error (Denial of Service). This vulnerability is fixed in 2.18.1.	7.5	More Details
CVE-2026-31256	A null pointer dereference vulnerability exists in the RTSP service of the MERCURY MIPC252W 1.0.5 Build 230306 Rel.79931n. During the processing of a SETUP request for the path rtsp://<IP>:554/stream1/track2, the device fails to properly validate the Transport header field. When this header is improperly constructed, the RTSP service can dereference a NULL pointer during request parsing. Successful exploitation causes the device to crash and automatically reboot.	7.5	More Details
CVE-2026-41636	Uncontrolled Recursion vulnerability in Apache Thrift Node.js bindings This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	7.5	More Details
CVE-2026-35064	A vulnerability in SenseLive X3050’s management ecosystem allows unauthenticated discovery of deployed units through the vendor’s management protocol, enabling identification of device presence, identifiers, and management interfaces without requiring credentials. Because discovery functions are exposed by the underlying service rather than gated by authentication, an attacker on the same network segment can rapidly enumerate targeted devices.	7.5	More Details
CVE-2026-31477	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix memory leaks and NULL deref in smb2_lock() smb2_lock() has three error handling issues after list_del() detaches smb_lock from lock_list at no_check_cl: 1) If vfs_lock_file() returns an unexpected error in the non-UNLOCK path, goto out leaks smb_lock and its flock because the out: handler only iterates lock_list and rollback_list, neither of which contains the detached smb_lock. 2) If vfs_lock_file() returns -ENOENT in the UNLOCK path, goto out leaks smb_lock and flock for the same reason. The error code returned to the dispatcher is also stale. 3) In the rollback path, smb_flock_init() can return NULL on allocation failure. The result is dereferenced unconditionally, causing a kernel NULL pointer dereference. Add a NULL check to prevent the crash and clean up the bookkeeping; the VFS lock itself cannot be rolled back without the allocation and will be released at file or connection teardown. Fix cases 1 and 2 by hoisting the locks_free_lock()/kfree() to before the if(!rc) check in the UNLOCK branch so all exit paths share one free site, and by freeing smb_lock and flock before goto out in the non-UNLOCK branch. Propagate the correct error code in both cases. Fix case 3 by wrapping the VFS unlock in an if(rlock) guard and adding a NULL check for locks_free_lock(rlock) in the shared cleanup. Found via call-graph analysis using sqry.	7.5	More Details

CVE-2026-33077	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to version 8.2.6.4, the oldconfig parameter in the haproxy_section_save interface has an arbitrary file read vulnerability. Version 8.2.6.4 fixes the issue.	7.5	More Details
CVE-2026-41405	OpenClaw before 2026.3.31 parses MS Teams webhook request bodies before performing JWT validation, allowing unauthenticated attackers to trigger resource exhaustion. Remote attackers can send malicious Teams webhook payloads to exhaust server resources by bypassing authentication checks.	7.5	More Details
CVE-2026-33662	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. From 3.8.0 to 4.10, in the function emsa_pkcs1_v1_5_encode() in core/drivers/crypto/crypto_api/acipher/rsassa.c, the amount of padding needed, "PS size", is calculated by subtracting the size of the digest and other fields required for the EMA-PKCS1-v1_5 encoding from the size of the modulus of the key. By selecting a small enough modulus, this subtraction can overflow. The padding is added as a string of 0xFF bytes with a call to memset(), and an underflowed integer will cause the memset() call to overwrite until OP-TEE crashes. This only affects platforms registering RSA acceleration.	7.5	More Details
CVE-2026-34065	nimiq-primitives contains primitives (e.g., block, account, transaction) to be used in Nimiq's Rust implementation. Prior to version 1.3.0, an untrusted p2p peer can cause a node to panic by announcing an election macro block whose `validators` set contains an invalid compressed BLS voting key. Hashing an election macro header hashes `validators` and reaches `Validators::voting_keys()`, which calls `validator.voting_key.uncompress().unwrap()` and panics on invalid bytes. The patch for this vulnerability is included as part of v1.3.0. No known workarounds are available.	7.5	More Details
CVE-2026-41395	OpenClaw before 2026.3.28 contains a webhook replay vulnerability in Plivo V3 signature verification that canonicalizes query ordering for signatures but hashes raw URLs for replay detection. Attackers can reorder query parameters to bypass replay cache detection and trigger duplicate voice-call processing with a captured valid signed webhook.	7.5	More Details
CVE-2026-41324	basic-ftp is an FTP client for Node.js. Versions prior to 5.3.0 are vulnerable to denial of service through unbounded memory growth while processing directory listings from a remote FTP server. A malicious or compromised server can send an extremely large or never-ending listing response to `Client.list()`, causing the client process to consume memory until it becomes unstable or crashes. Version 5.3.0 fixes the issue.	7.5	More Details
CVE-2025-67223	The Aranda File Server (AFS) component in Aranda Software Aranda Service Desk before 8.3.12 stores daily activity logs with predictable names in a publicly accessible directory, which allows unauthenticated remote attackers to obtain direct virtual paths of uploaded files and bypass access controls to download sensitive documents containing PII.	7.5	More Details
CVE-2026-6947	DWM-222W USB Wi-Fi Adapter developed by D-Link has a Brute-Force Protection Bypass vulnerability, allowing unauthenticated adjacent network attackers to bypass login attempt limits to perform brute-force attacks to gain control over the device.	7.5	More Details
CVE-2026-31600	In the Linux kernel, the following vulnerability has been resolved: arm64: mm: Handle invalid large leaf mappings correctly It has been possible for a long time to mark ptes in the linear map as invalid. This is done for secretmem, kfence, realm dma memory un/share, and others, by simply clearing the PTE_VALID bit. But until commit a166563e7ec37 ("arm64: mm: support large block mapping when rodata=full") large leaf mappings were never made invalid in this way. It turns out various parts of the code base are not equipped to handle invalid large leaf mappings (in the way they are currently encoded) and I've observed a kernel panic while booting a realm guest on a BBML2_NOABORT system as a result: [15.432706] software IO TLB: Memory encryption is active and system is using DMA bounce buffers [15.476896] Unable to handle kernel paging request at virtual address ffff000019600000 [15.513762] Mem abort info: [15.527245] ESR = 0x0000000096000046 [15.548553] EC = 0x25: DABT (current EL), IL = 32 bits [15.572146] SET = 0, FnV = 0 [15.592141] EA = 0, S1PTW = 0 [15.612694] FSC = 0x06: level 2 translation fault [15.640644] Data abort info: [15.661983] ISV = 0, ISS = 0x00000046, ISS2 = 0x00000000 [15.694875] CM = 0, WnR = 1, TnD = 0, TagAccess = 0 [15.723740] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [15.755776] swapper pgtable: 4k pages, 48-bit VAs, pgdp=0000000081f3f000 [15.800410] [ffff000019600000] pgd=0000000000000000, p4d=180000009ffff403, pud=180000009fffe403, pmd=00e8000199600704 [15.855046] Internal error: Oops: 0000000096000046 [#1] SMP [15.886394] Modules linked in: [15.900029] CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 7.0.0-rc4-dirty #4 PREEMPT [15.935258] Hardware name: linux,dummy-virt (DT) [15.955612] pstate: 21400005 (nzCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) [15.986009] pc : __pi_memcpy_generic+0x128/0x22c [16.006163] lr : swiotlb_bounce+0xf4/0x158 [16.024145] sp : ffff80008000b8f0 [16.038896] x29: ffff80008000b8f0 x28: 0000000000000000 x27: 0000000000000000 [16.069953] x26: ffffb3976d261ba8 x25: 0000000000000000 x24: ffff000019600000 [16.100876] x23: 0000000000000001 x22: ffff0000043430d0 x21: 0000000000007ff0 [16.131946] x20: 0000000084570010 x19: 0000000000000000 x18: ffff00001ffe3fcc [16.163073] x17: 0000000000000000 x16: 00000000003fffff x15: 646e612065766974 [16.194131] x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 [16.225059] x11: 0000000000000000 x10: 0000000000000010 x9 : 0000000000000018 [16.256113] x8 : 0000000000000018 x7 : 0000000000000000 x6 : 0000000000000000 [16.287203] x5 : ffff000019607ff0 x4 : ffff000004578000 x3 : ffff000019600000 [16.318145] x2 : 0000000000007ff0 x1 : ffff000004570010 x0 : ffff000019600000 [16.349071] Call trace: [16.360143] __pi_memcpy_generic+0x128/0x22c (P) [16.380310] swiotlb_tbl_map_single+0x154/0x2b4 [16.400282] swiotlb_map+0x5c/0x228 [16.415984] dma_map_phys+0x244/0x2b8 [16.432199] dma_map_page_attrs+0x44/0x58 [16.449782] virtqueue_map_page_attrs+0x38/0x44 [16.469596] virtqueue_map_single_attrs+0xc0/0x130 [16.490509] virtnet_rq_alloc.isra.0+0xa4/0x1fc [16.510355] try_fill_recv+0x2a4/0x584 [16.526989] virtnet_open+0xd4/0x238 [16.542775] __dev_open+0x110/0x24c [16.558280] __dev_change_flags+0x194/0x20c [16.576879] netif_change_flags+0x24/0x6c [16.594489] dev_change_flags+0x48/0x7c [16.611462] ip_auto_config+0x258/0x1114 [16.628727] do_one_initcall+0x80/0x1c8 [16.645590] kernel_init_freeable+0x208/0x2f0 [16.664917] kernel_init+0x24/0x1e0 [16.680295] ret_from_fork+0x10/0x20 [16.696369] Code: 927cec03 cb0e0021 8b0e0042 a9411c26 (a900340c) [16.723106] ---[end trace 0000000000000000]--- [16.752866] Kernel panic - not syncing: Attempted to kill init! exitcode=0x0000000b [16.792556] Kernel Offset: 0x3396ea200000 from 0xffff8000800000 ---truncated---	7.5	More Details
	free5GC UDR is the Policy Control Function (PCF) for free5GC, an an open-source project for 5th generation (5G) mobile core networks. A memory leak vulnerability in versions prior to 1.4.3 allows any unauthenticated attacker with network access to		

CVE-2026-41135	the PCF SBI interface to cause uncontrolled memory growth by sending repeated HTTP requests to the OAM endpoint. The root cause is a `router.Use()` call inside an HTTP handler that registers a new CORS middleware on every incoming request, permanently growing the Gin router's handler chain. This leads to progressive memory exhaustion and eventual Denial of Service of the PCF, preventing all UEs from obtaining AM and SM policies and blocking 5G session establishment. Version 1.4.3 contains a patch.	7.5	More Details
CVE-2026-3621	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.4 IBM WebSphere Application Server Liberty is vulnerable to identity spoofing under limited conditions when an application is deployed without authentication and authorization configured.	7.5	More Details
CVE-2026-6857	A flaw was found in camel-infinispan. This vulnerability involves unsafe deserialization in the ProtoStream remote aggregation repository. A remote attacker with low privileges could exploit this by sending specially crafted data, leading to arbitrary code execution. This allows the attacker to gain full control over the affected system, impacting its confidentiality, integrity, and availability.	7.5	More Details
CVE-2026-42039	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, toFormData recursively walks nested objects with no depth limit, so a deeply nested value passed as request data crashes the Node.js process with a RangeError. This vulnerability is fixed in 1.15.1 and 0.31.1.	7.5	More Details
CVE-2026-34063	Nimiq's network-libp2p is a Nimiq network implementation based on libp2p. Prior to version 1.3.0, `network-libp2p` discovery uses a libp2p `ConnectionHandler` state machine. the handler assumes there is at most one inbound and one outbound discovery substream per connection. if a remote peer opens/negotiate the discovery protocol substream a second time on the same connection, the handler hits a `panic!(\"Inbound already connected\")` / `panic!(\"Outbound already connected\")` path instead of failing closed. This causes a remote crash of the networking task (swarm), taking the node's p2p networking offline until restart. The patch for this vulnerability is formally released as part of v1.3.0. No known workarounds are available.	7.5	More Details
CVE-2018-25294	CEWE Photoshow 6.3.4 contains a buffer overflow vulnerability in the login dialog that allows attackers to crash the application by submitting oversized input. Attackers can inject 4000 bytes of data into the email address and password fields to trigger a denial of service condition.	7.5	More Details
CVE-2026-41416	PJSIP is a free and open source multimedia communication library written in C. In 2.16 and earlier, there is an integer overflow in media stream buffer size calculation when processing SDP with asymmetric ptime configuration. The overflow may result in an undersized buffer allocation, which can lead to unexpected application termination or memory corruption This vulnerability is fixed in 2.17.	7.5	More Details
CVE-2026-41180	PsiTransfer is an open source, self-hosted file sharing solution. Prior to version 2.4.3, the upload PATCH flow under `/files/:uploadId` validates the mounted request path using the still-encoded `req.path`, but the downstream tus handler later writes using the decoded `req.params.uploadId`. In deployments that use a supported custom `PSITRANSFER_UPLOAD_DIR` whose basename prefixes a startup-loaded JavaScript path, such as `conf`, an unauthenticated attacker can create `config.<NODE_ENV>.js` in the application root. The attacker-controlled file is then executed on the next process restart. Version 2.4.3 contains a patch.	7.5	More Details
CVE-2026-31598	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix possible deadlock between unlink and dio_end_io_write ocfs2_unlink takes orphan dir inode_lock first and then ip_alloc_sem, while in ocfs2_dio_end_io_write, it acquires these locks in reverse order. This creates an ABBA lock ordering violation on lock classes ocfs2_sysfile_lock_key[ORPHAN_DIR_SYSTEM_INODE] and ocfs2_file_ip_alloc_sem_key. Lock Chain #0 (orphan dir inode_lock -> ip_alloc_sem): ocfs2_unlink ocfs2_prepare_orphan_dir ocfs2_lookup_lock_orphan_dir inode_lock(orphan_dir_inode) <- lock A __ocfs2_prepare_orphan_dir ocfs2_prepare_dir_for_insert ocfs2_extend_dir ocfs2_expand_inline_dir down_write(&oi->ip_alloc_sem) <- Lock B Lock Chain #1 (ip_alloc_sem -> orphan dir inode_lock): ocfs2_dio_end_io_write down_write(&oi->ip_alloc_sem) <- Lock B ocfs2_del_inode_from_orphan() inode_lock(orphan_dir_inode) <- Lock A Deadlock Scenario: CPU0 (unlink) CPU1 (dio_end_io_write) ------ ------ inode_lock(orphan_dir_inode) down_write(ip_alloc_sem) down_write(ip_alloc_sem) inode_lock(orphan_dir_inode) Since ip_alloc_sem is to protect allocation changes, which is unrelated with operations in ocfs2_del_inode_from_orphan. So move ocfs2_del_inode_from_orphan out of ip_alloc_sem to fix the deadlock.	7.5	More Details
CVE-2026-33666	Zserio is a framework for serializing structured data with a compact and efficient way with low overhead. Prior to 2.18.1, in BitStreamReader.h readBytes() / readString(), the setBitPosition() bounds check receives the overflowed value and is completely bypassed. The code then reads len bytes (512 MB) from a buffer that is only a few bytes long, causing a segmentation fault. This vulnerability is fixed in 2.18.1.	7.5	More Details
CVE-2026-21728	Tempo queries with large limits can cause large memory allocations which can impact the availability of the service, depending on its deployment strategy. Mitigation can be done by setting max_result_limit in the search config, e.g. to 262144 (2^18).	7.5	More Details
CVE-2026-31563	In the Linux kernel, the following vulnerability has been resolved: net: macb: Use dev_consume_skb_any() to free TX SKBs The napi_consume_skb() function is not intended to be called in an IRQ disabled context. However, after commit 6bc8a5098bf4 ("net: macb: Fix tx_ptr_lock locking"), the freeing of TX SKBs is performed with IRQs disabled. To resolve the following call trace, use dev_consume_skb_any() for freeing TX SKBs: WARNING: kernel/softirq.c:430 at __local_bh_enable_ip+0x174/0x188, CPU#0: ksoftirqd/0/15 Modules linked in: CPU: 0 UID: 0 PID: 15 Comm: ksoftirqd/0 Not tainted 7.0.0-rc4-next-20260319-yocto-standard-dirty #37 PREEMPT Hardware name: ZynqMP ZCU102 Rev1.1 (DT) pstate: 200000c5 (nzCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __local_bh_enable_ip+0x174/0x188 lr : local_bh_enable+0x24/0x38 sp : ffff800082b3bb10 x29: ffff800082b3bb10 x28: ffff0008031f3c00 x27: 000000000011ede0 x26: ffff000800a7ff00 x25: ffff800083937ce8 x24: 0000000000017a80 x23: ffff000803243a78 x22: 0000000000000040 x21: 0000000000000000 x20: ffff000800394c80 x19: 0000000000000200 x18: 0000000000000001 x17: 0000000000000001 x16: ffff000803240000 x15: 0000000000000000 x14: ffffffffffffffff x13: 0000000000000028 x12: ffff000800395650 x11: ffff8000821d1528 x10: ffff800081c2bc08 x9 : ffff800081c1e258 x8 : 0000000100000301 x7 : ffff8000810426ec x6 : 0000000000000000 x5 : 0000000000000001 x4 : 0000000000000001 x3 : 0000000000000000 x2 : 0000000000000008 x1 : 0000000000000200 x0 : ffff8000810428dc Call trace: __local_bh_enable_ip+0x174/0x188 (P) local_bh_enable+0x24/0x38 skb_attempt_defer_free+0x190/0x1d8 napi_consume_skb+0x58/0x108	7.5	More Details

	macb_tx_poll+0x1a4/0x558 __napi_poll+0x50/0x198 net_rx_action+0x1f4/0x3d8 handle_softirqs+0x16c/0x560 run_ksoftirqd+0x44/0x80 smpboot_thread_fn+0x1d8/0x338 kthread+0x120/0x150 ret_from_fork+0x10/0x20 irq event stamp: 29751 hardirqs last enabled at (29750): [<ffff8000813be184>] _raw_spin_unlock_irqrestore+0x44/0x88 hardirqs last disabled at (29751): [<ffff8000813bdf60>] _raw_spin_lock_irqsave+0x38/0x98 softirqs last enabled at (29150): [<ffff8000800f1aec>] handle_softirqs+0x504/0x560 softirqs last disabled at (29153): [<ffff8000800f2fec>] run_ksoftirqd+0x44/0x80		
CVE-2026-31662	In the Linux kernel, the following vulnerability has been resolved: tipc: fix bc_ackers underflow on duplicate GRP_ACK_MSG The GRP_ACK_MSG handler in tipc_group_proto_rcv() currently decrements bc_ackers on every inbound group ACK, even when the same member has already acknowledged the current broadcast round. Because bc_ackers is a u16, a duplicate ACK received after the last legitimate ACK wraps the counter to 65535. Once wrapped, tipc_group_bc_cong() keeps reporting congestion and later group broadcasts on the affected socket stay blocked until the group is recreated. Fix this by ignoring duplicate or stale ACKs before touching bc_acked or bc_ackers. This makes repeated GRP_ACK_MSG handling idempotent and prevents the underflow path.	7.5	More Details
CVE-2026-7320	Information disclosure due to incorrect boundary conditions in the Audio/Video component. This vulnerability was fixed in Firefox 150.0.1, Firefox ESR 140.10.1, and Firefox ESR 115.35.1.	7.5	More Details
CVE-2026-41205	Mako is a template library written in Python. Prior to 1.3.11, TemplateLookup.get_template() is vulnerable to path traversal when a URI starts with // (e.g., //../../../secret.txt). The root cause is an inconsistency between two slash-stripping implementations. Any file readable by the process can be returned as rendered template content when an application passes untrusted input directly to TemplateLookup.get_template(). This vulnerability is fixed in 1.3.11.	7.5	More Details
CVE-2026-40972	An attacker on the same network as the remote application may be able to utilize a timing attack to discover information about the remote secret. In extreme circumstances this could result in the attacker determining the secret and uploading changed classes, thereby achieving remote code execution in the remote application. Affected: Spring Boot 4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14), 3.4.0–3.4.15 (fix 3.4.16), 3.3.0–3.3.18 (fix 3.3.19), 2.7.0–2.7.32 (fix 2.7.33); DevTools remote secret comparison. Versions that are no longer supported are also affected per vendor advisory.	7.5	More Details
CVE-2026-7040	Text::Minify::XS versions from v0.3.0 before v0.7.8 for Perl have a heap overflow when processing some malformed UTF-8 characters. The minify functions mishandled some malformed UTF-8 characters, leading to heap corruption. Note that the minify_utf8 function is an alias for minify.	7.5	More Details
CVE-2026-33593	A client can trigger a divide by zero error leading to crash by sending a crafted DNSCrypt query.	7.5	More Details
CVE-2026-41259	Mastodon is a free, open-source social network server based on ActivityPub. Prior to v4.5.9, v4.4.16, and v4.3.22, Mastodon allows restricting new user sign-up based on e-mail domain names, and performs basic validation on e-mail addresses, but fails to restrict characters that are interpreted differently by some mailing servers. This vulnerability is fixed in v4.5.9, v4.4.16, and v4.3.22.	7.5	More Details
CVE-2026-6022	In Progress® Telerik® UI for AJAX prior to 2026.1.421, RadAsyncUpload contains an uncontrolled resource consumption vulnerability that allows file uploads to exceed the configured maximum size due to missing cumulative size enforcement during chunk reassembly, leading to disk space exhaustion.	7.5	More Details
CVE-2026-31552	In the Linux kernel, the following vulnerability has been resolved: wifi: wlcore: Return -ENOMEM instead of -EAGAIN if there is not enough headroom Since upstream commit e75665dd0968 ("wifi: wlcore: ensure skb headroom before skb_push"), wl1271_tx_allocate() and with it wl1271_prepare_tx_frame() returns -EAGAIN if pskb_expand_head() fails. However, in wlcore_tx_work_locked(), a return value of -EAGAIN from wl1271_prepare_tx_frame() is interpreted as the aggregation buffer being full. This causes the code to flush the buffer, put the skb back at the head of the queue, and immediately retry the same skb in a tight while loop. Because wlcore_tx_work_locked() holds wl->mutex, and the retry happens immediately with GFP_ATOMIC, this will result in an infinite loop and a CPU soft lockup. Return -ENOMEM instead so the packet is dropped and the loop terminates. The problem was found by an experimental code review agent based on gemini-3.1-pro while reviewing backports into v6.18.y.	7.5	More Details
CVE-2026-31638	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Only put the call ref if one was acquired rxrpc_input_packet_on_conn() can process a to-client packet after the current client call on the channel has already been torn down. In that case chan->call is NULL, rxrpc_try_get_call() returns NULL and there is no reference to drop. The client-side implicit-end error path does not account for that and unconditionally calls rxrpc_put_call(). This turns a protocol error path into a kernel crash instead of rejecting the packet. Only drop the call reference if one was actually acquired. Keep the existing protocol error handling unchanged.	7.5	More Details
CVE-2026-31640	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix use of wrong skb when comparing queued RESP challenge serial In rxrpc_post_response(), the code should be comparing the challenge serial number from the cached response before deciding to switch to a newer response, but looks at the newer packet private data instead, rendering the comparison always false. Fix this by switching to look at the older packet. Fix further[1] to substitute the new packet in place of the old one if newer and also to release whichever we don't use.	7.5	More Details
CVE-2026-41066	lxml is a library for processing XML and HTML in the Python language. Prior to 6.1.0, using either of the two parsers in the default configuration (with resolve_entities=True) allows untrusted XML input to read local files. Setting the resolve_entities option explicitly to resolve_entities='internal' or resolve_entities=False disables the local file access. This vulnerability is fixed in 6.1.0.	7.5	More Details
CVE-2026-30350	An issue in the /store/items/search endpoint of Agent Protocol server commit e9a89f allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details

CVE-2026-31539	In the Linux kernel, the following vulnerability has been resolved: smb: smbdirect: introduce smbdirect_socket.recv_io.credits.available The logic off managing recv credits by counting posted recv_io and granted credits is racy. That's because the peer might already consumed a credit, but between receiving the incoming recv at the hardware and processing the completion in the 'recv_done' functions we likely have a window where we grant credits, which don't really exist. So we better have a decicated counter for the available credits, which will be incremented when we posted new recv buffers and drained when we grant the credits to the peer.	7.5	More Details
CVE-2026-30351	A path traversal vulnerability in the UI/static component of leonvanzyl autocoder commit 79d02a allows attackers to read arbitrary files via sending crafted URL path containing traversal sequences.	7.5	More Details
CVE-2026-31538	In the Linux kernel, the following vulnerability has been resolved: smb: server: make use of smbdirect_socket.recv_io.credits.available The logic off managing recv credits by counting posted recv_io and granted credits is racy. That's because the peer might already consumed a credit, but between receiving the incoming recv at the hardware and processing the completion in the 'recv_done' functions we likely have a window where we grant credits, which don't really exist. So we better have a decicated counter for the available credits, which will be incremented when we posted new recv buffers and drained when we grant the credits to the peer. This fixes regression Namjae reported with the 6.18 release.	7.5	More Details
CVE-2025-48431	Mismatched Memory Management Routines vulnerability in Apache Thrift c_glib language bindings. This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue. Description: Specially crafted requests can crash an c_glib-based Thrift server with a clean but fatal "free(): invalid pointer" error message.	7.5	More Details
CVE-2026-41680	Marked is a markdown parser and compiler. From 18.0.0 to 18.0.1, a critical Denial of Service (DoS) vulnerability exists in marked. By providing a specific 3-byte input sequence a tab, a vertical tab, and a newline (\x09\x0b\n)—an unauthenticated attacker can trigger an infinite recursion loop during parsing. This leads to unbounded memory allocation, causing the host Node.js application to crash via Memory Exhaustion (OOM). This vulnerability is fixed in 18.0.2.	7.5	More Details
CVE-2026-41266	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, /api/v1/public-chatbotConfig/:id ep exposes sensitive data including API keys, HTTP authorization headers and internal configuration without any authentication. An attacker with knowledge just of a chatflow UUID can retrieve credentials stored in password type fields and HTTP headers, leading to credential theft and more. This vulnerability is fixed in 3.1.0.	7.5	More Details
CVE-2026-41602	Integer Overflow or Wraparound vulnerability in Apache Thrift TFramedTransport Go language implementation This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	7.5	More Details
CVE-2026-22754	Vulnerability in Spring Spring Security. If an application uses <sec:intercept-url servlet-path="/servlet-path" pattern="/endpoint/**"/> to define the servlet path for computing a path matcher, then the servlet path is not included and the related authorization rules are not exercised. This can lead to an authorization bypass.This issue affects Spring Security: from 7.0.0 through 7.0.4.	7.5	More Details
CVE-2026-41279	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the text-to-speech generation endpoint (POST /api/v1/text-to-speech/generate) is whitelisted (no auth) and accepts a credentialId directly in the request body. When called without a chatflowId, the endpoint uses the provided credentialId to decrypt the stored credential (e.g., OpenAI or ElevenLabs API key) and generate speech. This vulnerability is fixed in 3.1.0.	7.5	More Details
CVE-2026-41278	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the GET /api/v1/public-chatflows/:id endpoint returns the full chatflow object without sanitization for public chatflows. Docker validation revealed this is worse than initially assessed: the sanitizeFlowDataForPublicEndpoint function does NOT exist in the released v3.0.13 Docker image. Both public-chatflows AND public-chatbotConfig return completely raw flowData including credential IDs, plaintext API keys, and password-type fields. This vulnerability is fixed in 3.1.0.	7.5	More Details
CVE-2026-31557	In the Linux kernel, the following vulnerability has been resolved: nvmet: move async event work off nvmet-wq For target nvmet_ctrl_free() flushes ctrl->async_event_work. If nvmet_ctrl_free() runs on nvmet-wq, the flush re-enters workqueue completion for the same worker:- A. Async event work queued on nvmet-wq (prior to disconnect): nvmet_execute_async_event() queue_work(nvmet_wq, &ctrl->async_event_work) nvmet_add_async_event() queue_work(nvmet_wq, &ctrl->async_event_work) B. Full pre-work chain (RDMA CM path): nvmet_rdma_cm_handler() nvmet_rdma_queue_disconnect() __nvmet_rdma_queue_disconnect() queue_work(nvmet_wq, &queue->release_work) process_one_work() lock((wq_completion)nvmet-wq) <--------- 1st nvmet_rdma_release_queue_work() C. Recursive path (same worker): nvmet_rdma_release_queue_work() nvmet_rdma_free_queue() nvmet_sq_destroy() nvmet_ctrl_put() nvmet_ctrl_free() flush_work(&ctrl->async_event_work) __flush_work() touch_wq_lockdep_map() lock((wq_completion)nvmet-wq) <--------- 2nd Lockdep splat: == WARNING: possible recursive locking detected 6.19.0-rc3nvme+ #14 Tainted: G N -- kworker/u192:42/44933 is trying to acquire lock: ffff888118a00948 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: touch_wq_lockdep_map+0x26/0x90 but task is already holding lock: ffff888118a00948 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x53e/0x660 3 locks held by kworker/u192:42/44933: #0: ffff888118a00948 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x53e/0x660 #1: ffffc9000e6cbe28 ((work_completion)(&queue->release_work)){+.+.}-{0:0}, at: process_one_work+0x1c5/0x660 #2: ffffffff82d4db60 (rcu_read_lock){....}-{1:3}, at: __flush_work+0x62/0x530 Workqueue: nvmet-wq nvmet_rdma_release_queue_work [nvmet_rdma] Call Trace: __flush_work+0x268/0x530 nvmet_ctrl_free+0x140/0x310 [nvmet] nvmet_cq_put+0x74/0x90 [nvmet] nvmet_rdma_free_queue+0x23/0xe0 [nvmet_rdma] nvmet_rdma_release_queue_work+0x19/0x50 [nvmet_rdma] process_one_work+0x206/0x660 worker_thread+0x184/0x320 kthread+0x10c/0x240 ret_from_fork+0x319/0x390 Move async event work to a dedicated nvmet-aen-wq to avoid reentrant flush on nvmet-wq.	7.5	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: rxrpc: only handle RESPONSE during service challenge Only process RESPONSE packets while the service connection is still in RXRPC_CONN_SERVICE_CHALLENGING. Check that		More

2026-31676	state under state_lock before running response verification and security initialization, then use a local secured flag to decide whether to queue the secured-connection work after the state transition. This keeps duplicate or late RESPONSE packets from re-running the setup path and removes the unlocked post-transition state test.	7.5	Details
CVE-2026-22753	Vulnerability in Spring Spring Security. If an application is using securityMatchers(String) and a PathPatternRequestMatcher.Builder bean to prepend a servlet path, matching requests to that filter chain may fail and its related security components will not be exercised as intended by the application. This can lead to the authentication, authorization, and other security controls being rendered inactive on intended requests.This issue affects Spring Security: from 7.0.0 through 7.0.4.	7.5	More Details
CVE-2026-41275	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the password reset functionality on cloud.flowiseai.com sends a reset password link over the unsecured HTTP protocol instead of HTTPS. This behavior introduces the risk of a man-in-the-middle (MITM) attack, where an attacker on the same network as the user (e.g., public Wi-Fi) can intercept the reset link and gain unauthorized access to the victim’s account. This vulnerability is fixed in 3.1.0.	7.5	More Details
CVE-2026-31635	In the Linux kernel, the following vulnerability has been resolved: rxrpc: fix oversized RESPONSE authenticator length check rxgk_verify_response() decodes auth_len from the packet and is supposed to verify that it fits in the remaining bytes. The existing check is inverted, so oversized RESPONSE authenticators are accepted and passed to rxgk_decrypt_skb(), which can later reach skb_to_sgvec() with an impossible length and hit BUG_ON(len). Decoded from the original latest-net reproduction logs with scripts/decode_stacktrace.sh: RIP: __skb_to_sgvec() [net/core/skbuff.c:5285 (discriminator 1)] Call Trace: skb_to_sgvec() [net/core/skbuff.c:5305] rxgk_decrypt_skb() [net/rxrpc/rxgk_common.h:81] rxgk_verify_response() [net/rxrpc/rxgk.c:1268] rxrpc_process_connection() [net/rxrpc/conn_event.c:266 net/rxrpc/conn_event.c:364 net/rxrpc/conn_event.c:386] process_one_work() [kernel/workqueue.c:3281] worker_thread() [kernel/workqueue.c:3353 kernel/workqueue.c:3440] kthread() [kernel/kthread.c:436] ret_from_fork() [arch/x86/kernel/process.c:164] Reject authenticator lengths that exceed the remaining packet payload.	7.5	More Details
CVE-2026-33608	An attacker can send a notify request that causes a new secondary domain to be added to the bind backend, but causes said backend to update its configuration to an invalid one, leading to the backend no longer able to run on the next restart, requiring manual operation to fix it.	7.4	More Details
CVE-2026-41603	Improper Validation of Certificate with Host Mismatch vulnerability in Apache Thrift. This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	7.4	More Details
CVE-2026-42033	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, when Object.prototype has been polluted by any co-dependency with keys that axios reads without a hasOwnProperty guard, an attacker can (a) silently intercept and modify every JSON response before the application sees it, or (b) fully hijack the underlying HTTP transport, gaining access to request credentials, headers, and body. The precondition is prototype pollution from a separate source in the same process. This vulnerability is fixed in 1.15.1 and 0.31.1.	7.4	More Details
CVE-2026-41414	Skim is a fuzzy finder designed to through files, lines, and commands. The generate-files job in .github/workflows/pr.yml checks out attacker-controlled fork code and executes it via cargo run, with access to SKIM_RS_BOT_PRIVATE_KEY and GITHUB_TOKEN (contents:write). No gates prevent exploitation - any GitHub user can trigger this by opening a pull request from a fork. This vulnerability is fixed with commit bf63404ad51985b00ed304690ba9d477860a5a75.	7.4	More Details
CVE-2026-42035	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, a prototype pollution gadget exists in the Axios HTTP adapter (lib/adapters/http.js) that allows an attacker to inject arbitrary HTTP headers into outgoing requests. The vulnerability exploits duck-type checking of the data payload, where if Object.prototype is polluted with getHeaders, append, pipe, on, once, and Symbol.toStringTag, Axios misidentifies any plain object payload as a FormData instance and calls the attacker-controlled getHeaders() function, merging the returned headers into the outgoing request. The vulnerable code resides exclusively in lib/adapters/http.js. The prototype pollution source does not need to originate from Axios itself — any prototype pollution primitive in any dependency in the application's dependency tree is sufficient to trigger this gadget. This vulnerability is fixed in 1.15.1 and 0.31.1.	7.4	More Details
CVE-2026-7025	A vulnerability was found in Typecho up to 1.3.0. This vulnerability affects the function Service::sendPingHandle of the file var/Widget/Service.php of the component Ping Back Service Endpoint. The manipulation of the argument X-Pingback/link results in server-side request forgery. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-7036	A vulnerability was identified in Tenda i9 1.0.0.5(2204). This vulnerability affects the function R7WebsSecurityHandlerfunction of the component HTTP Handler. The manipulation leads to path traversal. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-41380	OpenClaw before 2026.3.28 contains an execution approval vulnerability in exec-approvals-allowlist.ts that allows allow-always persistence to trust wrapper carrier executables instead of invoked targets. Attackers can exploit positional carrier executable routing through dispatch wrappers to establish broader allowlist entries than intended, weakening execution approval boundaries.	7.3	More Details
CVE-2026-41390	OpenClaw before 2026.3.28 contains an exec allowlist bypass vulnerability where allow-always persistence fails to unwrap /usr/bin/script and similar wrappers before storing trust decisions. Attackers can obtain user approval for one wrapped command to persist trust for wrapper binaries that execute different underlying programs.	7.3	More Details
CVE-2026-41355	OpenShell before 2026.3.28 contains an arbitrary code execution vulnerability in mirror mode that converts untrusted sandbox files into workspace hooks. Attackers with mirror mode access can execute arbitrary code on the host during gateway startup by exploiting enabled workspace hooks.	7.3	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Handle the case that EIOINTC's coremap is empty EIOINTC's coremap in eiointc_update_sw_coremap() can be empty, currently we get a cpuid with -1 in this case, but we actually need 0 because it's similar as the case that cpuid >= 4. This fix an out-of-bounds access to	7.3	More Details

31569	kvm_arch::phyid_map::phys_map[].		
CVE-2026-6977	A security vulnerability has been detected in vanna-ai vanna up to 2.0.2. The affected element is an unknown function of the component Legacy Flask API. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-5935	IBM Total Storage Service Console (TSSC) / TS4500 IMC 9.2, 9.3, 9.4, 9.5, 9.6 TSSC/IMC could allow an unauthenticated user to execute arbitrary commands with normal user privileges on the system due to improper validation of user supplied input.	7.3	More Details
CVE-2026-6980	A vulnerability has been found in Divyanshu-hash GitPilot-MCP up to 9ed9f153ba4158a2ad230ee4871b25130da29ffd. This impacts the function repo_path of the file main.py. Such manipulation of the argument command leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-7042	A flaw has been found in 666ghj MiroFish up to 0.1.2. This affects the function create_app of the file backend/app/__init__.py of the component REST API Endpoint. Executing a manipulation can lead to missing authentication. It is possible to launch the attack remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-41342	OpenClaw before 2026.3.28 contains an authentication bypass vulnerability in the remote onboarding component that persists unauthenticated discovery endpoints without explicit trust confirmation. Attackers can spoof discovery endpoints to redirect onboarding toward malicious gateways and capture gateway credentials or traffic.	7.3	More Details
CVE-2025-70994	Yadea T5 Electric Bicycles (models manufactured in/after 2024) have a weak authentication mechanism in their keyless entry system. The system utilizes the EV1527 fixed-code RF protocol without implementing rolling codes or cryptographic challenge-response mechanisms. This is vulnerable to signal forgery after a local attacker intercepts any legitimate key fob transmission, allowing for complete unauthorized vehicle operation via a replay attack.	7.3	More Details
CVE-2026-7002	A vulnerability was determined in KLiK SocialMediaWebsite up to 1.0.1. This vulnerability affects unknown code of the file /includes/get_message_ajax.php of the component Private Message Handler. Executing a manipulation of the argument c_id can lead to sql injection. It is possible to launch the attack remotely.	7.3	More Details
CVE-2026-7022	A security vulnerability has been detected in SmythOS sre up to 0.0.15. Affected is the function AgentRuntime of the file packages/core/src/subsystems/AgentManager/AgentRuntime.class.ts of the component HTTP Header Handler. Such manipulation of the argument X-DEBUG-RUN/X-DEBUG-INJ leads to improper authentication. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6987	A vulnerability was detected in PicoClaw up to 0.2.4. Impacted is an unknown function of the file /api/gateway/restart of the component Web Launcher Management Plane. Performing a manipulation results in command injection. It is possible to initiate the attack remotely. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7064	A flaw has been found in AgentDeskAI browser-tools-mcp up to 1.2.0. This issue affects some unknown processing of the file browser-tools-server/browser-connector.ts. Executing a manipulation can lead to os command injection. The attack may be performed from remote. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7216	A weakness has been identified in donchelo processing-claude-mcp-bridge up to e017b20a4b592a45531a6392f494007f04e661bd. Impacted is an unknown function of the file processing_server.py of the component create_sketch Tool. This manipulation of the argument sketch_name causes path traversal. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7077	A vulnerability was identified in itsourcecode Courier Management System 1.0. The affected element is an unknown function of the file /edit_parcel.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-7314	A vulnerability was detected in eiceblue spire-doc-mcp-server 1.0.0. This affects the function get_doc_path of the file src/spire_doc_mcp/api/base.py. Performing a manipulation of the argument document_name results in path traversal. The attack can be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7221	A vulnerability was found in TencentCloudBase CloudBase-MCP up to 2.17.0. Affected is the function openUrl of the file mcp/src/interactive-server.ts of the component open-url API Endpoint. The manipulation of the argument req.body.url results in server-side request forgery. It is possible to launch the attack remotely. The exploit has been made public and could be used. Upgrading to version 2.17.1 is able to address this issue. The patch is identified as 3f678a1e7bd400cd76469d61024097d4920dc6b5. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2026-7088	A weakness has been identified in SourceCodester Pharmacy Sales and Inventory System 1.0. The affected element is an unknown function of the file /ajax.php?action=save_receiving. Executing a manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-	A security flaw has been discovered in SourceCodester Pharmacy Sales and Inventory System 1.0. Impacted is an unknown function of the file /ajax.php?action=save_sales. Performing a manipulation of the argument ID results in sql injection. The	7.3	More

7087	attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.		Details
CVE-2026-7223	A vulnerability was identified in BigSweetPotatoStudio HyperChat up to 2.0.0-alpha.63. Affected by this issue is the function fetch of the file packages/core/src/http/aiProxyMiddleware.mts of the component AI Proxy Middleware. Such manipulation of the argument baseurl leads to server-side request forgery. The attack can be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7147	A vulnerability was detected in JoeCastrom mcp-chat-studio up to 1.5.0. Affected by this issue is some unknown functionality of the file server/routes/llm.js of the component LLM Models API. Performing a manipulation of the argument req.query.base_url results in server-side request forgery. Remote exploitation of the attack is possible. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7146	A security vulnerability has been detected in AlejandroArciniegas mcp-data-vis up to de5a51525a69822290eaee569a1ab447b490746d. Affected by this vulnerability is the function axios of the file src/servers/web-scraper/server.js of the component HTTP Request Handler. Such manipulation leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7076	A vulnerability was determined in itsourcecode Courier Management System 1.0. Impacted is an unknown function of the file /edit_branch.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-7315	A flaw has been found in eiceblue spire-pdf-mcp-server 0.1.1. This impacts the function get_pdf_path of the file src/spire_pdf_mcp/server.py of the component PDF File Handler. Executing a manipulation of the argument filepath can lead to path traversal. The attack can be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7225	A weakness has been identified in SourceCodester Pizzafy Ecommerce System 1.0. This vulnerability affects the function delete_menu of the file /admin/ajax.php?action=delete_menu. Executing a manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-7226	A security vulnerability has been detected in SourceCodester Pizzafy Ecommerce System 1.0. This issue affects the function login2 of the file /admin/ajax.php?action=login2. The manipulation of the argument e-mail leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-7075	A vulnerability was found in itsourcecode Construction Management System 1.0. This issue affects some unknown processing of the file /locations.php. Performing a manipulation of the argument address results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-7074	A vulnerability has been found in itsourcecode Construction Management System 1.0. This vulnerability affects unknown code of the file /execute1.php. Such manipulation of the argument code leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-7227	A vulnerability was detected in SourceCodester Pizzafy Ecommerce System 1.0. Impacted is the function Login of the file /admin/ajax.php?action=login. The manipulation of the argument e-mail results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-7228	A flaw has been found in SourceCodester Pizzafy Ecommerce System 1.0. The affected element is the function get_cart_count of the file /admin/ajax.php?action=get_cart_count. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-7234	A weakness has been identified in BrowserOperator browser-operator-core up to 0.6.0. Affected is the function startsWith of the file scripts/component_server/server.js. Executing a manipulation of the argument request.url can lead to path traversal. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7220	A vulnerability has been found in jackwrichards FastlyMCP up to 6f3d0b0e654fc51076badc7fa16c03c461f95620. This impacts an unknown function of the file fastly-mcp.mjs of the component fastly_cli Tool. The manipulation of the argument command leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7215	A security flaw has been discovered in egtai gmx-vmd-mcp up to 0.1.0. This issue affects the function launch_vmd_gui_tool of the file mcp_server.py of the component VMD Launch Handler. The manipulation of the argument structure_file/trajectory_file results in command injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7072	A vulnerability was detected in CodePanda Source canteen_management_system 1.0. Affected by this issue is some unknown functionality of the file /api/login.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-	A vulnerability was detected in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_product. Performing a manipulation of the argument ID results	7.3	More Details

7199	in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.		
CVE-2026-7177	A security flaw has been discovered in ChatGPTNextWeb NextChat up to 2.16.1. Affected by this issue is the function proxyHandler of the file app/api/[provider]/[...path]/route.ts. The manipulation results in server-side request forgery. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7178	A weakness has been identified in ChatGPTNextWeb NextChat up to 2.16.1. This affects the function storeUrl of the file app/api/artifacts/route.ts of the component Artifacts Endpoint. This manipulation of the argument ID causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7194	A weakness has been identified in SourceCodester Pharmacy Sales and Inventory System 1.0. This impacts an unknown function of the file /ajax.php?action=save_product. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-7158	A vulnerability has been found in dmitryglhf mcp-url-downloader up to 4b8cf2de55f6e8864a77d108e8a94a5b8e4394c6. Affected by this issue is the function _validate_url_safe of the file src/mcp_url_downloader/server.py. Such manipulation of the argument url leads to server-side request forgery. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-35338	A vulnerability in the chmod utility of uutils coreutils allows users to bypass the --preserve-root safety mechanism. The implementation only validates if the target path is literally / and does not canonicalize the path. An attacker or accidental user can use path variants such as /../ or symbolic links to execute destructive recursive operations (e.g., chmod -R 000) on the entire root filesystem, leading to system-wide permission loss and potential complete system breakdown.	7.3	More Details
CVE-2026-7157	A flaw has been found in disler aider-mcp-server up to b2516fa466d0d851932da92ee6d0e66946db9efc. Affected by this vulnerability is an unknown functionality of the file src/aider_mcp_server/server.py of the component aider_ai_code. This manipulation of the argument relative_editable_files causes command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7319	A flaw has been found in elinsky execution-system-mcp 0.1.0. The impacted element is the function _get_context_file_path of the file src/execution_system_mcp/server.py of the component add_action Tool. This manipulation of the argument context causes path traversal. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-7149	A vulnerability has been found in dexhunter kaggle-mcp up to 406127ffcb2b91b8c10e20e6c2ca787fbc1dc92d. This vulnerability affects the function prepare_kaggle_dataset of the file src/kaggle_mcp/server.py. The manipulation of the argument competition_id leads to path traversal. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7214	A vulnerability was identified in eghuzefa engineer-your-data up to 0.1.3. This vulnerability affects the function read_file/write_file/list_files/file_inf of the file src/server.py. The manipulation of the argument WORKSPACE_PATH leads to path traversal. The attack may be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7205	A vulnerability was identified in duartium papers-mcp-server 9ceb3812a6458ba7922ca24a7406f8807bc55598. Impacted is the function search_papers of the file src/main.py. Such manipulation of the argument topic leads to path traversal. The attack may be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7206	A security flaw has been discovered in dubydu sqlite-mcp up to 0.1.0. The affected element is the function extract_to_json of the file src/entry.py. Performing a manipulation of the argument output_filename results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The patch is named a5580cb992f4f6c308c9ffe6442b2e76709db548. Applying a patch is the recommended action to fix this issue.	7.3	More Details
CVE-2026-7211	A weakness has been identified in dvladimirov MCP up to 0.1.0. The impacted element is the function GitSearchRequest of the file mcp_server.py of the component Git Search API. Executing a manipulation of the argument repo_url/pattern can lead to command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7212	A security vulnerability has been detected in edvardlindelof notes-mcp up to 0.1.4. This affects an unknown function of the file notes_mcp.py. The manipulation of the argument root_dir/path leads to path traversal. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7094	A vulnerability was determined in ShadowCloneLabs GlutamateMCPServers up to e2de73280b01e5d943593dd1aa2c01c5b9112f78. Affected by this issue is some unknown functionality of the file src/puppeteer/index.ts of the component puppeteer_navigate. Executing a manipulation of the argument url can lead to server-side request forgery. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details

CVE-2026-7316	A vulnerability has been found in eiliyaabedini aider-mcp up to 667b914301aada695aab0e46d1fb3a7d5e32c8af. Affected is an unknown function of the file aider_mcp.py of the component code_with_ai. The manipulation of the argument working_dir/editable_files leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7213	A vulnerability was detected in ef10007 MLOps_MCP 1.0.0. This impacts an unknown function of the file fastmcp_server.py of the component save_file Tool. The manipulation of the argument filename/destination results in path traversal. The attack may be performed from remote. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7073	A flaw has been found in itsourcecode Construction Management System 1.0. This affects an unknown part of the file /execute.php. This manipulation of the argument code causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-7224	A security flaw has been discovered in SourceCodester Pizzafy Ecommerce System 1.0. This affects the function delete_cart of the file /admin/ajax.php?action=delete_cart. Performing a manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-7070	A weakness has been identified in code-projects Inventory Management System 1.0. Affected is an unknown function of the component Login. Executing a manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-7061	A weakness has been identified in Toowiredd chatgpt-mcp-server up to 0.1.0. Affected by this issue is some unknown functionality of the file src/services/docker.service.ts of the component MCP/HTTP. This manipulation causes os command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7127	A weakness has been identified in SourceCodester Pharmacy Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_receiving. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-7065	A vulnerability has been found in BidingCC BuildingAI up to 26.0.1. Impacted is the function uploadRemoteFile of the file packages/core/src/modules/upload/services/file-storage.service.ts of the component Remote Upload API. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7128	A security vulnerability has been detected in SourceCodester Pharmacy Sales and Inventory System 1.0. This issue affects some unknown processing of the file /ajax.php?action=save_type. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-7063	A vulnerability was detected in code-projects Employee Management System 1.0. This vulnerability affects unknown code of the file /370project/process/eprocess.php of the component Endpoint. Performing a manipulation of the argument pwd results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-7062	A security vulnerability has been detected in Intina47 context-sync up to 2.0.0. This affects an unknown part of the file src/git-integration.ts of the component Git Integration. Such manipulation leads to os command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-41605	Integer Overflow or Wraparound vulnerability in Apache Thrift. This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	7.3	More Details
CVE-2026-7130	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. The affected element is an unknown function of the file /ajax.php?action=delete_category. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	7.3	More Details
CVE-2026-7126	A security flaw has been discovered in SourceCodester Pharmacy Sales and Inventory System 1.0. This affects an unknown part of the file /ajax.php?action=save_category. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-7131	A vulnerability has been found in code-projects Online Lot Reservation System up to 1.0. The impacted element is an unknown function of the file /loginuser.php. The manipulation of the argument email/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-7060	A vulnerability was determined in liyupi yu-picture up to a053632c41340152bf75b66b3c543d129123d8ec. This impacts the function PageRequest of the file yu-picture-backend/src/main/java/com/yupi/yupicturebackend/service/impl/PictureServiceImpl.java of the component MyBatis-Plus. Executing a manipulation of the argument sortField can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. Applying a patch is advised to resolve this issue. The project was informed of the problem early through a pull request but has not reacted yet.	7.3	More Details
CVE-2026-5435	The deprecated functions ns_printrrf, ns_printrr and fp_nquery in the GNU C Library version 2.2 and newer fail to enforce the caller-supplied buffer length, and can result in an out-of-bounds write when printing TSIG records.	7.3	More Details

CVE-2026-7324	Memory safety bugs present in Firefox 150.0.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 150.0.1.	7.3	More Details
CVE-2026-7272	A flaw has been found in WilliamCloudQi matlab-mcp-server up to ab88f6b9bf5f36f725e8628029f7f6dd0d9913ca. The affected element is the function generate_matlab_code/execute_matlab_code of the file src/index.ts of the component MCP Interface. Executing a manipulation of the argument scriptPath can lead to path traversal. The attack can be executed remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7058	A vulnerability has been found in 666ghj MiroFish up to 0.1.2. The impacted element is the function SimulationIPCClient.send_command of the file backend/app/services/simulation_ipc.py of the component Inter-Process Communication. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7066	A vulnerability was found in choieastsea simple-openstack-mcp up to 767b2f4a8154cca344344b9725537a58399e6036. The affected element is the function exec_openstack of the file server.py. The manipulation results in os command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7159	A vulnerability was found in douinc mkdocs-mcp-plugin up to 0.4.1. This affects the function read_document/list_documents of the file server.py. Performing a manipulation of the argument docs_dir/file_path results in path traversal. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor confirms, that the "fix will be published within a few days."	7.3	More Details
CVE-2026-40542	Missing critical step in authentication in Apache HttpClient 5.6 allows an attacker to cause the client to accept SCRAM-SHA-256 authentication without proper mutual authentication verification. Users are recommended to upgrade to version 5.6.1, which fixes this issue.	7.3	More Details
CVE-2026-7237	A vulnerability was detected in AgiFlow scaffold-mcp up to 1.0.27. Affected by this issue is some unknown functionality of the file packages/scaffold-mcp/src/server/index.ts of the component write-to-file Tool. The manipulation of the argument file_path results in path traversal. The attack may be launched remotely. The exploit is now public and may be used. Upgrading to version 1.1.0 can resolve this issue. The patch is identified as c4d23592ae5fb59cfeefc4641e6826f8ac89b9c6. You should upgrade the affected component.	7.3	More Details
CVE-2026-7322	Memory safety bugs present in Firefox ESR 115.35.0, Firefox ESR 140.10.0 and Firefox 150.0.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 150.0.1, Firefox ESR 140.10.1, and Firefox ESR 115.35.1.	7.3	More Details
CVE-2026-7323	Memory safety bugs present in Firefox ESR 140.10.0 and Firefox 150.0.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 150.0.1 and Firefox ESR 140.10.1.	7.3	More Details
CVE-2026-7067	A vulnerability was determined in D-Link DIR-822 A_101. The impacted element is the function system of the file /udhcpcd/dhcpd.c of the component udhcpd DHCP Service. This manipulation of the argument Hostname causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-33733	EspoCRM is an open source customer relationship management application. Prior to version 9.3.4, the admin template management endpoints accept attacker-controlled `name` and `scope` values and pass them into template path construction without normalization or traversal filtering. As a result, an authenticated admin can use `../` sequences to escape the intended template directory and read, create, overwrite, or delete arbitrary files that resolve to `body.tpl` or `subject.tpl` under the web application user's filesystem permissions. Version 9.3.4 fixes the issue.	7.2	More Details
CVE-2026-7218	A vulnerability was detected in Totolink N300RT 3.4.0-B20250430. The impacted element is the function is_cmd_string_valid of the file /boafrm/formWsc of the component libapmib.so. Performing a manipulation of the argument localPin results in buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.2	More Details
CVE-2026-7219	A flaw has been found in Totolink N300RT 3.4.0-B20250430. This affects an unknown function of the file /boafrm/formIpQoS. Executing a manipulation of the argument entry_name can lead to buffer overflow. The attack may be performed from remote. The exploit has been published and may be used.	7.2	More Details
CVE-2026-7247	A vulnerability has been found in D-Link DI-8100 16.07.26A1. Affected by this issue is the function file_exten_asp of the file file_exten.asp of the component File Extension Handler. The manipulation of the argument Name leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.2	More Details
CVE-2026-4132	The HTTP Headers plugin for WordPress is vulnerable to External Control of File Name or Path leading to Remote Code Execution in all versions up to and including 1.19.2. This is due to insufficient validation of the file path stored in the 'hh_htpasswd_path' option and lack of sanitization on the 'hh_www_authenticate_user' option value. The plugin allows administrators to set an arbitrary file path for the htpasswd file location and does not validate that the path has a safe file extension (e.g., restricting to .htpasswd). Additionally, the username field used for HTTP Basic Authentication is written directly into the file without sanitization. The apache_auth_credentials() function constructs the file content using the unsanitized username via sprintf('%s:{SHA}%s', $user, ...), and update_auth_credentials() writes this content to the attacker-controlled path via file_put_contents(). This makes it possible for authenticated attackers, with Administrator-level access and above, to write arbitrary content (including PHP code) to arbitrary file paths on the server, effectively achieving Remote Code Execution.	7.2	More Details

CVE-2026-42043	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, an attacker who can influence the target URL of an Axios request can use any address in the 127.0.0.0/8 range (other than 127.0.0.1) to completely bypass the NO_PROXY protection. This vulnerability is due to an incomplete for CVE-2025-62718, This vulnerability is fixed in 1.15.1 and 0.31.1.	7.2	More Details
CVE-2026-1460	A post-authentication command injection vulnerability in the “DomainName” parameter of the DHCP configuration file in Zyxel DX3301-T0 and EX3301-T0 firmware versions through 5.50(ABVY.7.1)C0 could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device.	7.2	More Details
CVE-2026-5464	The ExactMetrics – Google Analytics Dashboard for WordPress (Website Stats Plugin) plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation and activation in all versions up to, and including, 9.1.2. This is due to the reports page exposing the 'onboarding_key' transient to any user with the 'exactmetrics_view_dashboard' capability. This key is the sole authorization gate for the '/wp-json/exactmetrics/v1/onboarding/connect-url' REST endpoint, which returns a one-time hash (OTH) token. This OTH token is then the only credential checked by the 'exactmetrics_connect_process' AJAX endpoint — which has no capability check, no nonce verification, and accepts an arbitrary plugin ZIP URL via the file parameter for installation and activation. This makes it possible for authenticated attackers, with Editor-level access and above granted the report viewing permission, to install and activate arbitrary plugins from attacker-controlled URLs, leading to Remote Code Execution.	7.2	More Details
CVE-2026-7191	Improper use of the static-eval npm package in the open source solution qnabot-on-aws versions 7.2.4 and earlier may allow an authenticated administrator to execute arbitrary code within the fulfillment Lambda execution context by injecting a crafted conditional chaining expression via the Content Designer interface, which bypasses the intended expression sandbox through JavaScript prototype manipulation. This may grant direct access to backend resources (Lambda environment variables, OpenSearch indices, S3 objects, DynamoDB tables) that are not exposed through normal administrative interfaces. We recommend you upgrade to version 7.3.0 or above.	7.2	More Details
CVE-2026-42255	Technitium DNS Server before 15.0 allows DNS traffic amplification via cyclic name server delegation.	7.2	More Details
CVE-2026-6992	A vulnerability was identified in Linksys MR9600 2.0.6.206937. This affects the function BTRequestGetSmartConnectStatus of the file /etc/init.d/run_central2.sh of the component JNAP Action Handler. The manipulation of the argument pin leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2026-6855	A flaw was found in InstructLab. A local attacker could exploit a path traversal vulnerability in the chat session handler by manipulating the `logs_dir` parameter. This allows the attacker to create new directories and write files to arbitrary locations on the system, potentially leading to unauthorized data modification or disclosure.	7.1	More Details
CVE-2026-41379	OpenClaw before 2026.3.28 contains a privilege escalation vulnerability allowing authenticated operators with write permissions to access admin-class Talk Voice configuration persistence. Attackers with operator.write privileges can exploit the chat.send endpoint to reach and modify sensitive voice configuration settings intended for administrators only.	7.1	More Details
CVE-2026-41359	OpenClaw before 2026.3.28 contains a privilege escalation vulnerability allowing authenticated operators with write permissions to access admin-class Telegram configuration and cron persistence settings via the send endpoint. Attackers with operator.write credentials can exploit insufficient access controls to reach sensitive administrative functionality and modify persistence mechanisms.	7.1	More Details
CVE-2026-34414	Xerte Online Toolkits versions 3.15 and earlier contain a relative path traversal vulnerability in the elFinder connector endpoint at /editor/elfinder/php/connector.php where the name parameter in rename commands is not sanitized for path traversal sequences. Attackers can supply a name value containing directory traversal sequences to move files from project media directories to arbitrary locations on the filesystem, potentially overwriting application files, achieving stored cross-site scripting, or combining with other vulnerabilities to achieve unauthenticated remote code execution by moving PHP code files to the application root.	7.1	More Details
CVE-2026-35341	A vulnerability in uutils coreutils mkfifo allows for the unauthorized modification of permissions on existing files. When mkfifo fails to create a FIFO because a file already exists at the target path, it fails to terminate the operation for that path and continues to execute a follow-up set_permissions call. This results in the existing file's permissions being changed to the default mode (often 644 after umask), potentially exposing sensitive files such as SSH private keys to other users on the system.	7.1	More Details
CVE-2026-31568	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Add missing secure storage access fixups for donated memory There are special cases where secure storage access exceptions happen in a kernel context for pages that don't have the PG_arch_1 bit set. That bit is set for non-exported guest secure storage (memory) but is absent on storage donated to the Ultravisor since the kernel isn't allowed to export donated pages. Prior to this patch we would try to export the page by calling arch_make_folio_accessible() which would instantly return since the arch bit is absent signifying that the page was already exported and no further action is necessary. This leads to secure storage access exception loops which can never be resolved. With this patch we unconditionally try to export and if that fails we fixup.	7.1	More Details
CVE-2026-41272	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the core security wrappers (secureAxiosRequest and secureFetch) intended to prevent Server-Side Request Forgery (SSRF) contain multiple logic flaws. These flaws allow attackers to bypass the allow/deny lists via DNS Rebinding (Time-of-Check Time-of-Use) or by exploiting the default configuration which fails to enforce any deny list. This vulnerability is fixed in 3.1.0.	7.1	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: hwmon: (pmbus/core) Protect regulator operations with mutex The regulator operations pmbus_regulator_get_voltage(), pmbus_regulator_set_voltage(), and pmbus_regulator_list_voltage() access PMBus registers and shared data but were not protected by the update_lock mutex. This could lead to race conditions. However, adding mutex protection directly to these functions causes a deadlock because pmbus_regulator_notify() (which calls regulator_notifier_call_chain()) is often called with the mutex already held (e.g., from	7.1	More

31486	pmbus_fault_handler()). If a regulator callback then calls one of the now-protected voltage functions, it will attempt to acquire the same mutex. Rework pmbus_regulator_notify() to utilize a worker function to send notifications outside of the mutex protection. Events are stored as atomics in a per-page bitmask and processed by the worker. Initialize the worker and its associated data during regulator registration, and ensure it is cancelled on device removal using devm_add_action_or_reset(). While at it, remove the unnecessary include of linux/of.h.		Details
CVE-2026-28747	A weak key generation vulnerability exists in specific firmware versions of Milesight AIOT cameras allows authorization to be bypassed.	7.1	More Details
CVE-2026-41270	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, a Server-Side Request Forgery (SSRF) protection bypass vulnerability exists in the Custom Function feature. While the application implements SSRF protection via HTTP_DENY_LIST for axios and node-fetch libraries, the built-in Node.js http, https, and net modules are allowed in the NodeVM sandbox without equivalent protection. This allows authenticated users to bypass SSRF controls and access internal network resources (e.g., cloud provider metadata services) This vulnerability is fixed in 3.1.0.	7.1	More Details
CVE-2026-31484	In the Linux kernel, the following vulnerability has been resolved: io_uring/fdinfo: fix OOB read in SQE_MIXED wrap check __io_uring_show_fdinfo() iterates over pending SQEs and, for 128-byte SQEs on an IORING_SETUP_SQE_MIXED ring, needs to detect when the second half of the SQE would be past the end of the sq_sqes array. The current check tests (++sq_head & sq_mask) == 0, but sq_head is only incremented when a 128-byte SQE is encountered, not on every iteration. The actual array index is sq_idx = (i + sq_head) & sq_mask, which can be sq_mask (the last slot) while the wrap check passes. Fix by checking sq_idx directly. Keep the sq_head increment so the loop still skips the second half of the 128-byte SQE on the next iteration.	7.1	More Details
CVE-2026-42429	OpenClaw before 2026.4.8 contains a privilege escalation vulnerability in the gateway plugin HTTP authentication mechanism that widens identity-bearing operator.read requests into runtime operator.write permissions. Attackers can exploit this by sending read-scoped requests through the gateway auth route to gain unauthorized write access to runtime operations.	7.1	More Details
CVE-2026-41269	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the Chatflow configuration file upload settings can be modified to allow the application/javascript MIME type. This lets an attacker upload .js files even though the frontend doesn't normally allow JavaScript uploads. This enables attackers to persistently store malicious Node.js web shells on the server, potentially leading to Remote Code Execution (RCE). This vulnerability is fixed in 3.1.0.	7.1	More Details
CVE-2026-31470	In the Linux kernel, the following vulnerability has been resolved: virt: tdx-guest: Fix handling of host controlled 'quote' buffer length Validate host controlled value `quote_buf->out_len` that determines how many bytes of the quote are copied out to guest userspace. In TDX environments with remote attestation, quotes are not considered private, and can be forwarded to an attestation server. Catch scenarios where the host specifies a response length larger than the guest's allocation, or otherwise races modifying the response while the guest consumes it. This prevents contents beyond the pages allocated for `quote_buf` (up to TSM_REPORT_OUTBLOB_MAX) from being read out to guest userspace, and possibly forwarded in attestation requests. Recall that some deployments want per-container configs-tsm-report interfaces, so the leak may cross container protection boundaries, not just local root.	7.1	More Details
CVE-2026-6940	radare2 prior to 6.1.4 contains a path traversal vulnerability in project deletion that allows local attackers to recursively delete arbitrary directories by supplying absolute paths that escape the configured dir.projects root directory. Attackers can craft absolute paths to project marker files outside the project storage boundary to cause recursive deletion of attacker-chosen directories with permissions of the radare2 process, resulting in integrity and availability loss.	7.1	More Details
CVE-2026-41347	OpenClaw before 2026.3.31 lacks browser-origin validation in HTTP operator endpoints when operating in trusted-proxy mode, allowing cross-site request forgery attacks. Attackers can exploit this by sending malicious requests from a browser in trusted-proxy deployments to perform unauthorized actions on HTTP operator endpoints.	7.1	More Details
CVE-2026-31679	In the Linux kernel, the following vulnerability has been resolved: openvswitch: validate MPLS set/set_masked payload length validate_set() accepted OVS_KEY_ATTR_MPLS as variable-sized payload for SET/SET_MASKED actions. In action handling, OVS expects fixed-size MPLS key data (struct ovs_key_mpls). Use the already normalized key_len (masked case included) and reject non-matching MPLS action key sizes. Reject invalid MPLS action payload lengths early.	7.1	More Details
CVE-2026-31674	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6t_rt: reject oversized addrnr in rt_mt6_check() Reject rt match rules whose addrnr exceeds IP6T_RT_HOPS. rt_mt6() expects addrnr to stay within the bounds of rtinfo->addrs[]. Validate addrnr during rule installation so malformed rules are rejected before the match logic can use an out-of-range value.	7.1	More Details
CVE-2026-41361	OpenClaw before 2026.3.28 contains an SSRF guard bypass vulnerability that fails to block four IPv6 special-use ranges. Attackers can exploit this by crafting URLs targeting internal or non-routable IPv6 addresses to bypass SSRF protections.	7.1	More Details
CVE-2026-42428	OpenClaw versions before 2026.4.8 fail to enforce integrity verification on downloaded plugin archives. Attackers can install malicious or tampered plugin packages without detection, compromising the local assistant environment.	7.1	More Details
CVE-2026-31626	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: initialize le_tmp64 in rtw_BIP_verify() Initialize le_tmp64 to zero in rtw_BIP_verify() to prevent using uninitialized data. Smatch warns that only 6 bytes are copied to this 8-byte (u64) variable, leaving the last two bytes uninitialized: drivers/staging/rtl8723bs/core/rtw_security.c:1308 rtw_BIP_verify() warn: not copying enough bytes for '&le_tmp64' (8 vs 6 bytes) Initializing the variable at the start of the function fixes this warning and ensures predictable behavior.	7.1	More Details
CVE-	A Time-of-Check to Time-of-Use (TOCTOU) race condition exists in the mkfifo utility of uutils coreutils. The utility creates a FIFO and then performs a path-based chmod to set permissions. A local attacker with write access to the parent directory		More

2026-35352	can swap the newly created FIFO for a symbolic link between these two operations. This redirects the chmod call to an arbitrary file, potentially enabling privilege escalation if the utility is run with elevated privileges.	7.0	Details
CVE-2026-41166	OpenRemote is an open-source internet-of-things platform. Prior to version 1.22.1, a user who has `write:admin` in one Keycloak realm can call the Manager API to update Keycloak realm roles for users in another realm, including `master`. The handler uses the `{realm}` path segment when talking to the identity provider but does not check that the caller may administer that realm. This could result in a privilege escalation to `master` realm administrator if the attacker controls any user in `master` realm. Version 1.22.1 fixes the issue.	7.0	More Details
CVE-2026-3006	Successful exploitation of the race condition vulnerability could allow an attacker to trigger a kernel heap overflow, potentially leading to local privilege escalation and granting system-level access to the affected software.	7.0	More Details
CVE-2026-40973	A local attacker on the same host as the application may be able to take control of the directory used by `ApplicationTemp`. When `server.servlet.session.persistent` is set to `true` and the attack persists across application restarts, this may allow the attacker to read session information and hijack authenticated users or deploy a gadget chain and execute code as the application's user. Affected: Spring Boot 4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14), 3.4.0–3.4.15 (fix 3.4.16), 3.3.0–3.3.18 (fix 3.3.19), 2.7.0–2.7.32 (fix 2.7.33); predictable temp directory / `ApplicationTemp` ownership verification. Versions that are no longer supported are also affected per vendor advisory.	7.0	More Details
CVE-2026-41238	DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Versions 3.0.1 through 3.3.3 are vulnerable to a prototype pollution-based XSS bypass. When an application uses `DOMPurify.sanitize()` with the default configuration (no `CUSTOM_ELEMENT_HANDLING` option), a prior prototype pollution gadget can inject permissive `tagNameCheck` and `attributeNameCheck` regex values into `Object.prototype`, causing DOMPurify to allow arbitrary custom elements with arbitrary attributes — including event handlers — through sanitization. Version 3.4.0 fixes the issue.	6.9	More Details
CVE-2026-41239	DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Starting in version 1.0.10 and prior to version 3.4.0, `SAFE_FOR_TEMPLATES` strips `{{...}}` expressions from untrusted HTML. This works in string mode but not with `RETURN_DOM` or `RETURN_DOM_FRAGMENT`, allowing XSS via template-evaluating frameworks like Vue 2. Version 3.4.0 patches the issue.	6.8	More Details
CVE-2026-32649	A command injection vulnerability exists in the web server of specific firmware versions of Milesight cameras.	6.8	More Details
CVE-2026-41397	OpenClaw before 2026.3.31 contains a sandbox escape vulnerability allowing attackers to traverse directory boundaries through symlink exploitation during file synchronization operations. Remote attackers can bypass sandbox restrictions by crafting malicious symlinks in mirror sync operations to access arbitrary files outside intended boundaries.	6.8	More Details
CVE-2026-28525	SWUpdate contains an integer underflow vulnerability in the multipart upload parser in mongoose_multipart.c that allows unauthenticated attackers to cause a denial of service by sending a crafted HTTP POST request to /upload with a malformed multipart boundary and controlled TCP stream timing. Attackers can trigger an integer underflow in the mg_http_multipart_continue_wait_for_chunk() function when the buffer length falls within a specific range, causing an out-of-bounds heap read that writes data beyond the allocated receive buffer to a local IPC socket.	6.8	More Details
CVE-2026-34068	nimiq-transaction provides the transaction primitive to be used in Nimiq's Rust implementation. Prior to version 1.3.0, the staking contract accepts `UpdateValidator` transactions that set `new_voting_key=Some(...)` while omitting `new_proof_of_knowledge`. this skips the proof-of-knowledge requirement that is needed to prevent BLS rogue-key attacks when public keys are aggregated. Because tendermint macro block justification verification aggregates validator voting keys and verifies a single aggregated BLS signature against that aggregate public key, a rogue-key voting key in the validator set can allow an attacker to forge a quorum-looking justification while only producing a single signature. While the impact is critical, the exploitability is low: The voting keys are fixed for the epoch, so the attacker would need to know the next epoch validator set (chosen through VRF), which is unlikely. The patch for this vulnerability is included as part of v1.3.0. No known workarounds are available.	6.8	More Details
CVE-2026-22747	Vulnerability in Spring Spring Security. SubjectX500PrincipalExtractor does not correctly handle certain malformed X.509 certificate CN values, which can lead to reading the wrong value for the username. In a carefully crafted certificate, this can lead to an attacker impersonating another user. This issue affects Spring Security: from 7.0.0 through 7.0.4.	6.8	More Details
CVE-2026-0711	A post-authentication command injection vulnerability in the EasyMesh-related APIs of Zyxel DX3300-T0 firmware versions through 5.50(ABVY.7.1)C0 could allow an authenticated, adjacent attacker with administrator privileges to execute OS commands on an affected device.	6.8	More Details
CVE-2026-42038	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, he fix for no_proxy hostname normalization bypass is incomplete. When no_proxy=localhost is set, requests to 127.0.0.1 and [::1] still route through the proxy instead of bypassing it. The shouldBypassProxy() function does pure string matching — it does not resolve IP aliases or loopback equivalents. This vulnerability is fixed in 1.15.1 and 0.31.1.	6.8	More Details
CVE-2026-41360	OpenClaw before 2026.4.2 contains an approval integrity vulnerability in pnpm dlx that fails to bind local script operands consistently with pnpm exec flows. Attackers can replace approved local scripts before execution without invalidating the approval plan, allowing execution of modified script contents.	6.7	More Details
CVE-2026-25908	Dell Alienware Command Center (AWCC), versions prior to 6.13.8.0, contain an Execution with Unnecessary Privileges vulnerability in the AWCC. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	6.7	More Details
CVE-2026-41989	Libgcrypt before 1.12.2 sometimes allows a heap-based buffer overflow and denial of service via crafted ECDH ciphertext to gcry_pk_decrypt.	6.7	More Details

CVE-2026-7280	AVACAST developed by eMPIA Technology has a Unquoted Service Path vulnerability, allowing privileged local attackers to place a malicious executable file in a specific directory, resulting in arbitrary code execution with system privileges when the AVACAST service starts.	6.7	More Details
CVE-2026-35349	A vulnerability in the rm utility of uutils coreutils allows a bypass of the --preserve-root protection. The implementation uses a path-string check rather than comparing device and inode numbers to identify the root directory. An attacker or accidental user can bypass this safeguard by using a symbolic link that resolves to the root directory (e.g., /tmp/rootlink -> /), potentially leading to the unintended recursive deletion of the entire root filesystem.	6.7	More Details
CVE-2026-41392	OpenClaw before 2026.3.31 contains an exec allowlist bypass vulnerability allowing attackers to inherit allowlist trust via shell init-file wrapper invocations. Attackers can exploit shell options like --rcfile, --init-file, and --startup-file to load attacker-chosen initialization files while bypassing exec allowlist matching restrictions.	6.7	More Details
CVE-2026-41411	Vim is an open source, command line text editor. Prior to 9.2.0357, A command injection vulnerability exists in Vim's tag file processing. When resolving a tag, the filename field from the tags file is passed through wildcard expansion to resolve environment variables and wildcards. If the filename field contains backtick syntax (e.g., `command`), Vim executes the embedded command via the system shell with the full privileges of the running user.	6.6	More Details
CVE-2026-3008	Successful exploitation of the string injection vulnerability could allow an attacker to obtain memory address information or crash the application.	6.6	More Details
CVE-2026-35365	The mv utility in uutils coreutils improperly handles directory trees containing symbolic links during moves across filesystem boundaries. Instead of preserving symlinks, the implementation expands them, copying the linked targets as real files or directories at the destination. This can lead to resource exhaustion (disk space or time) if symlinks point to large external directories, unexpected duplication of sensitive data into unintended locations, or infinite recursion and repeated copying in the presence of symlink loops.	6.6	More Details
CVE-2026-40450	Integer overflow in output tensor copy size calculation in Samsung Open Source ONE could cause incorrect copy length and memory corruption for oversized tensors. Affected version is prior to commit 1.30.0.	6.6	More Details
CVE-2026-6941	radare2 prior to 6.1.4 contains a path traversal vulnerability in its project notes handling that allows attackers to read or write files outside the configured project directory by importing a malicious .zrp archive containing a symlinked notes.txt file. Attackers can craft a .zrp archive with a symlinked notes.txt that bypasses directory confinement checks, allowing note operations to follow the symlink and access arbitrary files outside the dir.projects root directory.	6.6	More Details
CVE-2026-41667	Integer overflow in constant tensor data size calculation in Samsung Open Source ONE could cause incorrect buffer sizing for large constant nodes. Affected version is prior to commit 1.30.0.	6.6	More Details
CVE-2026-41664	Integer overflow in memory copy size calculation in Samsung Open Source ONE could lead to invalid memory operations with large tensor shapes. Affected version is prior to commit 1.30.0.	6.6	More Details
CVE-2026-40449	Integer overflow in buffer size calculation could result in out of bounds memory access when handling large tensors in Samsung Open Source ONE. Affected version is prior to commit 1.30.0.	6.6	More Details
CVE-2026-41666	Integer overflow in tensor copy size calculation in Samsung Open Source ONE could lead to out of bounds access during loop state propagation. Affected version is prior to commit 1.30.0.	6.6	More Details
CVE-2026-6839	Improper validation of STRING tensor offsets could allows malformed string metadata to trigger out of bounds access during constant tensor import in Samsung Open Source ONE Affected version is prior to commit 1.30.0.	6.6	More Details
CVE-2026-35350	The cp utility in uutils coreutils fails to properly handle setuid and setgid bits when ownership preservation fails. When copying with the -p (preserve) flag, the utility applies the source mode bits even if the chown operation is unsuccessful. This can result in a user-owned copy retaining original privileged bits, creating unexpected privileged executables that violate local security policies. This differs from GNU cp, which clears these bits when ownership cannot be preserved.	6.6	More Details
CVE-2026-42510	OpenStack Ironic before 35.0.1 allows ipmitool execution in a non-default configuration that has a console interface.	6.6	More Details
CVE-2026-6732	A flaw was found in libxml2. This vulnerability occurs when the library processes a specially crafted XML Schema Definition (XSD) validated document that includes an internal entity reference. An attacker could exploit this by providing a malicious document, leading to a type confusion error that causes the application to crash. This results in a denial of service (DoS), making the affected system or application unavailable.	6.5	More Details
CVE-2026-31192	Insufficient validation of Chrome extension identifiers in Raindrop.io Bookmark Manager Web App 5.6.76.0 allows attackers to obtain sensitive user data via a crafted request.	6.5	More Details
CVE-2026-41526	In KDE KCoreAddons before 6.25, KShell::quoteArgs is intended to safely quote arguments so that they can be passed to a shell command. This parsing does not adequately handle metacharacters, leading to an escape from the shell. All applications relying on this method in a security-critical path to handle user input are affected and could be exploited. In particular, because sendInput() sends a string to a terminal, a control character such as \x01 can be used during injection.	6.5	More Details

CVE-2026-41607	Out-of-bounds Read vulnerability in Apache Thrift. This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	6.5	More Details
CVE-2026-6834	The a+HRD developed by aEnrich has a Missing Authorization vulnerability, allowing authenticated remote attackers to arbitrarily read database contents through a specific API method.	6.5	More Details
CVE-2026-6833	The a+HRD developed by aEnrich has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2026-41127	BigBlueButton is an open-source virtual classroom. Versions prior to 3.0.24 have a missing authorization that allows viewers to inject/overwrite captions Version 3.0.24 tightened the permissions on who is able to submit captions. No known workarounds are available.	6.5	More Details
CVE-2026-40980	In Spring AI, a malicious PDF file can be crafted that triggers the allocation of unreasonable amounts of memory when handled by `ForkPDFLayoutTextStripper`. Affected versions: Spring AI: 1.0.0 - 1.0.5 (fixed in 1.0.6), 1.1.0 - 1.1.4 (fixed in 1.1.5)	6.5	More Details
CVE-2021-36438	SQL Injection vulnerability exists in Sourcecodester Online Job Portal phppdo 1.0 ivia the category parameter in /jobportal/index.php.	6.5	More Details
CVE-2026-41525	KDE Dolphin before 25.12.3 allows applications in a Flatpak (or with AppArmor confinement) to open folders outside of the application sandbox without additional scrutiny. Dolphin's implementation of the FileManager1 protocol allows the path given to be any type of file, including scripts or executables. (By default, Dolphin will then prompt the user to determine if they want to launch a script or executable; however, the intended behavior is to block the attempted action, not present a consent prompt.)	6.5	More Details
CVE-2026-41319	MailKit is a cross-platform mail client library built on top of MimeKit. A STARTTLS Response Injection vulnerability in versions prior to 4.16.0 allows a Man-in-the-Middle attacker to inject arbitrary protocol responses across the plaintext-to-TLS trust boundary, enabling SASL authentication mechanism downgrade (e.g., forcing PLAIN instead of SCRAM-SHA-256). The internal read buffer in `SmtpStream`, `ImapStream`, and `Pop3Stream` is not flushed when the underlying stream is replaced with `SslStream` during STARTTLS upgrade, causing pre-TLS attacker-injected data to be processed as trusted post-TLS responses. Version 4.16.0 patches the issue.	6.5	More Details
CVE-2026-4280	The Breaking News WP plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3. This is due to the brnwp_ajax_form AJAX endpoint lacking both authorization checks and CSRF verification, combined with insufficient path validation when the brnwp_theme option value is passed directly to an include() statement in the brnwp_show_breaking_news_wp() shortcode handler. While sanitize_text_field() is applied to user input, it does not strip directory traversal sequences (../). This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the brnwp_theme option with a directory traversal payload (e.g., ../../../../etc/passwd) and subsequently trigger file inclusion of arbitrary files on the server when the shortcode is rendered.	6.5	More Details
CVE-2025-67259	A Broken Access Control vulnerability exists in ClassroomIO v0.1.13 where an authenticated low-privileged "student" user can access unauthorized course-level information by modifying intercepted API requests. Changing a captured POST request to a GET request against the /rest/v1/course PostgREST endpoint results in disclosure of sensitive information including other students details, tutor/admin profiles, and internal course metadata.	6.5	More Details
CVE-2026-41481	LangChain is a framework for building agents and LLM-powered applications. Prior to langchain-text-splitters 1.1.2, HTMLHeaderTextSplitter.split_text_from_url() validated the initial URL using validate_safe_url() but then performed the fetch with requests.get() with redirects enabled (the default). Because redirect targets were not revalidated, a URL pointing to an attacker-controlled server could redirect to internal, localhost, or cloud metadata endpoints, bypassing SSRF protections. The response body is parsed and returned as Document objects to the calling application code. Whether this constitutes a data exfiltration path depends on the application: if it exposes Document contents (or derivatives) back to the requester who supplied the URL, sensitive data from internal endpoints could be leaked. Applications that store or process Documents internally without returning raw content to the requester are not directly exposed to data exfiltration through this issue. This vulnerability is fixed in 1.1.2.	6.5	More Details
CVE-2026-41388	OpenClaw before 2026.3.31 contains a configuration management vulnerability where startup migration treats empty-array settings as missing values. Attackers can restart the application to rehydrate revoked Tlon configuration from file state, bypassing intended revocation controls.	6.5	More Details
CVE-2026-40099	Kirby is an open-source content management system. Kirby's user permissions control which user role is allowed to perform specific actions to content models in the CMS. These permissions are defined for each role in the user blueprint (`site/blueprints/users/...`). It is also possible to customize the permissions for each target model in the model blueprints (such as in `site/blueprints/pages/...`) using the `options` feature. The permissions and options together control the authorization of user actions. For pages, Kirby provides the `pages.create` and `pages.changeStatus` permissions (among others). Prior to versions 4.9.0 and 5.4.0, Kirby checked these permissions independently and only for the respective action. However the `changeStatus` permission didn't take effect on page creation. New pages are created as drafts by default and need to be published by changing the page status of an existing page draft. This is ensured when the page is created via the Kirby Panel. However the REST API allows to override the `isDraft` flag when creating a new page. This allowed authenticated attackers with the `pages.create` permission to immediately create published pages, bypassing the normal editorial workflow. The problem has been patched in Kirby 4.9.0 and Kirby 5.4.0. Kirby has added a check to the page creation rules that ensures that users without the `pages.changeStatus` permission cannot create published pages, only page drafts.	6.5	More Details
CVE-	When generating an ICMP Destination Unreachable or Packet Too Big response, the handler copies a portion of the original packet into the ICMP error body using the IP header's self-declared total length (ip_tot_len for IPv4, ip6_plen for IPv6)		

2026-5265	without validating it against the actual packet buffer size. A VM can send a short packet with an inflated IP length field that triggers an ICMP error (e.g., by hitting a reject ACL), causing ovn-controller to read heap memory beyond the valid packet data and include it in the ICMP response sent back to the VM.	6.5	More Details
CVE-2026-42044	Axios is a promise based HTTP client for the browser and Node.js. From 1.0.0 to before 1.15.2, he Axios library is vulnerable to a Prototype Pollution "Gadget" attack that allows any Object.prototype pollution in the application's dependency tree to be escalated into surgical, invisible modification of all JSON API responses — including privilege escalation, balance manipulation, and authorization bypass. The default transformResponse function at lib/defaults/index.js:124 calls JSON.parse(data, this.parseReviver), where this is the merged config object. Because parseReviver is not present in Axios defaults, not validated by assertOptions, and not subject to any constraints, a polluted Object.prototype.parseReviver function is called for every key-value pair in every JSON response, allowing the attacker to selectively modify individual values while leaving the rest of the response intact. This vulnerability is fixed in 1.15.2.	6.5	More Details
CVE-2026-41043	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Apache ActiveMQ, Apache ActiveMQ Web. An authenticated attacker can show malicious content when browsing queues in the web console by overriding the content type to be HTML (instead of XML) and by injecting HTML into a JMS selector field. This issue affects Apache ActiveMQ: before 5.19.6, from 6.0.0 before 6.2.5; Apache ActiveMQ Web: before 5.19.6, from 6.0.0 before 6.2.5. Users are recommended to upgrade to version 6.2.5 or 5.19.6, which fixes the issue.	6.5	More Details
CVE-2026-41385	OpenClaw before 2026.3.31 stores Nostr privateKey as plaintext in configuration, allowing exposure through config.get method calls that bypass redaction mechanisms. Attackers can retrieve unredacted configuration data to obtain plaintext signing keys used for Nostr protocol operations.	6.5	More Details
CVE-2026-41370	OpenClaw before 2026.3.31 contains a path traversal vulnerability in ACP dispatch that allows attackers to read arbitrary files by manipulating inbound channel attachment paths. Remote attackers can bypass attachment-cache and root directory checks to access files outside intended directories.	6.5	More Details
CVE-2026-41369	OpenClaw before 2026.3.31 contains insufficient environment variable sanitization in host exec operations, failing to filter package, registry, Docker, compiler, and TLS override variables. Attackers can exploit this by injecting malicious environment variables to override critical system configurations and compromise host execution integrity.	6.5	More Details
CVE-2026-41368	OpenClaw before 2026.3.28 contains an environment variable disclosure vulnerability in the jq safe-bin policy that fails to block the $ENV filter. Attackers can bypass safe-bin restrictions by using $ENV in jq programs to access sensitive environment variables that should be restricted.	6.5	More Details
CVE-2026-41464	ProjeQtor versions 7.0 through 12.4.3 contain a missing authorization vulnerability in the objectDetail.php endpoint that allows authenticated users with guest-level privileges to retrieve sensitive data belonging to other users including password hashes and API keys. Attackers can bypass access controls by directly accessing the endpoint without ownership or role-based validation to extract administrator credentials and perform privilege escalation.	6.5	More Details
CVE-2026-6706	Improper access control in the vault documentation feature in Devolutions Server 2026.1.14.0 and earlier allows an authenticated attacker to read documentation content from unauthorized vaults via a crafted API request.	6.5	More Details
CVE-2026-31164	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the pppoeMtu parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2025-62110	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rescue Themes Rescue Shortcodes allows Stored XSS.This issue affects Rescue Shortcodes: from n/a through 3.3.	6.5	More Details
CVE-2026-33611	An operator allowed to use the REST API can cause the Authoritative server to produce invalid HTTPS or SVCB record data, which can in turn cause LMDB database corruption, if using the LMDB backend.	6.5	More Details
CVE-2026-41911	OpenClaw before 2026.4.8 contains a filesystem policy bypass vulnerability in docx upload processing that allows local file reads outside workspace boundaries. Attackers can exploit upload_file and upload_image endpoints to access files beyond the intended workspace-only filesystem policy.	6.5	More Details
CVE-2026-42410	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for Elementor) allows DOM-Based XSS.This issue affects TheGem Theme Elements (for Elementor): from n/a before 5.12.1.1.	6.5	More Details
CVE-2026-31172	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the user parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-31174	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the informEnable parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-6355	A vulnerability in the web application allows unauthorized users to access and manipulate sensitive data across different tenants by exploiting insecure direct object references. This could lead to unauthorized access to sensitive information and unauthorized changes to the tenant's configuration.	6.5	More Details
CVE-2026-31176	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stun_user parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details

CVE-2026-31179	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunPort parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-28040	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magepeople inc. Taxi Booking Manager for WooCommerce allows Stored XSS.This issue affects Taxi Booking Manager for WooCommerce: from n/a through 2.0.0.	6.5	More Details
CVE-2026-31162	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the ttlWay parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-42430	OpenClaw before 2026.4.8 contains a server-side request forgery vulnerability in Playwright redirect handling that allows attackers to bypass strict SSRF checks. Attackers can exploit request-time navigation to reach private targets that should be restricted by browser SSRF protections.	6.5	More Details
CVE-2026-31163	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the dhcpMtu parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2025-0186	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.6 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed an authenticated user to cause denial of service under certain conditions by exhausting server resources by making crafted requests to a discussions endpoint.	6.5	More Details
CVE-2025-3922	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.4 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed an authenticated user to cause denial of service by overwhelming system resources under certain conditions due to insufficient resource allocation limits in the GraphQL API.	6.5	More Details
CVE-2025-6016	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.2 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed an authenticated user to cause denial of service due to insufficient resource allocation limits when retrieving notes under certain conditions.	6.5	More Details
CVE-2026-31166	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the hour parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-1660	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.3 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that under certain conditions could have allowed an authenticated user to cause denial of service when importing issues due to improper input validation.	6.5	More Details
CVE-2026-32885	DDEV is an open-source tool for running local web development environments for PHP and Node.js. Versions prior to 1.25.2 have unsanitized extraction in both `Untar()` and `Unzip()` functions in `pkg/archive/archive.go`. Downloads and extracts archives from remote sources without path validation. Version 1.25.2 patches the issue.	6.5	More Details
CVE-2026-31167	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the mode parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-31168	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the recHour parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-31169	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the week parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-33602	A rogue backend can send a crafted UDP response with a query ID off by one related to the maximum configured value, triggering an out-of-bounds write leading to a denial of service.	6.5	More Details
CVE-2026-31171	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the url parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-6238	The deprecated functions ns_printrrf, ns_printrr and fp_nquery in the GNU C Library version 2.2 and newer fail to validate the RDATA content against the RDATA length in a DNS response when processing LOC, CERT, TKEY or TSIG records, which may allow an attacker to craft a DNS response, causing a target application to crash or read uninitialized memory. These functions are for application debugging only and hence not in the path of code executed by the DNS resolver. Further, they have been deprecated since version 2.34 and should not be used by any new applications. Applications should consider porting away from these interfaces since they may be removed in future versions.	6.5	More Details
CVE-2026-41312	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions prior to 6.10.2 can craft a PDF which leads to the RAM being exhausted. This requires accessing a stream compressed using `/FlateDecode` with a `/Predictor` unequal 1 and large predictor parameters. This has been fixed in pypdf 6.10.2. As a workaround, one may apply the changes from the patch manually.	6.5	More Details
CVE-2026-41465	ProjeQtor versions 7.0 through 12.4.3 contains a path traversal vulnerability in the log file viewer at dynamicDialog.php where the logname parameter is not validated against directory traversal sequences before constructing file paths. Authenticated attackers can inject directory traversal sequences ../ into the logname parameter to read arbitrary .log files accessible to the web server process on the filesystem.	6.5	More Details

CVE-2026-41313	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions prior to 6.10.2 can craft a PDF which leads to long runtimes. This requires loading a PDF with a large trailer `/Size` value in incremental mode. This has been fixed in pypdf 6.10.2. As a workaround, one may apply the changes from the patch manually.	6.5	More Details
CVE-2026-41314	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions prior to 6.10.2 can craft a PDF which leads to the RAM being exhausted. This requires accessing an image using `/FlateDecode` with large size values. This has been fixed in pypdf 6.10.2. As a workaround, one may apply the changes from the patch manually.	6.5	More Details
CVE-2026-41340	OpenClaw before 2026.3.31 contains an authentication boundary vulnerability where Telegram legacy allowFrom migration incorrectly fans default-account trust into all named accounts. Attackers can exploit this trust propagation to bypass authentication controls and gain unauthorized access to named accounts.	6.5	More Details
CVE-2026-24204	NVIDIA Flare SDK contains a vulnerability where an Attacker may cause an Improper Input Validation by path traversing. A successful exploit of this vulnerability may lead to information disclosure.	6.5	More Details
CVE-2026-41081	Improper Handling of TLS Client Authentication Failure Leading to Anonymous Principal Assignment in Apache Storm Versions Affected: up to 2.8.7 Description: When TLS transport is enabled in Apache Storm without requiring client certificate authentication (the default configuration), the TlsTransportPlugin assigns a fallback principal (CN=ANONYMOUS) if no client certificate is presented or if certificate verification fails. The underlying SSLPeerUnverifiedException is caught and suppressed rather than rejecting the connection. This fail-open behavior means an unauthenticated client can establish a TLS connection and receive a valid principal identity. If the configured authorizer (e.g., SimpleACLAuthorizer) does not explicitly deny access to CN=ANONYMOUS, this may result in unauthorized access to Storm services. The condition is logged at debug level only, reducing visibility in production. Impact: Unauthenticated clients may be assigned a principal identity, potentially bypassing authorization in permissive or misconfigured environments. Mitigation: Users should upgrade to 2.8.7 in which TLS authentication failures are handled in a fail-closed manner. Users who cannot upgrade immediately should: - Enable mandatory client certificate authentication (nimbus.thrift.tls.client.auth.required: true) - Ensure authorization rules explicitly deny access to CN=ANONYMOUS - Review all ACL configurations for implicit default-allow behavior	6.5	More Details
CVE-2026-5926	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	6.5	More Details
CVE-2026-31159	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the password parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-31160	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the provider parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-41334	OpenClaw before 2026.3.31 contains a decompression bomb vulnerability in image processing that fails to properly enforce pixel-limit guards on sips. Attackers can exploit this by uploading oversized images to cause denial of service through excessive memory consumption.	6.5	More Details
CVE-2026-41375	OpenClaw before 2026.3.28 contains an authorization bypass vulnerability in the /phone arm and /phone disarm endpoints that fails to properly enforce operator.admin scope checks for external channels. Attackers can bypass authentication restrictions to arm or disarm phone channels without proper administrative privileges.	6.5	More Details
CVE-2026-31165	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the pppoeServiceName parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-1352	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.5	More Details
CVE-2026-31173	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the interval parameter to /cgi-bin/cstecgi.cgi.	6.5	More Details
CVE-2026-4279	The Bread & Butter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'breadbutter-customevent-button' shortcode in all versions up to, and including, 8.2.0.25. This is due to insufficient input sanitization and output escaping on the 'event' shortcode attribute. The customEventShortCodeButton() function takes the 'event' attribute value and directly interpolates it into a JavaScript string within an onclick HTML attribute without applying esc_attr() or esc_js(). Notably, the sister function customEventShortCode() properly uses esc_js() for the same attribute, but this was omitted in the button variant. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the page and clicks the injected button.	6.4	More Details
CVE-2026-4353	The CI HUB Connector plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' attribute of the `cihub_metadata` shortcode in all versions up to, and including, 1.2.106 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-	The Text Snippets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `ts` shortcode in all versions up to, and including, 0.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in	6.4	More Details

5748	pages that will execute whenever a user accesses an injected page.		
CVE-2026-4078	The ITERAS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple shortcodes (iteras-ordering, iteras-signup, iteras-paywall-login, iteras-selfservice) in all versions up to and including 1.8.2. This is due to insufficient input sanitization and output escaping in the combine_attributes() function. The function directly concatenates shortcode attribute values into JavaScript code within <script> tags using double-quoted string interpolation (line 489: '"'.$key.'": "'.$value.'"') without any escaping. An attacker can break out of the JavaScript string context by including a double-quote character in a shortcode attribute value and inject arbitrary JavaScript. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5767	The SlideShowPro SC plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `slideShowProSC` shortcode in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6246	The Simple Random Posts Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'container_right_width' attribute of the 'simple_random_posts' shortcode in all versions up to, and including, 0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1395	The Gutentools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Post Slider block's block_id attribute in all versions up to, and including, 1.1.3. This is due to insufficient input sanitization and output escaping combined with a custom unescaping routine that reintroduces dangerous characters. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1913	The Gallagher Website Design plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's login_link shortcode in all versions up to, and including, 2.6.4 due to insufficient input sanitization and output escaping on the 'prefix' attribute. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4125	The WPMK Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' shortcode attribute in all versions up to and including 1.0.1. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, in the wpmk_block_shortcode() function, the 'class' attribute is extracted from user-controllable shortcode attributes and directly concatenated into an HTML div element's class attribute without any escaping (e.g., esc_attr()). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5428	The Royal Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image captions in the Image Grid/Slider/Carousel widget in versions up to and including 1.7.1056. This is due to insufficient output escaping in the render_post_thumbnail() function, where wp_kses_post() is used instead of esc_attr() for the alt attribute context. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses a page with the malicious image displayed in the media grid widget.	6.4	More Details
CVE-2026-4085	The Easy Social Photos Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wrapper_class' shortcode attribute of the 'my-instagram-feed' shortcode in all versions up to, and including, 3.1.2. This is due to insufficient input sanitization and output escaping on user supplied attributes. Specifically, the plugin uses sanitize_text_field() instead of esc_attr() when outputting the 'wrapper_class' attribute inside a double-quoted HTML class attribute. Since sanitize_text_field() does not encode double quotes, an attacker can break out of the class attribute and inject arbitrary HTML event handlers. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-31953	Xibo is an open source digital signage platform with a web content management system and Windows display player software. A stored Cross-Site Scripting (XSS) vulnerability in versions prior to 4.4.1 allows an authenticated user with notification creation permissions to inject arbitrary JavaScript into the notification body. When the notification is set as an "interrupt," the payload executes automatically in the browser of any targeted user upon login, requiring zero user interaction. Exploitation of the vulnerability is possible on behalf of an authorized user who has both of the following privileges, which are not granted to non-admins as standard: Access to the Notification Centre to view past notifications, and include "Add Notification" button to allow for the creation of new notifications. Users should upgrade to version 4.4.1 which fixes this issue. Upgrading to a fixed version is necessary to remediate. Users unable to upgrade should revoke such privileges from users they do not trust.	6.4	More Details
CVE-2026-1923	The Social Rocket – Social Sharing Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 1.3.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4805	The Woostify plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.5.0 This is due to insufficient input sanitization and output escaping in the bundled Lity.js lightbox library, where user-controlled input from the href attribute is concatenated directly into a jQuery HTML string without sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-	The Timeline Blocks for Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titleTag' attribute of the timeline-blocks/tb-timeline-blocks block in all versions up to, and including, 1.1.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with	6.4	More Details

6551	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-4074	The Quran Live Multilanguage plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cheikh' and 'lang' shortcode attributes in all versions up to, and including, 1.0.3. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. The quran_live_render() function of quran-live.php receives shortcode attributes and passes them directly through shortcode_atts() and extract() without any sanitization. These values are then passed to Render_Quran_Live::render_verse_quran_live() where they are echoed directly into inline <script> blocks using PHP short tags (<?=$cheikh;?> and <?=$lang;?>) at lines 191, 216, 217, 245, and 246 of Class_QuranLive.php. Since the output occurs inside a JavaScript context within <script> tags, an attacker can break out of the JavaScript string and inject arbitrary script code. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4076	The Slider Bootstrap Carousel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'category' and 'template' shortcode attributes in all versions up to and including 1.0.7. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. The plugin uses extract() on shortcode_atts() to parse attributes, then directly outputs the $category variable into multiple HTML attributes (id, data-target, href) on lines 38, 47, 109, and 113 without applying esc_attr(). Similarly, the $template attribute flows into a class attribute on line 93 without escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4082	The ER Swiffy Insert plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the [swiffy] shortcode in all versions up to and including 1.0.0. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes ('n', 'w', 'h'). These attributes are extracted using extract() and directly interpolated into the HTML output without any escaping such as esc_attr(). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3361	The WP Store Locator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpsl_address' post meta value in versions up to, and including, 2.2.261 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page and opens an injected map marker info window.	6.4	More Details
CVE-2026-6236	The Posts map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' shortcode attribute in all versions up to, and including, 0.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4089	The Twittee Text Tweet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute in all versions up to and including 1.0.8. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. The ttt_twittee_tweeter() function uses extract() to pull shortcode attributes into local variables and then directly concatenates them into HTML output without any escaping. Specifically, the $id parameter is inserted into an HTML id attribute context without esc_attr(), allowing an attacker to break out of the attribute and inject arbitrary HTML event handlers. Additionally, the $tweet, $content, $balloon, and $theme attributes are similarly injected into inline JavaScript without escaping (lines 87, 93, 101, 117). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-58344	Carbon Forum 5.9.0 contains a persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious JavaScript code through the Forum Name field in dashboard settings. Attackers with admin privileges can store JavaScript payloads in the Forum Name field that execute in the browsers of all users visiting the forum, enabling session hijacking and data theft.	6.4	More Details
CVE-2026-5820	The Zypento Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Table of Contents block in all versions up to, and including, 1.0.6. This is due to the front-end TOC rendering script reading heading text via `innerText` and inserting it into the page using `innerHTML` without proper sanitization. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6809	The Social Post Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Threads embed handler in all versions up to, and including, 2.0.1. This is due to insufficient input sanitization and output escaping on the user-supplied URL. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6725	The WPC Smart Messages for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' attribute of the `wpcsm_text_rotator` shortcode in all versions up to, and including, 4.2.8. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4088	The Switch CTA Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wppw_cta_box' shortcode in all versions up to, and including, 1.1. This is due to insufficient input sanitization and output escaping on user-supplied post meta values including 'cta_box_button_link', 'cta_box_button_id', 'cta_box_button_text', and 'cta_box_description'. The shortcode reads post meta from a user-specified post ID and echoes these values directly into HTML output without any escaping functions (no esc_attr(), esc_url(), or esc_html()). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-	A security vulnerability has been detected in SourceCodester Pizzafy Ecommerce System 1.0. The affected element is the function Category of the file pizza/index.php?page=category. The manipulation of the argument ID leads to sql injection.	6.3	More

7265	Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.		Details
CVE-2026-7268	A vulnerability has been found in SourceCodester Pizzafy Ecommerce System 1.0. This impacts the function save_category of the file /admin/ajax.php?action=save_category. Such manipulation of the argument Name leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-35364	A Time-of-Check to Time-of-Use (TOCTOU) race condition exists in the mv utility of uutils coreutils during cross-device operations. The utility removes the destination path before recreating it through a copy operation. A local attacker with write access to the destination directory can exploit this window to replace the destination with a symbolic link. The subsequent privileged move operation will follow the symlink, allowing the attacker to redirect the write and overwrite an arbitrary target file with contents from the source.	6.3	More Details
CVE-2026-7267	A flaw has been found in SourceCodester Pizzafy Ecommerce System 1.0. This affects an unknown function of the file /view_prod.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-7266	A vulnerability was detected in SourceCodester Pizzafy Ecommerce System 1.0. The impacted element is the function save_order of the file /admin/ajax.php?action=save_order. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-35374	A Time-of-Check to Time-of-Use (TOCTOU) vulnerability exists in the split utility of uutils coreutils. The program attempts to prevent data loss by checking for identity between input and output files using their file paths before initiating the split operation. However, the utility subsequently opens the output file with truncation after this path-based validation is complete. A local attacker with write access to the directory can exploit this race window by manipulating mutable path components (e.g., swapping a path with a symbolic link). This can cause split to truncate and write to an unintended target file, potentially including the input file itself or other sensitive files accessible to the process, leading to permanent data loss.	6.3	More Details
CVE-2026-7045	A vulnerability was determined in baomidou dynamic-datasource 2.5.0. Affected by this vulnerability is the function DsSpelExpressionProcessor#doDetermineDatasource of the file dynamic-datasource-spring/src/main/java/com/baomidou/dynamic/datasource/processor/DsSpelExpressionProcessor.java of the component StandardEvaluationContext/SpelExpressionParser. This manipulation causes injection. The attack may be initiated remotely. Patch name: 273fcedaee984c08197c0890f14190b86ab7e0b8. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2026-7264	A weakness has been identified in SourceCodester Pizzafy Ecommerce System 1.0. Impacted is the function get_cart_items of the file /admin/ajax.php?action=get_cart_items. Executing a manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-7043	A vulnerability has been found in GreenCMS up to 2.3. This impacts the function pluginAddLocal of the file /index.php?m=admin&c=custom&a=pluginadd. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-7229	A vulnerability was found in code-projects Coaching Management System 1.0. This affects an unknown function of the file /cims/modules/admin/reply.php of the component POST Handler. Performing a manipulation of the argument complaintreply results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-7044	A vulnerability was found in GreenCMS up to 2.3. Affected is the function themeadd of the file /index.php?m=admin&c=custom&a=themeadd. The manipulation results in unrestricted upload. The attack can be launched remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-7142	A vulnerability was determined in Wooey up to 0.13.2. The impacted element is the function add_or_update_script of the file wooey/api/scripts.py of the component API Endpoint. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.13.3rc1 and 0.14.0 is sufficient to resolve this issue. This patch is called f7846fc0c323da8325422cab32623491757f1b88. The affected component should be upgraded.	6.3	More Details
CVE-2026-7084	A vulnerability was found in HBAI-Ltd Toonflow-app up to 1.1.1. This affects the function fetch of the file src/routes/setting/vendorConfig/getCodeByLink.ts of the component getCodeByLink Endpoint. The manipulation of the argument Link results in server-side request forgery. The attack may be performed from remote. The exploit has been made public and could be used. There is ongoing doubt regarding the real existence of this vulnerability. The vendor explains in a reply to the issue report, that "[t]he /getCodeByLink interface is used to obtain TS code and run it locally. It is inherently a high-risk interface, and users must clearly understand the risks before requesting to use it."	6.3	More Details
CVE-2026-7107	A weakness has been identified in code-projects Invoice System in Laravel 1.0. The impacted element is an unknown function of the file /company. This manipulation of the argument logo causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-35360	The touch utility in uutils coreutils is vulnerable to a Time-of-Check to Time-of-Use (TOCTOU) race condition during file creation. When the utility identifies a missing path, it later attempts creation using File::create(), which internally uses O_TRUNC. An attacker can exploit this window to create a file or swap a symlink at the target path, causing touch to truncate an existing file and leading to permanent data loss.	6.3	More Details
CVE-2026-7115	A vulnerability was identified in code-projects Employee Management System 1.0. This vulnerability affects unknown code of the file 370project/delete.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-	A flaw has been found in CodeAstro Online Classroom 1.0. This affects an unknown part of the file /addnewfaculty.		More

2026-7148	Executing a manipulation of the argument fname can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	Details
CVE-2026-7305	A weakness has been identified in Xuxueli xxl-job up to 3.3.2. The affected element is the function triggerJob of the file xxl-job-admin/src/main/java/com/xxl/job/admin/service/impl/XxlJobServiceImpl.java of the component trigger Endpoint. This manipulation of the argument addressList causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. There is ongoing doubt regarding the real existence of this vulnerability. The project maintainer explains (translated from Chinese): "Triggers are manually activated and involve login and access control, thus requiring management." The pull request by the researcher got rejected because of that.	6.3	More Details
CVE-2026-7117	A weakness has been identified in code-projects Employee Management System 1.0. Impacted is an unknown function of the file 370project/approve.php. Executing a manipulation of the argument id/token can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-7118	A security vulnerability has been detected in code-projects Employee Management System 1.0. The affected element is an unknown function of the file 370project/cancel.php. The manipulation of the argument id/token leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-6994	A weakness has been identified in Envoy up to 1.33.0. Affected is the function params.add of the file source/extensions/filters/http/header_mutation/header_mutation.cc of the component Query Parameter Handler. This manipulation causes injection. Remote exploitation of the attack is possible. Patch name: f8f4f1e02fdc64ecd4acf2d903208dd7285ad3a4. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-6991	A vulnerability was determined in colinhacks Zod up to 4.3.6. The impacted element is an unknown function of the file packages/zod/src/v4/core/regexes.ts of the component CUID Data Type Handler. Executing a manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-7143	A vulnerability was identified in 1000 Projects Portfolio Management System MCA up to 1.0. This affects an unknown function of the file /admin/block_status.php. The manipulation of the argument q leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-24231	NVIDIA NemoClaw contains a vulnerability in the validateEndpointUrl() SSRF protection component, where an attacker could cause a server-side request forgery by supplying a crafted endpoint URL referencing the 0.0.0.0/8 address range through a blueprint configuration file or CLI flag. A successful exploit of this vulnerability may lead to information disclosure.	6.3	More Details
CVE-2026-6989	A vulnerability has been found in Tenda F453 up to 1.0.0.3. Impacted is the function TendaTelnet of the file /goform/telnet of the component Telnet Service. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-6982	A vulnerability was determined in star7th ShowDoc up to 2.10.10/3.6.2/3.8.0. Affected by this vulnerability is an unknown functionality of the file server/Application/Api/Controller/PageController.class.PHP of the component API Page Sort Endpoint. Executing a manipulation of the argument pages can lead to sql injection. The attack may be launched remotely. Upgrading to version 3.8.1 addresses this issue. It is suggested to upgrade the affected component. According to the researcher, "[t]he vendor explicitly stated they will not backport patches to the older affected versions."	6.3	More Details
CVE-2026-6981	A vulnerability was found in IhateCreatingUserNames2 AiraHub2 up to 3e4b77fd7d48ed811ffe5b8d222068c17c76495e. Affected is the function connect_stream_endpoint/sync_agents of the file AiraHub.py of the component Endpoint. Performing a manipulation results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. Multiple endpoints are affected. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6979	A flaw has been found in devlikeapro WAHA up to 2026.3.4. This affects an unknown function of the file src/api/media.controller.ts of the component API Request Handler. This manipulation causes server-side request forgery. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-7290	A vulnerability was determined in JeecgBoot up to 3.9.1. Impacted is the function SqlInjectionUtil of the file jeecg-boot/jeecg-boot-base-core/src/main/java/org/jeecg/common/util/SqlInjectionUtil.java of the component loadDict Endpoint. This manipulation of the argument keyword causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. Patch name: a9c8e8eb1185751c4c3c68d2a53f3dadee9edc6b. To fix this issue, it is recommended to deploy a patch.	6.3	More Details
CVE-2026-7114	A vulnerability was determined in code-projects Employee Management System 1.0. This affects an unknown part of the file 370project/edit.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-7150	A vulnerability was found in dh1011 auto-favicon up to f189116a9259950c2393f114dbcb94dde0ad864b. This issue affects the function generate_favicon_from_url of the file src/auto_favicon/server.py of the component MCP Tool. The manipulation of the argument image_url results in server-side request forgery. The attack may be performed from remote. The exploit has been made public and could be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-7102	A vulnerability was found in Tenda F456 1.0.0.5. This impacts the function FromWriteFacMac of the file /goform/WriteFacMac of the component httpd. The manipulation of the argument mac results in command injection. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details

CVE-2026-7023	A vulnerability was detected in ByteDance coze-studio up to 0.5.1. Affected by this vulnerability is the function ExecuteSQL of the file backend/domain/memory/database/service/database_impl.go of the component databaseTool. Performing a manipulation results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-7091	A flaw has been found in code-projects Invoice System in Laravel 1.0. This impacts an unknown function of the file /user of the component User Management Handler. This manipulation causes improper authorization. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2026-7092	A vulnerability has been found in code-projects Invoice System in Laravel 1.0. Affected is an unknown function of the file /profile/ of the component Profile Handler. Such manipulation of the argument ID leads to improper authorization. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-35356	A Time-of-Check to Time-of-Use (TOCTOU) vulnerability exists in the install utility of uutils coreutils when using the -D flag. The command creates parent directories and subsequently performs a second path resolution to create the target file, neither of which is anchored to a directory file descriptor. An attacker with concurrent write access can replace a path component with a symbolic link between these operations, redirecting the privileged write to an arbitrary file system location.	6.3	More Details
CVE-2026-35355	The install utility in uutils coreutils is vulnerable to a Time-of-Check to Time-of-Use (TOCTOU) race condition during file installation. The implementation unlinks an existing destination file and then recreates it using a path-based operation without the O_EXCL flag. A local attacker can exploit the window between the unlink and the subsequent creation to swap the path with a symbolic link, allowing them to redirect privileged writes to overwrite arbitrary system files.	6.3	More Details
CVE-2026-7093	A vulnerability was found in code-projects Invoice System in Laravel 1.0. Affected by this vulnerability is an unknown functionality of the file /invoice/ of the component Invoice Endpoint. Performing a manipulation of the argument ID results in improper authorization. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-62233	Deserialization of Untrusted Data vulnerability in Apache DolphinScheduler RPC module. This issue affects Apache DolphinScheduler: Version >= 3.2.0 and < 3.3.1. Attackers who can access the Master or Worker nodes can compromise the system by creating a StandardRpcRequest, injecting a malicious class type into it, and sending RPC requests to the DolphinScheduler Master/Worker nodes. Users are recommended to upgrade to version [3.3.1], which fixes the issue.	6.3	More Details
CVE-2026-7196	A security vulnerability has been detected in CodeAstro Online Classroom 1.0. Affected is an unknown function of the file /guestdetails. Such manipulation of the argument deleteid leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-7291	A weakness has been identified in o2oa up to 10.0. This affects the function FileAction of the file FileAction.java of the component URL Fetching. Executing a manipulation of the argument fileUrl can lead to server-side request forgery. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2018-25295	ObserverIP Scan Tool 1.4.0.1 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string in the IP input field. Attackers can paste a 2000-byte buffer of repeated characters into the IP field and trigger a search operation to cause an application crash.	6.2	More Details
CVE-2018-25275	Faleemi Plus 1.0.2 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying oversized input strings. Attackers can paste a 2000-byte payload into the Camera name and DID number fields during camera addition to trigger an application crash.	6.2	More Details
CVE-2018-25279	jiNa OCR Image to Text 1.0 contains a denial of service vulnerability that allows local attackers to crash the application by processing a malformed PNG file. Attackers can create a specially crafted PNG file with an oversized buffer and trigger the crash when the application attempts to convert the file to PDF.	6.2	More Details
CVE-2018-25271	Textpad 8.1.2 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long buffer string through the Run command interface. Attackers can paste a 5000-byte payload into the Command field via Tools > Run to trigger a buffer overflow that crashes the application.	6.2	More Details
CVE-2018-25267	UltraISO 9.7.1.3519 contains a local buffer overflow vulnerability in the Output FileName field of the Make CD/DVD Image dialog that allows attackers to overwrite SEH and SE handler records. Attackers can craft a malicious filename string with 304 bytes of data followed by SEH record overwrite values and paste it into the Output FileName field to trigger a denial of service crash.	6.2	More Details
CVE-2018-25266	Angry IP Scanner 3.5.3 contains a buffer overflow vulnerability in the preferences dialog that allows local attackers to crash the application by supplying an excessively large string. Attackers can generate a file containing a massive buffer of repeated characters and paste it into the unavailable value field in the display preferences to trigger a denial of service.	6.2	More Details
CVE-2026-6386	In order to apply a particular protection key to an address range, the kernel must update the corresponding page table entries. The subroutine which handled this failed to take into account the presence of 1GB largepage mappings created using the shm_create_largepage(3) interface. In particular, it would always treat a page directory page entry as pointing to another page table page. The bug can be abused by an unprivileged user to cause pmap_pkru_update_range() to treat userspace memory as a page table page, and thus overwrite memory to which the application would otherwise not have access.	6.2	More Details
CVE-2018-25282	Nmap 7.70 contains a denial of service vulnerability that allows local attackers to crash the application by processing malicious XML files with exponential entity expansion. Attackers can create a crafted XML file with nested entity definitions and open it through ZenMap's scan import functionality to cause the program to consume excessive system resources and crash.	6.2	More Details

CVE-2018-25262	Angry IP Scanner for Linux 3.5.3 contains a denial of service vulnerability that allows local attackers to crash the application by supplying malformed input to the port selection field. Attackers can craft a malicious string containing buffer overflow patterns and paste it into the Preferences Ports tab to trigger an application crash.	6.2	More Details
CVE-2026-35902	The RTSP service of MERCURY IP camera MIPC252W 1.0.5 Build 230306 has an issue handling failed Digest authentication attempts. By repeatedly sending RTSP requests with invalid authentication parameters, an unauthenticated attacker can cause the RTSP service to enter a persistent authentication failure state, preventing legitimate clients from authenticating and leading to a denial of service.	6.2	More Details
CVE-2018-25297	Wansview 1.0.2 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying oversized input strings. Attackers can inject 2000-byte payloads into the Camera name and DID number fields during camera addition to trigger application crashes.	6.2	More Details
CVE-2018-25284	HD Tune Pro 5.70 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the folder/file name field. Attackers can trigger a denial of service by entering a 6000-byte payload through the File > Options > Save dialog's folder/file name input field.	6.2	More Details
CVE-2018-25293	Prime95 29.4b7 contains a buffer overflow vulnerability in the PrimeNet connection dialog that allows local attackers to crash the application by supplying an excessively long string in the optional proxy password field. Attackers can trigger a denial of service by entering a 6000-byte payload into the proxy password parameter, causing the application to crash when processing the connection settings.	6.2	More Details
CVE-2018-25277	PixGPS 1.1.8 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized string to the folder path input field. Attackers can craft a payload exceeding 6000 bytes and paste it into the 'Folder with picture files' field to trigger a denial of service condition.	6.2	More Details
CVE-2018-25292	Bome Restorator 1793 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Name field. Attackers can create a malicious payload exceeding 4000 bytes and paste it into the Name input field to trigger an application crash and denial of service.	6.2	More Details
CVE-2018-25274	InfraRecorder 0.53 contains a denial of service vulnerability that allows local attackers to crash the application by importing a maliciously crafted text file. Attackers can create a text file containing 6000 bytes of data and import it through the Edit menu's Import function to trigger an application crash.	6.2	More Details
CVE-2018-25278	PicaJet FX 2.6.5 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input to registration fields. Attackers can paste a 6000-byte buffer into the Registration Name and Registration Key fields via the Help menu's Register PicaJet dialog to trigger an application crash.	6.2	More Details
CVE-2018-25290	Easyboot 6.6.0 contains a buffer overflow vulnerability in the Replace Text function that allows local attackers to crash the application by supplying an oversized string. Attackers can trigger the vulnerability by accessing File > Tools > Replace Text and pasting a 7000-byte payload into the text fields to cause a denial of service.	6.2	More Details
CVE-2018-25264	TransMac 12.2 contains a buffer overflow vulnerability in the license key input field that allows local attackers to crash the application by submitting an oversized string. Attackers can generate a payload file containing 4000 bytes of data, paste it into the License Key field, and trigger a denial of service condition.	6.2	More Details
CVE-2026-28950	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.8 and iPadOS 18.7.8, iOS 26.4.2 and iPadOS 26.4.2. Notifications marked for deletion could be unexpectedly retained on the device.	6.2	More Details
CVE-2018-25289	Softdisk 3.0.3 contains a buffer overflow vulnerability in the registration code dialog that allows local attackers to crash the application by supplying an oversized string. Attackers can trigger the vulnerability by entering a 6000-byte payload in the Registration Name field through the Help menu's Enter Registration Code dialog to cause a denial of service.	6.2	More Details
CVE-2018-25288	StyleWriter 1.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string. Attackers can paste a 6000-byte payload into the Pattern to Find or Advice Message fields in the Add Pattern dialog to trigger a denial of service condition.	6.2	More Details
CVE-2018-25291	Project64 2.3.2 contains a buffer overflow vulnerability in the Plugin Directory settings field that allows local attackers to crash the application by supplying an excessively long string. Attackers can input a 6000-byte payload into the Plugin Directory field through the Options > Settings > Directories interface to trigger an application crash when settings are reopened.	6.2	More Details
CVE-2018-25286	Easy PhotoResQ 1.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Folder/filename field. Attackers can input a 6000-byte payload through the File Options dialog to trigger a denial of service condition.	6.2	More Details
CVE-2018-25273	CrossFont 7.5 contains a buffer overflow vulnerability that allows local attackers to crash the application by submitting an oversized payload in the License Key field. Attackers can generate a malicious file containing 4000 bytes of data, paste it into the License Key input field, and trigger an application crash when processing the input.	6.2	More Details
CVE-2026-38935	A reflected cross-site scripting (XSS) vulnerability exists in diskover-community <= 2.3.5 in public/view.php via the doctype parameter	6.1	More Details
CVE-2026-41067	Astro is a web framework. Prior to 6.1.6, the defineScriptVars function in Astro's server-side rendering pipeline uses a case-sensitive regex /<\/script>/g to sanitize values injected into inline <script> tags via the define:vars directive. HTML parsers close <script> elements case-insensitively and also accept whitespace or / before the closing >, allowing an attacker to bypass the sanitization with payloads like </Script>, </script >, or </script/> and inject arbitrary HTML/JavaScript. This vulnerability is fixed in 6.1.6.	6.1	More Details

CVE-2026-41426	pretalx is a conference planning tool. Prior to 2026.1.0, an unauthenticated attacker can send arbitrary HTML-rendered emails from a pretalx instance's configured sender address by embedding malformed HTML or markdown link syntax in a user-controlled template placeholder such as the account display name. The most direct vector is the password-reset flow: the attacker registers an account with a malicious name, enters the victim's email address, and triggers a password reset. The resulting email is delivered from the event's legitimate sender address and passes SPF/DKIM/DMARC validation, making it a ready-made phishing vector. This vulnerability is fixed in 2026.1.0.	6.1	More Details
CVE-2026-41373	OpenClaw before 2026.3.31 contains an incomplete host-env-security-policy.json that fails to restrict compiler binary environment variables, allowing untrusted models to substitute CC, CXX, CARGO_BUILD_RUSTC, and CMAKE_C_COMPILER via environment overrides. Attackers with approved host-exec requests can override compiler binaries to execute arbitrary code during build processes.	6.1	More Details
CVE-2026-38936	A reflected cross-site scripting (XSS) vulnerability exists in diskover-community <= 2.3.5 in public/selectindices.php via the namecontains parameter	6.1	More Details
CVE-2026-40979	In Spring AI, having access to a shared environment can expose the ONNX model used by the application. Affected versions: Spring AI: 1.0.0 - 1.0.5 (fixed in 1.0.6), 1.1.0 - 1.1.4 (fixed in 1.1.5)	6.1	More Details
CVE-2026-41472	CyberPanel versions prior to 2.4.4 contain a stored cross-site scripting vulnerability in the AI Scanner dashboard where the POST /api/ai-scanner/callback endpoint lacks authentication and allows unauthenticated attackers to inject malicious JavaScript by overwriting the findings_json field of ScanHistory records. Attackers can inject JavaScript that executes in an administrator's authenticated session when they visit the AI Scanner dashboard, allowing them to issue same-origin requests to plant cron jobs and achieve remote code execution on the server.	6.1	More Details
CVE-2026-29971	A reflected cross-site scripting (XSS) vulnerability exists in WebFileSys version before 2.32.0 and fixed in v.2.32.0. User-controlled input is reflected into HTML and JavaScript contexts without proper output encoding, allowing arbitrary JavaScript execution in the victim's browser via the ftpBackup functionality, authentication input handling, search functionality, and error message rendering components	6.1	More Details
CVE-2025-61872	Mahara before 25.04.2 and 24.04.11 are vulnerable to displaying results that can trigger XSS via a malicious search query string. This occurs in the 'search site' feature when using the Elasticsearch7 search plugin. The Elasticsearch function does not properly sanitize input in the query parameter.	6.1	More Details
CVE-2026-6835	The a+HCM developed by aEnrich has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload arbitrary files to any path, including HTML documents, which may result in a XSS-like effect.	6.1	More Details
CVE-2018-25269	ICEWARP 11.0.0.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious HTML elements into emails by embedding base64-encoded payloads in object and embed tags. Attackers can craft emails containing data URIs with embedded scripts that execute in the client when the email is viewed, compromising user sessions and stealing sensitive information.	6.1	More Details
CVE-2026-30139	A reflected cross-site scripting (XSS) vulnerability in the AdvancedSearch functionality of Silverpeas Core before version 6.4.6 allows attackers to execute arbitrary JavaScript in the context of a user's browser via crafted input.	6.1	More Details
CVE-2026-4090	The Inquiry Cart plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.4.2. This is due to missing nonce verification in the rd_ic_settings_page function when processing settings form submissions. This makes it possible for unauthenticated attackers to update the plugin's settings, including injecting malicious scripts that will be stored and executed in the admin area, via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-41305	PostCSS takes a CSS file and provides an API to analyze and modify its rules by transforming the rules into an Abstract Syntax Tree. Versions prior to 8.5.10 do not escape `</style>` sequences when stringifying CSS ASTs. When user-submitted CSS is parsed and re-stringified for embedding in HTML `<style>` tags, `</style>` in CSS values breaks out of the style context, enabling XSS. Version 8.5.10 fixes the issue.	6.1	More Details
CVE-2026-29050	melange allows users to build apk packages using declarative pipelines. Starting in version 0.32.0 and prior to version 0.43.4, an attacker who can influence a melange configuration file — for example through pull-request-driven CI or build-as-a-service scenarios — could set `pipeline[].uses` to a value containing `../` sequences or an absolute path. The `(*Compiled).compilePipeline` function in `pkg/build/compile.go` passed `uses` directly to `filepath.Join(pipelineDir, uses + ".yaml")` without validating the value, so the resolved path could escape each `--pipeline-dir` and read an arbitrary YAML-parseable file visible to the melange process. Because the loaded file is subsequently interpreted as a melange pipeline and its `runs:` block is executed via `/bin/sh -c` in the build sandbox, this additionally allowed shell commands sourced from an out-of-tree file to run during the build, bypassing the review boundary that normally covers the in-tree pipeline definition. The issue is fixed in melange v0.43.4 via commit 5829ca4. The fix rejects `uses` values that are absolute paths or contain `..`, and verifies (via `filepath.Rel` after `filepath.Clean`) that the resolved target remains within the pipeline directory. As a workaround, only run `melange build` against configuration files from trusted sources. In CI systems that build user-supplied melange configs, gate builds behind manual review of `pipeline[].uses` values and reject any containing `..` or leading `/`.	6.1	More Details
CVE-2026-4131	The WP Responsive Popup + Optin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 1.4. This is due to the settings form on the admin page (wpo_admin_page.php) lacking nonce generation (wp_nonce_field) and verification (wp_verify_nonce/check_admin_referer). This makes it possible for unauthenticated attackers to update all plugin settings including the 'wpo_image_url' parameter via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	6.1	More Details
CVE-	A flaw was found in GNU Emacs. This vulnerability, a memory corruption issue, occurs when Emacs processes specially		

2026-6861	crafted SVG (Scalable Vector Graphics) CSS (Cascading Style Sheets) data. A local user could exploit this by convincing a victim to open a malicious SVG file, which may lead to a denial of service (DoS) or potentially information disclosure.	6.1	More Details
CVE-2026-41665	Integer overflow in scratch buffer initialization size calculation in Samsung Open Source ONE cause incorrect memory initialization for large intermediate tensors. Affected version is prior to commit 1.30.0.	6.1	More Details
CVE-2026-6967	Missing expiration, hash, and length enforcement in delegated metadata validation in awslabs/tough before tough-v0.22.0 allows remote authenticated users with delegated signing authority to bypass TUF specification integrity checks for delegated targets metadata and poison the local metadata cache, because load_delegations does not apply the same validation checks as the top-level targets metadata path. We recommend you upgrade to tough-v0.22.0 / tuftool-v0.15.0.	5.9	More Details
CVE-2026-41173	The AWS X-Ray Remote Sampler package provides a sampler which can get sampling configurations from AWS X-Ray. Prior to 0.1.0-alpha.8, OpenTelemetry.Sampler.AWS reads unbounded HTTP response bodies from a configured AWS X-Ray remote sampling endpoint into memory. AWSXRaySamplerClient.DoRequestAsync called HttpClient.SendAsync followed by ReadAsStringAsync(), which materializes the entire HTTP response body into a single in-memory string with no size limit. The sampling endpoint is configurable via AWSXRayRemoteSamplerBuilder.SetEndpoint (default: http://localhost:2000). An attacker who controls the configured endpoint, or who can intercept traffic to it (MitM), can return an arbitrarily large response body. This causes unbounded heap allocation in the consuming process, leading to high transient memory pressure, garbage-collection stalls, or an OutOfMemoryException that terminates the process. This vulnerability is fixed in 0.1.0-alpha.8.	5.9	More Details
CVE-2026-40355	In MIT Kerberos 5 (aka krb5) before 1.22.3, there is a NULL pointer dereference if an application calls gss_accept_sec_context() on a system with a NegoEx mechanism registered in /etc/gss/mech. An unauthenticated remote attacker can trigger this, causing the process to terminate in parse_nego_message.	5.9	More Details
CVE-2026-41213	@node-oauth/oauth2-server is a module for implementing an OAuth2 server in Node.js. The token exchange path accepts RFC7636-invalid code_verifier values (including one-character strings) for S256 PKCE flows. Because short/weak verifiers are accepted and failed verifier attempts do not consume the authorization code, an attacker who intercepts an authorization code can brute-force code_verifier guesses online until token issuance succeeds.	5.9	More Details
CVE-2026-6968	Incomplete path traversal fixes in awslabs/tough before tough-v0.22.0 allow remote authenticated users with delegated signing authority to write files outside intended output directories via absolute target names in copy_target/link_target, symlinked parent directories in save_target, or symlinked metadata filenames in SignedRole::write, because write paths trust the joined destination path without post-resolution containment verification. We recommend you upgrade to tough-v0.22.0 / tuftool-v0.15.0.	5.9	More Details
CVE-2026-7318	A vulnerability was detected in elie mcp-project 0.1.0. The affected element is the function search_papers of the file research_server.py. The manipulation of the argument topic results in path traversal. Attacking locally is a requirement. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.9	More Details
CVE-2026-33262	An attacker can send replies that result in a null pointer dereference, caused by a missing consistency check and leading to a denial of service. Cookies are disabled by default.	5.9	More Details
CVE-2026-40356	In MIT Kerberos 5 (aka krb5) before 1.22.3, there is an integer underflow and resultant out-of-bounds read if an application calls gss_accept_sec_context() on a system with a NegoEx mechanism registered in /etc/gss/mech. An unauthenticated remote attacker can trigger this, possibly causing the process to terminate in parse_message.	5.9	More Details
CVE-2026-40514	SmarterTools SmarterMail builds prior to 9610 contain a cryptographic weakness in the file and email sharing endpoints that use DES-CBC encryption with keys and initialization vectors derived from System.Random seeded with insufficient entropy, reducing the seed space to approximately 19,000 possible values. An unauthenticated attacker can use the attachment download endpoint as an oracle to determine the seed in use and derive encryption keys and initialization vectors to forge sharing tokens for arbitrary emails, attachments, or file storage contents without prior access to the targeted content.	5.9	More Details
CVE-2026-33467	Improper Verification of Cryptographic Signature (CWE-347) in Elastic Package Registry could allow an attacker positioned to intercept network traffic, or to otherwise influence the contents served to a self-hosted registry, to substitute a tampered package without the integrity check failing closed.	5.9	More Details
CVE-2026-33610	A rogue primary server may cause file descriptor exhaustion and eventually a denial of service, when a PowerDNS secondary server forwards a DNS update request to it.	5.9	More Details
CVE-2026-33261	A zone transition from NSEC to NSEC3 might trigger an internal inconsistency and cause a denial of service.	5.9	More Details
CVE-2026-40966	In Spring AI, an attacker can bypass conversation isolation and exfiltrate sensitive memory from other users' chat histories, including secrets and credentials, by injecting filter logic through conversationId. Only applications that use VectorStoreChatMemoryAdvisor and pass user-supplied input as a conversationId are affected.	5.9	More Details
CVE-2026-41078	OpenTelemetry dotnet is a dotnet telemetry framework. In 1.6.0-rc.1 and earlier, OpenTelemetry.Exporter.Jaeger may allow sustained memory pressure when the internal pooled-list sizing grows based on a large observed span/tag set and that enlarged size is reused for subsequent allocations. Under high-cardinality or attacker-influenced telemetry input, this can increase memory consumption and potentially cause denial of service. There is no plan to fix this issue as OpenTelemetry.Exporter.Jaeger was deprecated in 2023.	5.9	More Details

CVE-2026-40343	free5GC UDR is the user data repository (UDR) for free5GC, an an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.2, a fail-open request handling flaw in the UDR service causes the `/nudr-dr/v2/policy-data/subs-to-notify` POST handler to continue processing requests even after request body retrieval or deserialization errors. This may allow unintended creation of Policy Data notification subscriptions with invalid, empty, or partially processed input, depending on downstream processor behavior. As of time of publication, a patched version is not available.	5.8	More Details
CVE-2026-41372	OpenClaw before 2026.4.2 fails to normalize trailing-dot localhost hosts in remote CDP discovery responses, allowing bypass of loopback protections. Attackers can craft hostile discovery responses returning localhost. to retarget authenticated browser control toward localhost endpoints and expose browser state.	5.8	More Details
CVE-2026-42424	OpenClaw before 2026.4.8 treats shared reply MEDIA paths as trusted, allowing crafted references to trigger cross-channel local file exfiltration. Attackers can exploit this by crafting malicious shared reply MEDIA references to cause another channel to read local file paths as trusted generated media.	5.7	More Details
CVE-2025-13763	Multiple uses of uninitialized variables were found in libopensc that may lead to information disclosure or application crash. An attack requires a crafted USB device or smart card that would present the system with specially crafted responses to the APDUs	5.7	More Details
CVE-2026-7112	A vulnerability has been found in NousResearch hermes-agent 0.8.0. Affected by this vulnerability is the function _check_auth of the file gateway/platforms/api_server.py of the component API_SERVER_KEY Handler. The manipulation leads to improper authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	5.6	More Details
CVE-2026-7292	A security vulnerability has been detected in o2oa up to 10.0. This impacts the function syncFile of the file NodeAgent.java of the component NodeAgent. The manipulation leads to improper authorization. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is said to be difficult. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.6	More Details
CVE-2026-35363	A vulnerability in the rm utility of uutils coreutils allows the bypass of safeguard mechanisms intended to protect the current directory. While the utility correctly refuses to delete . or .., it fails to recognize equivalent paths with trailing slashes, such as ./ or .///. An accidental or malicious execution of rm -rf ./ results in the silent recursive deletion of all contents within the current directory. The command further obscures the data loss by reporting a misleading 'Invalid input' error, which may cause users to miss the critical window for data recovery.	5.6	More Details
CVE-2026-7141	A vulnerability was found in vllm up to 0.19.0. The affected element is the function has_mamba_layers of the file vllm/v1/kv_cache_interface.py of the component KV Block Handler. Performing a manipulation results in uninitialized resource. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is described as difficult. The exploit has been made public and could be used. The patch is named 1ad67864c0c20f167929e64c875f5c28e1aad9fd. To fix this issue, it is recommended to deploy a patch.	5.6	More Details
CVE-2026-7306	A security vulnerability has been detected in Xuxueli xxl-job up to 3.3.2. The impacted element is an unknown function of the file xxl-job-admin/src/main/java/com/xxl/job/admin/scheduler/openapi/OpenApiController.java of the component OpenAPI Endpoint. Such manipulation of the argument default_token leads to use of hard-coded cryptographic key . It is possible to launch the attack remotely. A high complexity level is associated with this attack. The exploitability is regarded as difficult. The exploit has been disclosed publicly and may be used.	5.6	More Details
CVE-2026-7018	A vulnerability was determined in Datavane Datavines up to 13607645e14a4982468cfdbcf75c85cde63bae71. The affected element is an unknown function of the file datavines-core/src/main/java/io/datavines/core/utils/TokenManager.java of the component JWT Token Handler. Executing a manipulation of the argument tokenSecret can lead to use of hard-coded cryptographic key . The attack can be executed remotely. The attack requires a high level of complexity. The exploitability is described as difficult. The exploit has been publicly disclosed and may be utilized. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. This patch is called e540d6dc04e2e6ad11907fb655f3728a13e7b939. It is advisable to implement a patch to correct this issue. The project was informed of the problem early through a pull request but has not reacted yet.	5.6	More Details
CVE-2026-7020	A security flaw has been discovered in Ollama up to 0.20.2. This affects the function digestToPath of the file x/imagegen/transfer/transfer.go of the component Tensor Model Transfer Handler. The manipulation of the argument digest results in path traversal. The attack may be performed from remote. This attack is characterized by high complexity. The exploitability is reported as difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2026-7113	A vulnerability was found in NousResearch hermes-agent 0.8.0. Affected by this issue is some unknown functionality of the file gateway/platforms/webhook.py of the component Webhooks Endpoint. The manipulation of the argument _INSECURE_NO_AUTH results in missing authentication. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitation is known to be difficult. The exploit has been made public and could be used. The project was informed of the problem early through a pull request but has not reacted yet.	5.6	More Details
CVE-2026-6878	A vulnerability was identified in ByteDance verl up to 0.7.0. Affected is the function math_equal of the file prime_math/grader.py. The manipulation leads to sandbox issue. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: module: Fix kernel panic when a symbol st_shndx is out of bounds The module loader doesn't check for bounds of the ELF section index in simplify_symbols(): for (i = 1; i < symsec->sh_size / sizeof(Elf_Sym); i++) { const char *name = info->strtab + sym[i].st_name; switch (sym[i].st_shndx) { case SHN_COMMON: [...] default: /* Divert to percpu allocation if a percpu var. */ if (sym[i].st_shndx == info->index.pcpu) secbase = (unsigned long)mod_percpu(mod); else /** HERE --> **/ secbase = info->sechdrs[sym[i].st_shndx].sh_addr;		

2026-31521	sym[i].st_value += secbase; break; } } A symbol with an out-of-bounds st_shndx value, for example 0xffff (known as SHN_XINDEX or SHN_HIRESERVE), may cause a kernel panic: BUG: unable to handle page fault for address: ... RIP: 0010:simplify_symbols+0x2b2/0x480 ... Kernel panic - not syncing: Fatal exception This can happen when module ELF is legitimately using SHN_XINDEX or when it is corrupted. Add a bounds check in simplify_symbols() to validate that st_shndx is within the valid range before using it. This issue was discovered due to a bug in llvm-objcopy, see relevant discussion for details [1]. [1] https://lore.kernel.org/linux-modules/20251224005752.201911-1-ihor.solodrai@linux.dev/	5.5	More Details
CVE-2026-31520	In the Linux kernel, the following vulnerability has been resolved: HID: apple: avoid memory leak in apple_report_fixup() The apple_report_fixup() function was returning a newly kmemdup()-allocated buffer, but never freeing it. The caller of report_fixup() does not take ownership of the returned pointer, but it *is* permitted to return a sub-portion of the input rdesc, whose lifetime is managed by the caller.	5.5	More Details
CVE-2026-6844	A flaw was found in the `readelf` utility of the binutils package. A local attacker could exploit two Denial of Service (DoS) vulnerabilities by providing a specially crafted Executable and Linkable Format (ELF) file. One vulnerability, a resource exhaustion (CWE-400), can lead to an out-of-memory condition. The other, a null pointer dereference (CWE-476), can cause a segmentation fault. Both issues can result in the `readelf` utility becoming unresponsive or crashing, leading to a denial of service.	5.5	More Details
CVE-2026-35380	A logic error in the cut utility of uutils coreutils causes the program to incorrectly interpret the literal two-byte string '' (two single quotes) as an empty delimiter. The implementation mistakenly maps this string to the NUL character for both the -d (delimiter) and --output-delimiter options. This vulnerability can lead to silent data corruption or logic errors in automated scripts and data pipelines that process strings containing these characters, as the utility may unintentionally split or join data on NUL bytes rather than the intended literal characters.	5.5	More Details
CVE-2018-25287	Drive Power Manager 1.10 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Name field. Attackers can paste a 6000-byte payload into the Name field and click Register to trigger a denial of service condition.	5.5	More Details
CVE-2026-31529	In the Linux kernel, the following vulnerability has been resolved: cxl/region: Fix leakage in __construct_region() Failing the first sysfs_update_group() needs to explicitly kfree the resource as it is too early for cxl_region_iomem_release() to do so.	5.5	More Details
CVE-2026-31524	In the Linux kernel, the following vulnerability has been resolved: HID: asus: avoid memory leak in asus_report_fixup() The asus_report_fixup() function was returning a newly allocated kmemdup()-allocated buffer, but never freeing it. Switch to devm_kzalloc() to ensure the memory is managed and freed automatically when the device is removed. The caller of report_fixup() does not take ownership of the returned pointer, but it is permitted to return a pointer whose lifetime is at least that of the input buffer. Also fix a harmless out-of-bounds read by copying only the original descriptor size.	5.5	More Details
CVE-2026-35369	An argument parsing error in the kill utility of uutils coreutils incorrectly interprets kill -1 as a request to send the default signal (SIGTERM) to PID -1. Sending a signal to PID -1 causes the kernel to terminate all processes visible to the caller, potentially leading to a system crash or massive process termination. This differs from GNU coreutils, which correctly recognizes -1 as a signal number in this context and would instead report a missing PID argument.	5.5	More Details
CVE-2026-31519	In the Linux kernel, the following vulnerability has been resolved: btrfs: set BTRFS_ROOT_ORPHAN_CLEANUP during subvol create We have recently observed a number of subvolumes with broken dentries. ls-ing the parent dir looks like: drwxrwxrwt 1 root root 16 Jan 23 16:49 . drwxr-xr-x 1 root root 24 Jan 23 16:48 .. d????????? ? ? ? ? ? broken_subvol and similarly stat-ing the file fails. In this state, deleting the subvol fails with ENOENT, but attempting to create a new file or subvol over it errors out with EEXIST and even aborts the fs. Which leaves us a bit stuck. dmesg contains a single notable error message reading: "could not do orphan cleanup -2" 2 is ENOENT and the error comes from the failure handling path of btrfs_orphan_cleanup(), with the stack leading back up to btrfs_lookup(). btrfs_lookup btrfs_lookup_dentry btrfs_orphan_cleanup // prints that message and returns -ENOENT After some detailed inspection of the internal state, it became clear that: - there are no orphan items for the subvol - the subvol is otherwise healthy looking, it is not half-deleted or anything, there is no drop progress, etc. - the subvol was created a while ago and does the meaningful first btrfs_orphan_cleanup() call that sets BTRFS_ROOT_ORPHAN_CLEANUP much later. - after btrfs_orphan_cleanup() fails, btrfs_lookup_dentry() returns -ENOENT, which results in a negative dentry for the subvolume via d_splice_alias(NULL, dentry), leading to the observed behavior. The bug can be mitigated by dropping the dentry cache, at which point we can successfully delete the subvolume if we want. i.e., btrfs_lookup() btrfs_lookup_dentry() if (!sb_rdonly(inode->vfs_inode)->vfs_inode) btrfs_orphan_cleanup(sub_root) test_and_set_bit(BTRFS_ROOT_ORPHAN_CLEANUP) btrfs_search_slot() // finds orphan item for inode N ... prints "could not do orphan cleanup -2" if (inode == ERR_PTR(-ENOENT)) inode = NULL; return d_splice_alias(NULL, dentry) // NEGATIVE DENTRY for valid subvolume btrfs_orphan_cleanup() does test_and_set_bit(BTRFS_ROOT_ORPHAN_CLEANUP) on the root when it runs, so it cannot run more than once on a given root, so something else must run concurrently. However, the obvious routes to deleting an orphan when nlinks goes to 0 should not be able to run without first doing a lookup into the subvolume, which should run btrfs_orphan_cleanup() and set the bit. The final important observation is that create_subvol() calls d_instantiate_new() but does not set BTRFS_ROOT_ORPHAN_CLEANUP, so if the dentry cache gets dropped, the next lookup into the subvolume will make a real call into btrfs_orphan_cleanup() for the first time. This opens up the possibility of concurrently deleting the inode/orphan items but most typical evict() paths will be holding a reference on the parent dentry (child dentry holds parent->d_lockref.count via dget in d_alloc(), released in __dentry_kill()) and prevent the parent from being removed from the dentry cache. The one exception is delayed iputs. Ordered extent creation calls igrab() on the inode. If the file is unlinked and closed while those refs are held, iput() in __dentry_kill() decrements i_count but does not trigger eviction (i_count > 0). The child dentry is freed and the subvol dentry's d_lockref.count drops to 0, making it evictable while the inode is still alive. Since there are two races (the race between writeback and unlink and the race between lookup and delayed iputs), and there are too many moving parts, the following three diagrams show the complete picture. (Only the second and third are races) Phase 1: Create Subvol in dentry cache without BTRFS_ROOT_ORPHAN_CLEANUP set btrfs_mksubvol() lookup_one_len() __lookup_slow() d_alloc_parallel() __d_alloc() // d_lockref.count = 1 create_subvol(dentry) // doesn't touch the bit.. d_instantiate_new(dentry, inode) // dentry in cache with d_lockref.c ---truncated---	5.5	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: esp: fix skb leak with espintcp and async crypto When the		

2026-31518	TX queue for espintcp is full, esp_output_tail_tcp will return an error and not free the skb, because with synchronous crypto, the common xfrm output code will drop the packet for us. With async crypto (esp_output_done), we need to drop the skb when esp_output_tail_tcp returns an error.	5.5	More Details
CVE-2026-6843	A flaw was found in nano. A local user could exploit a format string vulnerability in the `statusline()` function. By creating a directory with a name containing `printf` specifiers, the application attempts to display this name, leading to a segmentation fault (SEGV). This results in a Denial of Service (DoS) for the `nano` application.	5.5	More Details
CVE-2026-31522	In the Linux kernel, the following vulnerability has been resolved: HID: magicmouse: avoid memory leak in magicmouse_report_fixup() The magicmouse_report_fixup() function was returning a newly kmemdup()-allocated buffer, but never freeing it. The caller of report_fixup() does not take ownership of the returned pointer, but it *is* permitted to return a sub-portion of the input rdesc, whose lifetime is managed by the caller.	5.5	More Details
CVE-2026-41177	Squidex is an open source headless content management system and content management hub. Prior to version 7.23.0, the Squidex Restore API is vulnerable to Blind Server-Side Request Forgery (SSRF). The application fails to validate the URI scheme of the user-supplied `Url` parameter, allowing the use of the `file://` protocol. This allows an authenticated administrator to force the backend server to interact with the local filesystem, which can lead to Local File Interaction (LFI) and potential disclosure of sensitive system information through side-channel analysis of internal logs. Version 7.23.0 contains a fix.	5.5	More Details
CVE-2026-35340	A flaw in the ChownExecutor used by uutils coreutils chown and chgrp causes the utilities to return an incorrect exit code during recursive operations. The final exit code is determined only by the last file processed. If the last operation succeeds, the command returns 0 even if earlier ownership or group changes failed due to permission errors. This can lead to security misconfigurations where administrative scripts incorrectly assume that ownership has been successfully transferred across a directory tree.	5.5	More Details
CVE-2026-31517	In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: fix skb_put() panic on non-linear skb during reassembly In iptfs_reassem_cont(), IP-TFS attempts to append data to the new inner packet 'newskb' that is being reassembled. First a zero-copy approach is tried if it succeeds then newskb becomes non-linear. When a subsequent fragment in the same datagram does not meet the fast-path conditions, a memory copy is performed. It calls skb_put() to append the data and as newskb is non-linear it triggers SKB_LINEAR_ASSERT check. Oops: invalid opcode: 0000 [#1] SMP NOPTI [...] RIP: 0010:skb_put+0x3c/0x40 [...] Call Trace: <IRQ> iptfs_reassem_cont+0x1ab/0x5e0 [xfrm_iptfs] iptfs_input_ordered+0x2af/0x380 [xfrm_iptfs] iptfs_input+0x122/0x3e0 [xfrm_iptfs] xfrm_input+0x91e/0x1a50 xfrm4_esp_rcv+0x3a/0x110 ip_protocol_deliver_rcu+0x1d7/0x1f0 ip_local_deliver_finish+0xbe/0x1e0 __netif_receive_skb_core.constprop.0+0xb56/0x1120 __netif_receive_skb_list_core+0x133/0x2b0 netif_receive_skb_list_internal+0x1ff/0x3f0 napi_complete_done+0x81/0x220 virtnet_poll+0x9d6/0x116e [virtio_net] __napi_poll.constprop.0+0x2b/0x270 net_rx_action+0x162/0x360 handle_softirqs+0xdc/0x510 __irq_exit_rcu+0xe7/0x110 irq_exit_rcu+0xe/0x20 common_interrupt+0x85/0xa0 </IRQ> <TASK> Fix this by checking if the skb is non-linear. If it is, linearize it by calling skb_linearize(). As the initial allocation of newskb originally reserved enough tailroom for the entire reassembled packet we do not need to check if we have enough tailroom or extend it.	5.5	More Details
CVE-2018-25285	Fathom 2.4 contains a buffer overflow vulnerability in the Authorization Code field that allows local attackers to crash the application by submitting an oversized input string. Attackers can paste a 6000-byte payload into the Authorization Code field and click Activate to trigger a denial of service condition.	5.5	More Details
CVE-2018-25281	iCash 7.6.5 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload through the Connect to Server dialog. Attackers can paste a 7000-byte string into the Host field and click Connect to trigger an application crash.	5.5	More Details
CVE-2018-25280	Infiltrator Network Security Scanner 4.6 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized input string. Attackers can paste a 6000-byte payload into the Scan Target field and trigger a denial of service condition when the Scan button is clicked.	5.5	More Details
CVE-2026-31509	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: fix circular locking dependency in nci_close_device nci_close_device() flushes rx_wq and tx_wq while holding req_lock. This causes a circular locking dependency because nci_rx_work() running on rx_wq can end up taking req_lock too: nci_rx_work -> nci_rx_data_packet -> nci_data_exchange_complete -> __sk_destruct -> rawsock_destruct -> nfc_deactivate_target -> nci_deactivate_target -> nci_request -> mutex_lock(&ndev->req_lock) Move the flush of rx_wq after req_lock has been released. This should safe (I think) because NCI_UP has already been cleared and the transport is closed, so the work will see it and return -ENETDOWN. NIPA has been hitting this running the nci selftest with a debug kernel on roughly 4% of the runs.	5.5	More Details
CVE-2026-31503	In the Linux kernel, the following vulnerability has been resolved: udp: Fix wildcard bind conflict check when using hash2 When binding a udp_sock to a local address and port, UDP uses two hashes (udptable->hash and udptable->hash2) for collision detection. The current code switches to "hash2" when hslot->count > 10. "hash2" is keyed by local address and local port. "hash" is keyed by local port only. The issue can be shown in the following bind sequence (pseudo code): bind(fd1, "[fd00::1]:8888") bind(fd2, "[fd00::2]:8888") bind(fd3, "[fd00::3]:8888") bind(fd4, "[fd00::4]:8888") bind(fd5, "[fd00::5]:8888") bind(fd6, "[fd00::6]:8888") bind(fd7, "[fd00::7]:8888") bind(fd8, "[fd00::8]:8888") bind(fd9, "[fd00::9]:8888") bind(fd10, "[fd00::10]:8888") /* Correctly return -EADDRINUSE because "hash" is used * instead of "hash2". udp_lib_lport_inuse() detects the * conflict. */ bind(fail_fd, "[::]:8888") /* After one more socket is bound to "[fd00::11]:8888", * hslot->count exceeds 10 and "hash2" is used instead. */ bind(fd11, "[fd00::11]:8888") bind(fail_fd, "[::]:8888") /* succeeds unexpectedly */ The same issue applies to the IPv4 wildcard address "0.0.0.0" and the IPv4-mapped wildcard address "::ffff:0.0.0.0". For example, if there are existing sockets bound to "192.168.1.[1-11]:8888", then binding "0.0.0.0:8888" or "[::ffff:0.0.0.0]:8888" can also miss the conflict when hslot->count > 10. TCP inet_csk_get_port() already has the correct check in inet_use_bhash2_on_bind(). Rename it to inet_use_hash2_on_bind() and move it to inet_hashtables.h so udp.c can reuse it in this fix.	5.5	More Details
CVE-2018-	RoboImport 1.2.0.72 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input to registration fields. Attackers can paste a 6000-byte buffer into the Registration Name and	5.5	More Details

25276	Registration Key fields and click Register to trigger an application crash.		
CVE-2026-31499	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix deadlock in l2cap_conn_del() l2cap_conn_del() calls cancel_delayed_work_sync() for both info_timer and id_addr_timer while holding conn->lock. However, the work functions l2cap_info_timeout() and l2cap_conn_update_id_addr() both acquire conn->lock, creating a potential AB-BA deadlock if the work is already executing when l2cap_conn_del() takes the lock. Move the work cancellations before acquiring conn->lock and use disable_delayed_work_sync() to additionally prevent the works from being rearmed after cancellation, consistent with the pattern used in hci_conn_del().	5.5	More Details
CVE-2026-31498	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix ERTM re-init and zero pdu_len infinite loop l2cap_config_req() processes CONFIG_REQ for channels in BT_CONNECTED state to support L2CAP reconfiguration (e.g. MTU changes). However, since both CONF_INPUT_DONE and CONF_OUTPUT_DONE are already set from the initial configuration, the reconfiguration path falls through to l2cap_ertm_init(), which re-initializes tx_q, srej_q, srej_list, and retrans_list without freeing the previous allocations and sets chan->sdu to NULL without freeing the existing skb. This leaks all previously allocated ERTM resources. Additionally, l2cap_parse_conf_req() does not validate the minimum value of remote_mps derived from the RFC max_pdu_size option. A zero value propagates to l2cap_segment_sdu() where pdu_len becomes zero, causing the while loop to never terminate since len is never decremented, exhausting all available memory. Fix the double-init by skipping l2cap_ertm_init() and l2cap_chan_ready() when the channel is already in BT_CONNECTED state, while still allowing the reconfiguration parameters to be updated through l2cap_parse_conf_req(). Also add a pdu_len zero check in l2cap_segment_sdu() as a safeguard.	5.5	More Details
CVE-2026-31531	In the Linux kernel, the following vulnerability has been resolved: ipv4: nexthop: allocate skb dynamically in rtm_get_nexthop() When querying a nexthop object via RTM_GETNEXTHOP, the kernel currently allocates a fixed-size skb using NLMSG_GOODSIZE. While sufficient for single nexthops and small Equal-Cost Multi-Path groups, this fixed allocation fails for large nexthop groups like 512 nexthops. This results in the following warning splat: WARNING: net/ipv4/nexthop.c:3395 at rtm_get_nexthop+0x176/0x1c0, CPU#20: rep/4608 [...] RIP: 0010:rtm_get_nexthop (net/ipv4/nexthop.c:3395) [...] Call Trace: <TASK> rtnetlink_rcv_msg (net/core/rtnetlink.c:6989) netlink_rcv_skb (net/netlink/af_netlink.c:2550) netlink_unicast (net/netlink/af_netlink.c:1319 net/netlink/af_netlink.c:1344) netlink_sendmsg (net/netlink/af_netlink.c:1894) ____sys_sendmsg (net/socket.c:721 net/socket.c:736 net/socket.c:2585) ___sys_sendmsg (net/socket.c:2641) __sys_sendmsg (net/socket.c:2671) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) </TASK> Fix this by allocating the size dynamically using nh_nlmsg_size() and using nlmsg_new(), this is consistent with nexthop_notify() behavior. In addition, adjust nh_nlmsg_size_grp() so it calculates the size needed based on flags passed. While at it, also add the size of NHA_FDB for nexthop group size calculation as it was missing too. This cannot be reproduced via iproute2 as the group size is currently limited and the command fails as follows: addattr_l ERROR: message exceeded bound of 1048	5.5	More Details
CVE-2026-31497	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: clamp SCO altsetting table indices btusb_work() maps the number of active SCO links to USB alternate settings through a three-entry lookup table when CVSD traffic uses transparent voice settings. The lookup currently indexes alts[] with data->sco_num - 1 without first constraining sco_num to the number of available table entries. While the table only defines alternate settings for up to three SCO links, data->sco_num comes from hci_conn_num() and is used directly. Cap the lookup to the last table entry before indexing it so the driver keeps selecting the highest supported alternate setting without reading past alts[].	5.5	More Details
CVE-2026-31496	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_expect: skip expectations in other netns via proc Skip expectations that do not reside in this netns. Similar to e77e6ff502ea ("netfilter: conntrack: do not dump other netns's conntrack entries via proc").	5.5	More Details
CVE-2026-4918	IBM Guardium Data Protection 12.1 is vulnerable to stored cross-site scripting. This vulnerability allows an administrative user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.5	More Details
CVE-2026-31495	In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: use netlink policy range checks Replace manual range and mask validations with netlink policy annotations in ctnetlink code paths, so that the netlink core rejects invalid values early and can generate extack errors. - CTA_PROTOINFO_TCP_STATE: reject values > TCP_CONNTRACK_SYN_SENT2 at policy level, removing the manual >= TCP_CONNTRACK_MAX check. - CTA_PROTOINFO_TCP_WSCALE_ORIGINAL/REPLY: reject values > TCP_MAX_WSCALE (14). The normal TCP option parsing path already clamps to this value, but the ctnetlink path accepted 0-255, causing undefined behavior when used as a u32 shift count. - CTA_FILTER_ORIG_FLAGS/REPLY_FLAGS: use NLA_POLICY_MASK with CTA_FILTER_F_ALL, removing the manual mask checks. - CTA_EXPECT_FLAGS: use NLA_POLICY_MASK with NF_CT_EXPECT_MASK, adding a new mask define grouping all valid expect flags. Extracted from a broader nf-next patch by Florian Westphal, scoped to ctnetlink for the fixes tree.	5.5	More Details
CVE-2026-31492	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Initialize free_qp completion before using it In irdma_create_qp, if ib_copy_to_udata fails, it will call irdma_destroy_qp to clean up which will attempt to wait on the free_qp completion, which is not initialized yet. Fix this by initializing the completion before the ib_copy_to_udata call.	5.5	More Details
CVE-2018-25296	P10 Central Management Software 1.4.13 contains a buffer overflow vulnerability in the login password field that allows local attackers to crash the application by submitting an oversized input string. Attackers can paste a 2000-byte payload into the password field and click login to trigger an application crash and denial of service.	5.5	More Details
CVE-2026-31491	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Harden depth calculation functions An issue was exposed where OS can pass in U32_MAX for SQ/RQ/SRQ size. This can cause integer overflow and truncation of SQ/RQ/SRQ depth returning a success when it should have failed. Harden the functions to do all depth calculations and boundary checking in u64 sizes.	5.5	More Details
CVE-2026-31487	In the Linux kernel, the following vulnerability has been resolved: spi: use generic driver_override infrastructure When a driver is probed through __driver_attach(), the bus' match() callback is called without the device lock held, thus accessing the driver_override field without a lock, which can cause a UAF. Fix this by using the driver-core driver_override infrastructure taking care of proper locking internally. Note that calling match() from __driver_attach() without the device lock held is intentional. [1] Also note that we do not enable the driver_override feature of struct bus_type, as SPI - in	5.5	More Details

	contrast to most other buses - passes "" to sysfs_emit() when the driver_override pointer is NULL. Thus, printing "\n" instead of "(null)\n".		
CVE-2026-31483	In the Linux kernel, the following vulnerability has been resolved: s390/syscalls: Add spectre boundary for syscall dispatch table The s390 syscall number is directly controlled by userspace, but does not have an array_index_nospec() boundary to prevent access past the syscall function pointer tables.	5.5	More Details
CVE-2026-31482	In the Linux kernel, the following vulnerability has been resolved: s390/entry: Scrub r12 register on kernel entry Before commit f33f2d4c7c80 ("s390/bp: remove TIF_ISOLATE_BP"), all entry handlers loaded r12 with the current task pointer (lg %r12,__LC_CURRENT) for use by the BPENTER/BPEXIT macros. That commit removed TIF_ISOLATE_BP, dropping both the branch prediction macros and the r12 load, but did not add r12 to the register clearing sequence. Add the missing xgr %r12,%r12 to make the register scrub consistent across all entry points.	5.5	More Details
CVE-2026-31481	In the Linux kernel, the following vulnerability has been resolved: tracing: Drain deferred trigger frees if kthread creation fails Boot-time trigger registration can fail before the trigger-data cleanup kthread exists. Deferring those frees until late init is fine, but the post-boot fallback must still drain the deferred list if kthread creation never succeeds. Otherwise, boot-deferred nodes can accumulate on trigger_data_free_list, later frees fall back to synchronously freeing only the current object, and the older queued entries are leaked forever. To trigger this, add the following to the kernel command line: trace_event=sched_switch trace_trigger=sched_switch.traceon,sched_switch.traceon The second traceon trigger will fail and be freed. This triggers a NULL pointer dereference and crashes the kernel. Keep the deferred boot-time behavior, but when kthread creation fails, drain the whole queued list synchronously. Do the same in the late-init drain path so queued entries are not stranded there either.	5.5	More Details
CVE-2026-31480	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix potential deadlock in cpu hotplug with osnoise The following sequence may leads deadlock in cpu hotplug: task1 task2 task3 ----- ----- ----- mutex_lock(&interface_lock) [CPU GOING OFFLINE] cpus_write_lock(); osnoise_cpu_die(); kthread_stop(task3); wait_for_completion(); osnoise_sleep(); mutex_lock(&interface_lock); cpus_read_lock(); [DEAD LOCK] Fix by swap the order of cpus_read_lock() and mutex_lock(&interface_lock).	5.5	More Details
CVE-2026-31472	In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: validate inner IPv4 header length in IPTFS payload Add validation of the inner IPv4 packet tot_len and ihl fields parsed from decrypted IPTFS payloads in __input_process_payload(). A crafted ESP packet containing an inner IPv4 header with tot_len=0 causes an infinite loop: iplen=0 leads to capturelen=min(0, remaining)=0, so the data offset never advances and the while(data < tail) loop never terminates, spinning forever in softirq context. Reject inner IPv4 packets where tot_len < ihl*4 or ihl*4 < sizeof(struct iphdr), which catches both the tot_len=0 case and malformed ihl values. The normal IP stack performs this validation in ip_rcv_core(), but IPTFS extracts and processes inner packets before they reach that layer.	5.5	More Details
CVE-2026-31510	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix null-ptr-deref on l2cap_sock_ready_cb Before using sk pointer, check if it is null. Fix the following: KASAN: null-ptr-deref in range [0x0000000000000260-0x0000000000000267] CPU: 0 UID: 0 PID: 5985 Comm: kworker/0:5 Not tainted 7.0.0-rc4-00029-ga989fde763f4 #1 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-9.fc43 06/10/2025 Workqueue: events l2cap_info_timeout RIP: 0010:kasan_byte_accessible+0x12/0x30 Code: 79 ff ff ff 0f 1f 40 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 0f 1f 40 d6 48 c1 ef 03 48 b8 00 00 00 00 00 fc ff df <0f> b6 04 07 3c 08 0f 92 c0 c3 cc cce veth0_macvtap: entered promiscuous mode RSP: 0018:ffffc90006e0f808 EFLAGS: 00010202 RAX: dfffffc0000000000 RBX: ffffffff89746018 RCX: 0000000080000001 RDX: 0000000000000000 RSI: ffffffff89746018 RDI: 000000000000004c RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: dfffffc0000000000 R11: ffffffff8aae3e70 R12: 0000000000000000 R13: 0000000000000260 R14: 0000000000000260 R15: 0000000000000001 FS: 0000000000000000(0000) GS:ffff8880983c2000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00005582615a5008 CR3: 000000007007e000 CR4: 0000000000752ef0 PKRU: 55555554 Call Trace: <TASK> __kasan_check_byte+0x12/0x40 lock_acquire+0x79/0x2e0 lock_sock_nested+0x48/0x100 ? l2cap_sock_ready_cb+0x46/0x160 l2cap_sock_ready_cb+0x46/0x160 l2cap_conn_start+0x779/0xff0 ? __pfx_l2cap_conn_start+0x10/0x10 ? l2cap_info_timeout+0x60/0xa0 ? __pfx___mutex_lock+0x10/0x10 l2cap_info_timeout+0x68/0xa0 ? process_scheduled_works+0xa8d/0x18c0 process_scheduled_works+0xb6e/0x18c0 ? __pfx_process_scheduled_works+0x10/0x10 ? assign_work+0x3d5/0x5e0 worker_thread+0xa53/0xfc0 kthread+0x388/0x470 ? __pfx_worker_thread+0x10/0x10 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x51e/0xb90 ? __pfx_ret_from_fork+0x10/0x10 veth1_macvtap: entered promiscuous mode ? __switch_to+0xc7d/0x1450 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Modules linked in: ---[end trace 0000000000000000]--- batman_adv: batadv0: Interface activated: batadv_slave_0 batman_adv: batadv0: Interface activated: batadv_slave_1 netdevsim netdevsim7 netdevsim0: set [1, 0] type 2 family 0 port 6081 - 0 netdevsim netdevsim7 netdevsim1: set [1, 0] type 2 family 0 port 6081 - 0 netdevsim netdevsim7 netdevsim2: set [1, 0] type 2 family 0 port 6081 - 0 netdevsim netdevsim7 netdevsim3: set [1, 0] type 2 family 0 port 6081 - 0 RIP: 0010:kasan_byte_accessible+0x12/0x30 Code: 79 ff ff ff 0f 1f 40 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 0f 1f 40 d6 48 c1 ef 03 48 b8 00 00 00 00 00 fc ff df <0f> b6 04 07 3c 08 0f 92 c0 c3 cc cce ieee80211 phy39: Selected rate control algorithm 'minstrel_ht' RSP: 0018:ffffc90006e0f808 EFLAGS: 00010202 RAX: dfffffc0000000000 RBX: ffffffff89746018 RCX: 0000000080000001 RDX: 0000000000000000 RSI: ffffffff89746018 RDI: 000000000000004c RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: dfffffc0000000000 R11: ffffffff8aae3e70 R12: 0000000000000000 R13: 0000000000000260 R14: 0000000000000260 R15: 0000000000000001 FS: 0000000000000000(0000) GS:ffff8880983c2000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f7e16139e9c CR3: 000000000e74e000 CR4: 0000000000752ef0 PKRU: 55555554 Kernel panic - not syncing: Fatal exception	5.5	More Details
CVE-2026-31512	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Validate PDU length before reading SDU length in l2cap_ecred_data_rcv() l2cap_ecred_data_rcv() reads the SDU length field from skb->data using get_unaligned_le16() without first verifying that skb contains at least L2CAP_SDULEN_SIZE (2) bytes. When skb->len is less than 2, this reads past the valid data in the skb. The ERTM reassembly path correctly calls pskb_may_pull() before reading the SDU length (l2cap_reassemble_sdu, L2CAP_SAR_START case). Apply the same validation to the Enhanced Credit Based Flow Control data path.	5.5	More Details

CVE-2025-36074	IBM Security Verify Directory (Container) 10.0.0 through 10.0.0.3 IBM Security Verify Directory could be vulnerable to malicious file upload by not validating file type. A privileged user could upload malicious files into the system that can be sent to victims for performing further attacks against the system.	5.5	More Details
CVE-2026-6807	A vulnerability in GRASSMARLIN v3.2.1 allows crafted session data to trigger improper handling of XML input, which may result in unintended exposure of sensitive information. The flaw stems from insufficient hardening of the XML parsing process.	5.5	More Details
CVE-2026-31514	In the Linux kernel, the following vulnerability has been resolved: erofs: set fileio bio failed in short read case For file-backed mount, IO requests are handled by vfs_iocb_iter_read(). However, it can be interrupted by SIGKILL, returning the number of bytes actually copied. Unused folios in bio are unexpectedly marked as uptodate. vfs_read filemap_read filemap_get_pages filemap_readahead erofs_fileio_readahead erofs_fileio_rq_submit vfs_iocb_iter_read filemap_read filemap_get_pages <= detect signal erofs_fileio_ki_complete <= set all folios uptodate This patch addresses this by setting short read bio with an error directly.	5.5	More Details
CVE-2026-41366	OpenClaw before 2026.3.31 contains a local roots self-whitelisting vulnerability in appendLocalMediaParentRoots that allows model-initiated arbitrary host file read. Attackers can exploit improper media parent directory validation to exfiltrate credentials and access sensitive files.	5.5	More Details
CVE-2026-31515	In the Linux kernel, the following vulnerability has been resolved: af_key: validate families in pfkey_send_migrate() syzbot was able to trigger a crash in skb_put() [1] Issue is that pfkey_send_migrate() does not check old/new families, and that set_ipsecrequest() @family argument was truncated, thus possibly overfilling the skb. Validate families early, do not wait set_ipsecrequest(). [1] skbuff: skb_over_panic: text:ffffffff8a752120 len:392 put:16 head:ffff88802a4ad040 data:ffff88802a4ad040 tail:0x188 end:0x180 dev:<NULL> kernel BUG at net/core/skbuff.c:214 ! Call Trace: <TASK> skb_over_panic net/core/skbuff.c:219 [inline] skb_put+0x159/0x210 net/core/skbuff.c:2655 skb_put_zero include/linux/skbuff.h:2788 [inline] set_ipsecrequest net/key/af_key.c:3532 [inline] pfkey_send_migrate+0x1270/0x2e50 net/key/af_key.c:3636 km_migrate+0x155/0x260 net/xfrm/xfrm_state.c:2848 xfrm_migrate+0x2140/0x2450 net/xfrm/xfrm_policy.c:4705 xfrm_do_migrate+0x8ff/0xaa0 net/xfrm/xfrm_user.c:3150	5.5	More Details
CVE-2026-2717	The HTTP Headers plugin for WordPress is vulnerable to CRLF Injection in all versions up to, and including, 1.19.2. This is due to insufficient sanitization of custom header name and value fields before writing them to the Apache .htaccess file via `insert_with_markers()`. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary newline characters and additional Apache directives into the .htaccess configuration file via the 'Custom Headers' settings, leading to Apache configuration parse errors and potential site-wide denial of service.	5.5	More Details
CVE-2026-31526	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix exception exit lock checking for subprogs process_bpf_exit_full() passes check_lock = !curframe to check_resource_leak(), which is false in cases when bpf_throw() is called from a static subprog. This makes check_resource_leak() to skip validation of active_rcu_locks, active_preempt_locks, and active_irq_id on exception exits from subprogs. At runtime bpf_throw() unwinds the stack via ORC without releasing any user-acquired locks, which may cause various issues as the result. Fix by setting check_lock = true for exception exits regardless of curframe, since exceptions bypass all intermediate frame cleanup. Update the error message prefix to "bpf_throw" for exception exits to distinguish them from normal BPF_EXIT. Fix reject_subprog_with_rcu_read_lock test which was previously passing for the wrong reason. Test program returned directly from the subprog call without closing the RCU section, so the error was triggered by the unclosed RCU lock on normal exit, not by bpf_throw. Update __msg annotations for affected tests to match the new "bpf_throw" error prefix. The spin_lock case is not affected because they are already checked [1] at the call site in do_check_insn() before bpf_throw can run. [1] https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/tree/kernel/bpf/verifier.c?h=v7.0-rc4#n21098	5.5	More Details
CVE-2026-5942	Flaws in page lifecycle management allow document structure changes to desynchronize internal component states, causing subsequent operations to access invalidated objects and crash the program.	5.5	More Details
CVE-2026-31632	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix leak of rxgk context in rxgk_verify_response() Fix rxgk_verify_response() to clean up the rxgk context it creates.	5.5	More Details
CVE-2026-31661	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmsmac: Fix dma_free_coherent() size dma_alloc_consistent() may change the size to align it. The new size is saved in alloced. Change the free size to match the allocation size.	5.5	More Details
CVE-2026-31559	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Fix missing NULL checks for kstrdup() 1. Replace "of_find_node_by_path("/")" with "of_root" to avoid multiple calls to "of_node_put()". 2. Fix a potential kernel oops during early boot when memory allocation fails while parsing CPU model from device tree.	5.5	More Details
CVE-2026-31573	In the Linux kernel, the following vulnerability has been resolved: media: verisilicon: Fix kernel panic due to __initconst misuse Fix a kernel panic when probing the driver as a module: Unable to handle kernel paging request at virtual address ffffd9c18eb05000 of_find_matching_node_and_match+0x5c/0x1a0 hantro_probe+0x2f4/0x7d0 [hantro_vpu] The imx8mq_vpu_shared_resources array is referenced by variant structures through their shared_devices field. When built as a module, __initconst causes this data to be freed after module init, but it's later accessed during probe, causing a page fault. The imx8mq_vpu_shared_resources is referenced from non-init code, so keeping __initconst or __initconst_or_module here is wrong. Drop the __initconst annotation and let it live in the normal .rodata section. A bug of __initconst called from regular non-init probe code leading to bugs during probe deferrals or during unbind-bind cycles.	5.5	More Details
CVE-2026-31556	In the Linux kernel, the following vulnerability has been resolved: xfs: scrub: unlock dquot before early return in quota scrub xchk_quota_item can return early after calling xchk_fblock_process_error. When that helper returns false, the function returned immediately without dropping dq->q_qlock, which can leave the dquot lock held and risk lock leaks or deadlocks in later quota operations. Fix this by unlocking dq->q_qlock before the early return.	5.5	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: rxrpc: fix reference count leak in rxrpc_server_keyring()	5.5	More

31634	This patch fixes a reference count leak in rxrpc_server_keyring() by checking if rx->securities is already set.		Details
CVE-2026-31664	In the Linux kernel, the following vulnerability has been resolved: xfrm: clear trailing padding in build_polexpire() build_expire() clears the trailing padding bytes of struct xfrm_user_expire after setting the hard field via memset_after(), but the analogous function build_polexpire() does not do this for struct xfrm_user_polexpire. The padding bytes after the __u8 hard field are left uninitialized from the heap allocation, and are then sent to userspace via netlink multicast to XFRMNLGRP_EXPIRE listeners, leaking kernel heap memory contents. Add the missing memset_after() call, matching build_expire().	5.5	More Details
CVE-2026-31555	In the Linux kernel, the following vulnerability has been resolved: futex: Clear stale exiting pointer in futex_lock_pi() retry path Fuzzying/stressing futexes triggered: WARNING: kernel/futex/core.c:825 at wait_for_owner_exiting+0x7a/0x80, CPU#11: futex_lock_pi_s/524 When futex_lock_pi_atomic() sees the owner is exiting, it returns -EBUSY and stores a refcounted task pointer in 'exiting'. After wait_for_owner_exiting() consumes that reference, the local pointer is never reset to nil. Upon a retry, if futex_lock_pi_atomic() returns a different error, the bogus pointer is passed to wait_for_owner_exiting(). CPU0 CPU1 CPU2 futex_lock_pi(uaddr) // acquires the PI futex exit() futex_cleanup_begin() futex_state = EXITING; futex_lock_pi(uaddr) futex_lock_pi_atomic() attach_to_pi_owner() // observes EXITING *exiting = owner; // takes ref return -EBUSY wait_for_owner_exiting(-EBUSY, owner) put_task_struct(); // drops ref // exiting still points to owner goto retry; futex_lock_pi_atomic() lock_pi_update_atomic() cmpxchg(uaddr) *uaddr ^= WAITERS // whatever // value changed return -EAGAIN; wait_for_owner_exiting(-EAGAIN, exiting) // stale WARN_ON_ONCE(exiting) Fix this by resetting upon retry, essentially aligning it with requeue_pi.	5.5	More Details
CVE-2026-31660	In the Linux kernel, the following vulnerability has been resolved: nfc: pn533: allocate rx skb before consuming bytes pn532_receive_buf() reports the number of accepted bytes to the serdev core. The current code consumes bytes into recv_skb and may already hand a complete frame to pn533_recv_frame() before allocating a fresh receive buffer. If that alloc_skb() fails, the callback returns 0 even though it has already consumed bytes, and it leaves recv_skb as NULL for the next receive callback. That breaks the receive_buf() accounting contract and can also lead to a NULL dereference on the next skb_put_u8(). Allocate the receive skb lazily before consuming the next byte instead. If allocation fails, return the number of bytes already accepted.	5.5	More Details
CVE-2026-31574	In the Linux kernel, the following vulnerability has been resolved: clockevents: Add missing resets of the next_event_forced flag The prevention mechanism against timer interrupt starvation missed to reset the next_event_forced flag in a couple of places: - When the clock event state changes. That can cause the flag to be stale over a shutdown/startup sequence - When a non-forced event is armed, which then prevents rearming before that event. If that event is far out in the future this will cause missed timer interrupts. - In the suspend wakeup handler. That led to stalls which have been reported by several people. Add the missing resets, which fixes the problems for the reporters.	5.5	More Details
CVE-2026-31575	In the Linux kernel, the following vulnerability has been resolved: mm/userfaultfd: fix hugetlb fault mutex hash calculation In mfill_atomic_hugetlb(), linear_page_index() is used to calculate the page index for hugetlb_fault_mutex_hash(). However, linear_page_index() returns the index in PAGE_SIZE units, while hugetlb_fault_mutex_hash() expects the index in huge page units. This mismatch means that different addresses within the same huge page can produce different hash values, leading to the use of different mutexes for the same huge page. This can cause races between faulting threads, which can corrupt the reservation map and trigger the BUG_ON in resv_map_release(). Fix this by introducing hugetlb_linear_page_index(), which returns the page index in huge page granularity, and using it in place of linear_page_index().	5.5	More Details
CVE-2026-31551	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: Fix static_branch_dec() underflow for aql_disable. syzbot reported static_branch_dec() underflow in aql_enable_write(). [0] The problem is that aql_enable_write() does not serialise concurrent write()s to the debugfs. aql_enable_write() checks static_key_false(&aql_disable.key) and later calls static_branch_inc() or static_branch_dec(), but the state may change between the two calls. aql_disable does not need to track inc/dec. Let's use static_branch_enable() and static_branch_disable(). [0]: val == 0 WARNING: kernel/jump_label.c:311 at __static_key_slow_dec_cpuslocked.part.0+0x107/0x120 kernel/jump_label.c:311, CPU#0: syz.1.3155/20288 Modules linked in: CPU: 0 UID: 0 PID: 20288 Comm: syz.1.3155 Tainted: G U L syzkaller #0 PREEMPT(full) Tainted: [U]=USER, [L]=SOFTLOCKUP Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/24/2026 RIP: 0010:__static_key_slow_dec_cpuslocked.part.0+0x107/0x120 kernel/jump_label.c:311 Code: f2 c9 ff 5b 5d c3 cc cc cc cc e8 54 f2 c9 ff 48 89 df e8 ac f9 ff ff eb ad e8 45 f2 c9 ff 90 0f 0b 90 eb a2 e8 3a f2 c9 ff 90 <0f> 0b 90 eb 97 48 89 df e8 5c 4b 33 00 e9 36 ff ff ff 0f 1f 80 00 RSP: 0018:ffffc9000b9f7c10 EFLAGS: 00010293 RAX: 0000000000000000 RBX: ffffffff9b3e5d40 RCX: ffffffff823c57b4 RDX: ffff8880285a0000 RSI: ffffffff823c5846 RDI: ffff8880285a0000 RBP: 0000000000000000 R08: 0000000000000005 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: 000000000000000a R13: 1ffff9200173ef88 R14: 0000000000000001 R15: ffffc9000b9f7e98 FS: 00007f530dd726c0(0000) GS:ffff8881245e3000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000200000001140 CR3: 000000007cc4a000 CR4: 00000000003526f0 Call Trace: <TASK> __static_key_slow_dec_cpuslocked kernel/jump_label.c:297 [inline] __static_key_slow_dec kernel/jump_label.c:321 [inline] static_key_slow_dec+0x7c/0xc0 kernel/jump_label.c:336 aql_enable_write+0x2b2/0x310 net/mac80211/debugfs.c:343 short_proxy_write+0x133/0x1a0 fs/debugfs/file.c:383 vfs_write+0x2aa/0x1070 fs/read_write.c:684 ksys_pwrite64 fs/read_write.c:793 [inline] __do_sys_pwrite64 fs/read_write.c:801 [inline] __se_sys_pwrite64 fs/read_write.c:798 [inline] __x64_sys_pwrite64+0x1eb/0x250 fs/read_write.c:798 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xc9/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f530cf9aeb9 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f530dd72028 EFLAGS: 00000246 ORIG_RAX: 0000000000000012 RAX: ffffffffffffffda RBX: 00007f530d215fa0 RCX: 00007f530cf9aeb9 RDX: 0000000000000003 RSI: 0000000000000000 RDI: 0000000000000010 RBP: 00007f530d008c1f R08: 0000000000000000 R09: 0000000000000000 R10: 4200000000000005 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f530d216038 R14: 00007f530d215fa0 R15: 00007ffde89fb978 </TASK>	5.5	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix NULL i_assoc_inode dereference in nilfs_mdt_save_to_shadow_map The DAT inode's btree node cache (i_assoc_inode) is initialized lazily during btree operations. However, nilfs_mdt_save_to_shadow_map() assumes i_assoc_inode is already initialized when copying dirty pages to the shadow map during GC. If NILFS_IOCTL_CLEAN_SEGMENTS is called immediately after mount before any btree	5.5	More Details

31577	operation has occurred on the DAT inode, i_assoc_inode is NULL leading to a general protection fault. Fix this by calling nilfs_attach_btree_node_cache() on the DAT inode in nilfs_dat_read() at mount time, ensuring i_assoc_inode is always initialized before any GC operation can use it.		
CVE-2026-31628	In the Linux kernel, the following vulnerability has been resolved: x86/CPU: Fix FPDSS on Zen1 Zen1's hardware divider can leave, under certain circumstances, partial results from previous operations. Those results can be leaked by another, attacker thread. Fix that with a chicken bit.	5.5	More Details
CVE-2026-31579	In the Linux kernel, the following vulnerability has been resolved: wireguard: device: use exit_rtnl callback instead of manual rtnl_lock in pre_exit wg_netns_pre_exit() manually acquires rtnl_lock() inside the pernet .pre_exit callback. This causes a hung task when another thread holds rtnl_mutex - the cleanup_net workqueue (or the setup_net failure rollback path) blocks indefinitely in wg_netns_pre_exit() waiting to acquire the lock. Convert to .exit_rtnl, introduced in commit 7a60d91c690b ("net: Add ->exit_rtnl() hook to struct pernet_operations."), where the framework already holds RTNL and batches all callbacks under a single rtnl_lock()/rtnl_unlock() pair, eliminating the contention window. The rcu_assign_pointer(wg->creating_net, NULL) is safe to move from .pre_exit to .exit_rtnl (which runs after synchronize_rcu()) because all RCU readers of creating_net either use maybe_get_net() - which returns NULL for a dying namespace with zero refcount - or access net->user_ns which remains valid throughout the entire ops_undo_list sequence. [Jason: added __net_exit and __read_mostly annotations that were missing.]	5.5	More Details
CVE-2026-31639	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix key reference count leak from call->key When creating a client call in rxrpc_alloc_client_call(), the code obtains a reference to the key. This is never cleaned up and gets leaked when the call is destroyed. Fix this by freeing call->key in rxrpc_destroy_call(). Before the patch, it shows the key reference counter elevated: $ cat /proc/keys | grep afs@54321 1bffe9cd I--Q--i 8053480 4169w 3b010000 1000 1000 rxrpc afs@54321: ka $ After the patch, the invalidated key is removed when the code exits: $ cat /proc/keys | grep afs@54321 $	5.5	More Details
CVE-2026-31658	In the Linux kernel, the following vulnerability has been resolved: net: altera-tse: fix skb leak on DMA mapping error in tse_start_xmit() When dma_map_single() fails in tse_start_xmit(), the function returns NETDEV_TX_OK without freeing the skb. Since NETDEV_TX_OK tells the stack the packet was consumed, the skb is never freed, leaking memory on every DMA mapping failure. Add dev_kfree_skb_any() before returning to properly free the skb.	5.5	More Details
CVE-2026-31585	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: fix nfeeds state corruption on start_streaming failure syzbot reported a memory leak in vidtv_psi_service_desc_init [1]. When vidtv_start_streaming() fails inside vidtv_start_feed(), the nfeeds counter is left incremented even though no feed was actually started. This corrupts the driver state: subsequent start_feed calls see nfeeds > 1 and skip starting the mux, while stop_feed calls eventually try to stop a non-existent stream. This state corruption can also lead to memory leaks, since the mux and channel resources may be partially allocated during a failed start_streaming but never cleaned up, as the stop path finds dvb->streaming == false and returns early. Fix by decrementing nfeeds back when start_streaming fails, keeping the counter in sync with the actual number of active feeds. [1] BUG: memory leak unreferenced object 0xffff888145b50820 (size 32): comm "syz.0.17", pid 6068, jiffies 4294944486 backtrace (crc 90a0c7d4): vidtv_psi_service_desc_init+0x74/0x1b0 drivers/media/test-drivers/vidtv/vidtv_psi.c:288 vidtv_channel_s302m_init+0xb1/0x2a0 drivers/media/test-drivers/vidtv/vidtv_channel.c:83 vidtv_channels_init+0x1b/0x40 drivers/media/test-drivers/vidtv/vidtv_channel.c:524 vidtv_mux_init+0x516/0xbe0 drivers/media/test-drivers/vidtv/vidtv_mux.c:518 vidtv_start_streaming drivers/media/test-drivers/vidtv/vidtv_bridge.c:194 [inline] vidtv_start_feed+0x33e/0x4d0 drivers/media/test-drivers/vidtv/vidtv_bridge.c:239	5.5	More Details
CVE-2026-31562	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: dsi: Store driver data before invoking mipi_dsi_host_register The call to mipi_dsi_host_register triggers a callback to mtk_dsi_bind, which uses dev_get_drvdata to retrieve the mtk_dsi struct, so this structure needs to be stored inside the driver data before invoking it. As drvdata is currently uninitialized it leads to a crash when registering the DSI DRM encoder right after acquiring the mode_config.idr_mutex, blocking all subsequent DRM operations. Fixes the following crash during mediatek-drm probe (tested on Xiaomi Smart Clock x04g): Unable to handle kernel NULL pointer dereference at virtual address 0000000000000040 [...] Modules linked in: mediatek_drm(+) drm_display_helper cec drm_client_lib drm_dma_helper drm_kms_helper panel_simple [...] Call trace: drm_mode_object_add+0x58/0x98 (P) __drm_encoder_init+0x48/0x140 drm_encoder_init+0x6c/0xa0 drm_simple_encoder_init+0x20/0x34 [drm_kms_helper] mtk_dsi_bind+0x34/0x13c [mediatek_drm] component_bind_all+0x120/0x280 mtk_drm_bind+0x284/0x67c [mediatek_drm] try_to_bring_up_aggregate_device+0x23c/0x320 __component_add+0xa4/0x198 component_add+0x14/0x20 mtk_dsi_host_attach+0x78/0x100 [mediatek_drm] mipi_dsi_attach+0x2c/0x50 panel_simple_dsi_probe+0x4c/0x9c [panel_simple] mipi_dsi_drv_probe+0x1c/0x28 really_probe+0xc0/0x3dc __driver_probe_device+0x80/0x160 driver_probe_device+0x40/0x120 __device_attach_driver+0xbc/0x17c bus_for_each_drv+0x88/0xf0 __device_attach+0x9c/0x1cc device_initial_probe+0x54/0x60 bus_probe_device+0x34/0xa0 device_add+0x5b0/0x800 mipi_dsi_device_register_full+0xdc/0x16c mipi_dsi_host_register+0xc4/0x17c mtk_dsi_probe+0x10c/0x260 [mediatek_drm] platform_probe+0x5c/0xa4 really_probe+0xc0/0x3dc __driver_probe_device+0x80/0x160 driver_probe_device+0x40/0x120 __driver_attach+0xc8/0x1f8 bus_for_each_dev+0x7c/0xe0 driver_attach+0x24/0x30 bus_add_driver+0x11c/0x240 driver_register+0x68/0x130 __platform_register_drivers+0x64/0x160 mtk_drm_init+0x24/0x1000 [mediatek_drm] do_one_initcall+0x60/0x1d0 do_init_module+0x54/0x240 load_module+0x1838/0x1dc0 init_module_from_file+0xd8/0xf0 __arm64_sys_finit_module+0x1b4/0x428 invoke_syscall.constprop.0+0x48/0xc8 do_el0_svc+0x3c/0xb8 el0_svc+0x34/0xe8 el0t_64_sync_handler+0xa0/0xe4 el0t_64_sync+0x198/0x19c Code: 52800022 941004ab 2a0003f3 37f80040 (29005a80)	5.5	More Details
CVE-2026-31565	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Fix deadlock during netdev reset with active connections Resolve deadlock that occurs when user executes netdev reset while RDMA applications (e.g., rping) are active. The netdev reset causes ice driver to remove irdma auxiliary driver, triggering device_delete and subsequent client removal. During client removal, uverbs_client waits for QP reference count to reach zero while cma_client holds the final reference, creating circular dependency and indefinite wait in iWARP mode. Skip QP reference count wait during device reset to prevent deadlock.	5.5	More Details
CVE-2026-31645	In the Linux kernel, the following vulnerability has been resolved: net: lan966x: fix page pool leak in error paths lan966x_fdma_rx_alloc() creates a page pool but does not destroy it if the subsequent fdma_alloc_coherent() call fails, leaking the pool. Similarly, lan966x_fdma_init() frees the coherent DMA memory when lan966x_fdma_tx_alloc() fails but does not destroy the page pool that was successfully created by lan966x_fdma_rx_alloc(), leaking it. Add the missing	5.5	More Details

	page_pool_destroy() calls in both error paths.		
CVE-2026-31646	In the Linux kernel, the following vulnerability has been resolved: net: lan966x: fix page_pool error handling in lan966x_fdma_rx_alloc_page_pool() page_pool_create() can return an ERR_PTR on failure. The return value is used unconditionally in the loop that follows, passing the error pointer through xdp_rxq_info_reg_mem_model() into page_pool_use_xdp_mem(), which dereferences it, causing a kernel oops. Add an IS_ERR check after page_pool_create() to return early on failure.	5.5	More Details
CVE-2026-31642	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix call removal to use RCU safe deletion Fix rxrpc call removal from the rxnet->calls list to use list_del_rcu() rather than list_del_init() to prevent stuffing up reading /proc/net/rxrpc/calls from potentially getting into an infinite loop. This, however, means that list_empty() no longer works on an entry that's been deleted from the list, making it harder to detect prior deletion. Fix this by: Firstly, make rxrpc_destroy_all_calls() only dump the first ten calls that are unexpectedly still on the list. Limiting the number of steps means there's no need to call cond_resched() or to remove calls from the list here, thereby eliminating the need for rxrpc_put_call() to check for that. rxrpc_put_call() can then be fixed to unconditionally delete the call from the list as it is the only place that the deletion occurs.	5.5	More Details
CVE-2026-31647	In the Linux kernel, the following vulnerability has been resolved: idpf: fix PREEMPT_RT raw/bh spinlock nesting for async VC handling Switch from using the completion's raw spinlock to a local lock in the idpf_vc_xn struct. The conversion is safe because complete/_all() are called outside the lock and there is no reason to share the completion lock in the current logic. This avoids invalid wait context reported by the kernel due to the async handler taking BH spinlock: [805.726977] ============================= [805.726991] [BUG: Invalid wait context] [805.727006] 7.0.0-rc2-net-devq-031026+ #28 Tainted: G S OE [805.727026] ----------------------------- [805.727038] kworker/u261:0/572 is trying to lock: [805.727051] ff190da6a8dbb6a0 (&vport_config->mac_filter_list_lock){+...}-{3:3}, at: idpf_mac_filter_async_handler+0xe9/0x260 [idpf] [805.727099] other info that might help us debug this: [805.727111] context-{5:5} [805.727119] 3 locks held by kworker/u261:0/572: [805.727132] #0: ff190da6db3e6148 ((wq_completion)idpf-0000:83:00.0-mbx){+.+.}-{0:0}, at: process_one_work+0x4b5/0x730 [805.727163] #1: ff3c6f0a6131fe50 ((work_completion)(&(&adapter->mbx_task)->work)){+.+.}-{0:0}, at: process_one_work+0x1e5/0x730 [805.727191] #2: ff190da765190020 (&x->wait#34){+.+.}-{2:2}, at: idpf_recv_mb_msg+0xc8/0x710 [idpf] [805.727218] stack backtrace: ... [805.727238] Workqueue: idpf-0000:83:00.0-mbx idpf_mbx_task [idpf] [805.727247] Call Trace: [805.727249] <TASK> [805.727251] dump_stack_lvl+0x77/0xb0 [805.727259] __lock_acquire+0xb3b/0x2290 [805.727268] ? __irq_work_queue_local+0x59/0x130 [805.727275] lock_acquire+0xc6/0x2f0 [805.727277] ? idpf_mac_filter_async_handler+0xe9/0x260 [idpf] [805.727284] ? _printk+0x5b/0x80 [805.727290] _raw_spin_lock_bh+0x38/0x50 [805.727298] ? idpf_mac_filter_async_handler+0xe9/0x260 [idpf] [805.727303] idpf_mac_filter_async_handler+0xe9/0x260 [idpf] [805.727310] idpf_recv_mb_msg+0x1c8/0x710 [idpf] [805.727317] process_one_work+0x226/0x730 [805.727322] worker_thread+0x19e/0x340 [805.727325] ? __pfx_worker_thread+0x10/0x10 [805.727328] kthread+0xf4/0x130 [805.727333] ? __pfx_kthread+0x10/0x10 [805.727336] ret_from_fork+0x32c/0x410 [805.727345] ? __pfx_kthread+0x10/0x10 [805.727347] ret_from_fork_asm+0x1a/0x30 [805.727354] </TASK>	5.5	More Details
CVE-2026-31564	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Fix base address calculation in kvm_eiointc_regs_access() In function kvm_eiointc_regs_access(), the register base address is caculated from array base address plus offset, the offset is absolute value from the base address. The data type of array base address is u64, it should be converted into the "void *" type and then plus the offset.	5.5	More Details
CVE-2026-31651	In the Linux kernel, the following vulnerability has been resolved: mmc: vub300: fix NULL-deref on disconnect Make sure to deregister the controller before dropping the reference to the driver data on disconnect to avoid NULL-pointer dereferences or use-after-free.	5.5	More Details
CVE-2026-31571	In the Linux kernel, the following vulnerability has been resolved: drm/i915: Unlink NV12 planes earlier unlink_nv12_plane() will clobber parts of the plane state potentially already set up by plane_atomic_check(), so we must make sure not to call the two in the wrong order. The problem happens when a plane previously selected as a Y plane is now configured as a normal plane by user space. plane_atomic_check() will first compute the proper plane state based on the userspace request, and unlink_nv12_plane() later clears some of the state. This used to work on account of unlink_nv12_plane() skipping the state clearing based on the plane visibility. But I removed that check, thinking it was an impossible situation. Now when that situation happens unlink_nv12_plane() will just WARN and proceed to clobber the state. Rather than reverting to the old way of doing things, I think it's more clear if we unlink the NV12 planes before we even compute the new plane state. (cherry picked from commit 017ecd04985573eeeb0745fa2c23896fb22ee0cc)	5.5	More Details
CVE-2026-31561	In the Linux kernel, the following vulnerability has been resolved: x86/cpu: Remove X86_CR4_FRED from the CR4 pinned bits mask Commit in Fixes added the FRED CR4 bit to the CR4 pinned bits mask so that whenever something else modifies CR4, that bit remains set. Which in itself is a perfectly fine idea. However, there's an issue when during boot FRED is initialized: first on the BSP and later on the APs. Thus, there's a window in time when exceptions cannot be handled. This becomes particularly nasty when running as SEV-{ES,SNP} or TDX guests which, when they manage to trigger exceptions during that short window described above, triple fault due to FRED MSRs not being set up yet. See Link tag below for a much more detailed explanation of the situation. So, as a result, the commit in that Link URL tried to address this shortcoming by temporarily disabling CR4 pinning when an AP is not online yet. However, that is a problem in itself because in this case, an attack on the kernel needs to only modify the online bit - a single bit in RW memory - and then disable CR4 pinning and then disable SM*P, leading to more and worse things to happen to the system. So, instead, remove the FRED bit from the CR4 pinning mask, thus obviating the need to temporarily disable CR4 pinning. If someone manages to disable FRED when poking at CR4, then idt_invalidate() would make sure the system would crash'n'burn on the first exception triggered, which is a much better outcome security-wise.	5.5	More Details
CVE-2026-31653	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: dealloc repeat_call_control if damon_call() fails damon_call() for repeat_call_control of DAMON_SYSFS could fail if somehow the kdamond is stopped before the damon_call(). It could happen, for example, when te damon context was made for monitroing of a virtual address processes, and the process is terminated immediately, before the damon_call() invocation. In the case, the dyanmically allocated repeat_call_control is not deallocated and leaked. Fix the leak by deallocating the repeat_call_control under the	5.5	More Details

	damon_call() failure. This issue is discovered by sashiko [1].		
CVE-2026-31654	In the Linux kernel, the following vulnerability has been resolved: mm/vma: fix memory leak in __mmap_region() commit 605f6586ecf7 ("mm/vma: do not leak memory when .mmap_prepare swaps the file") handled the success path by skipping get_file() via file_doesnt_need_get, but missed the error path. When /dev/zero is mmap'd with MAP_SHARED, mmap_zero_prepare() calls shmem_zero_setup_desc() which allocates a new shmem file to back the mapping. If __mmap_new_vma() subsequently fails, this replacement file is never fput()'d - the original is released by ksys_mmap_pgoff(), but nobody releases the new one. Add fput() for the swapped file in the error path. Reproducible with fault injection. FAULT_INJECTION: forcing a failure. name failslab, interval 1, probability 0, space 0, times 1 CPU: 2 UID: 0 PID: 366 Comm: syz.7.14 Not tainted 7.0.0-rc6 #2 PREEMPT(full) Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x164/0x1f0 should_fail_ex+0x525/0x650 should_failslab+0xdf/0x140 kmem_cache_alloc_noprof+0x78/0x630 vm_area_alloc+0x24/0x160 __mmap_region+0xf6b/0x2660 mmap_region+0x2eb/0x3a0 do_mmap+0xc79/0x1240 vm_mmap_pgoff+0x252/0x4c0 ksys_mmap_pgoff+0xf8/0x120 __x64_sys_mmap+0x12a/0x190 do_syscall_64+0xa9/0x580 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> kmemleak: 1 new suspected memory leaks (see /sys/kernel/debug/kmemleak) BUG: memory leak unreferenced object 0xffff8881118aca80 (size 360): comm "syz.7.14", pid 366, jiffies 4294913255 hex dump (first 32 bytes): 00 00 00 00 ad 4e ad de ff ff ff ff 00 00 00 00 .....N..... ff ff ff ff ff ff ff ff c0 28 4d ae ff ff ff ff .....(M..... backtrace (crc db0f53bc): kmem_cache_alloc_noprof+0x3ab/0x630 alloc_empty_file+0x5a/0x1e0 alloc_file_pseudo+0x135/0x220 __shmem_file_setup+0x274/0x420 shmem_zero_setup_desc+0x9c/0x170 mmap_zero_prepare+0x123/0x140 __mmap_region+0xdda/0x2660 mmap_region+0x2eb/0x3a0 do_mmap+0xc79/0x1240 vm_mmap_pgoff+0x252/0x4c0 ksys_mmap_pgoff+0xf8/0x120 __x64_sys_mmap+0x12a/0x190 do_syscall_64+0xa9/0x580 entry_SYSCALL_64_after_hwframe+0x76/0x7e Found by syzkaller.	5.5	More Details
CVE-2026-31567	In the Linux kernel, the following vulnerability has been resolved: PM: sleep: Drop spurious WARN_ON() from pm_restore_gfp_mask() Commit 35e4a69b2003f ("PM: sleep: Allow pm_restrict_gfp_mask() stacking") introduced refcount-based GFP mask management that warns when pm_restore_gfp_mask() is called with saved_gfp_count == 0. Some hibernation paths call pm_restore_gfp_mask() defensively where the GFP mask may or may not be restricted depending on the execution path. For example, the uswsusp interface invokes it in SNAPSHOT_CREATE_IMAGE, SNAPSHOT_UNFREEZE, and snapshot_release(). Before the stacking change this was a silent no-op; it now triggers a spurious WARNING. Remove the WARN_ON() wrapper from the !saved_gfp_count check while retaining the check itself, so that defensive calls remain harmless without producing false warnings. [rjw: Subject tweak]	5.5	More Details
CVE-2026-31655	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx8mp-blk-ctrl: Keep the NOC_HDCP clock enabled Keep the NOC_HDCP clock always enabled to fix the potential hang caused by the NoC ADB400 port power down handshake.	5.5	More Details
CVE-2026-31560	In the Linux kernel, the following vulnerability has been resolved: spi: spi-dw-dma: fix print error log when wait finish transaction If an error occurs, the device may not have a current message. In this case, the system will crash. In this case, it's better to use dev from the struct ctlr (struct spi_controller*).	5.5	More Details
CVE-2026-31670	In the Linux kernel, the following vulnerability has been resolved: net: rfkill: prevent unlimited numbers of rfkill events from being created Userspace can create an unlimited number of rfkill events if the system is so configured, while not consuming them from the rfkill file descriptor, causing a potential out of memory situation. Prevent this from bounding the number of pending rfkill events at a "large" number (i.e. 1000) to prevent abuses like this.	5.5	More Details
CVE-2026-31550	In the Linux kernel, the following vulnerability has been resolved: pmdomain: bcm: bcm2835-power: Increase ASB control timeout The bcm2835_asb_control() function uses a tight polling loop to wait for the ASB bridge to acknowledge a request. During intensive workloads, this handshake intermittently fails for V3D's master ASB on BCM2711, resulting in "Failed to disable ASB master for v3d" errors during runtime PM suspend. As a consequence, the failed power-off leaves V3D in a broken state, leading to bus faults or system hangs on later accesses. As the timeout is insufficient in some scenarios, increase the polling timeout from 1us to 5us, which is still negligible in the context of a power domain transition. Also, replace the open-coded ktime_get_ns()/ cpu_relax() polling loop with readl_poll_timeout_atomic().	5.5	More Details
CVE-2026-31625	In the Linux kernel, the following vulnerability has been resolved: HID: alps: fix NULL pointer dereference in alps_raw_event() Commit ecfa6f34492c ("HID: Add HID_CLAIMED_INPUT guards in raw_event callbacks missing them") attempted to fix up the HID drivers that had missed the previous fix that was done in 2ff5baa9b527 ("HID: appleir: Fix potential NULL dereference at raw event handle"), but the alps driver was missed. Fix this up by properly checking in the hid-alps driver that it had been claimed correctly before attempting to process the raw event.	5.5	More Details
CVE-2026-31624	In the Linux kernel, the following vulnerability has been resolved: HID: core: clamp report_size in s32ton() to avoid undefined shift s32ton() shifts by n-1 where n is the field's report_size, a value that comes directly from a HID device. The HID parser bounds report_size only to <= 256, so a broken HID device can supply a report descriptor with a wide field that triggers shift exponents up to 256 on a 32-bit type when an output report is built via hid_output_field() or hid_set_field(). Commit ec61b41918587 ("HID: core: fix shift-out-of-bounds in hid_report_raw_event") added the same n > 32 clamp to the function snto32(), but s32ton() was never given the same fix as I guess syzbot hadn't figured out how to fuzz a device the same way. Fix this up by just clamping the max value of n, just like snto32() does.	5.5	More Details
CVE-2026-6862	A flaw was found in libefiboot, a component of efivar. The device path node parser in libefiboot fails to validate that each node's Length field is at least 4 bytes, which is the minimum size for an EFI (Extensible Firmware Interface) device path node header. A local user could exploit this vulnerability by providing a specially crafted device path node. This can lead to infinite recursion, causing stack exhaustion and a process crash, resulting in a denial of service (DoS).	5.5	More Details
CVE-2026-31537	In the Linux kernel, the following vulnerability has been resolved: smb: server: make use of smbdirect_socket.send_io.bcredits It turns out that our code will corrupt the stream of reassabled data transfer messages when we trigger an immendiate (empty) send. In order to fix this we'll have a single 'batch' credit per connection. And code getting that credit is free to use as much messages until remaining_length reaches 0, then the batch credit it given back and the next logical send can happen.	5.5	More Details

CVE-2026-6840	Missing bounds validation for operator could allow out of range operator-code lookup during model loading Affected version is prior to commit 1.30.0.	5.5	More Details
CVE-2026-31619	In the Linux kernel, the following vulnerability has been resolved: ALSA: fireworks: bound device-supplied status before string array lookup The status field in an EFW response is a 32-bit value supplied by the firewire device. efr_status_names[] has 17 entries so a status value outside that range goes off into the weeds when looking at the %s value. Even worse, the status could return EFR_STATUS_INCOMPLETE which is 0x80000000, and is obviously not in that array of potential strings. Fix this up by properly bounding the index against the array size and printing "unknown" if it's not recognized.	5.5	More Details
CVE-2026-31618	In the Linux kernel, the following vulnerability has been resolved: fbdev: tdfxfb: avoid divide-by-zero on FBIOPUT_VSCREENINFO Much like commit 19f953e74356 ("fbdev: fb_pm2fb: Avoid potential divide by zero error"), we also need to prevent that same crash from happening in the udlfb driver as it uses pixclock directly when dividing, which will crash.	5.5	More Details
CVE-2026-31617	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ncm: validate minimum block_len in ncm_unwrap_ntb() The block_len read from the host-supplied NTB header is checked against ntb_max but has no lower bound. When block_len is smaller than opts->ndp_size, the bounds check of: ndp_index > (block_len - opts->ndp_size) will underflow producing a huge unsigned value that ndp_index can never exceed, defeating the check entirely. The same underflow occurs in the datagram index checks against block_len - opts->dpe_size. With those checks neutered, a malicious USB host can choose ndp_index and datagram offsets that point past the actual transfer, and the skb_put_data() copies adjacent kernel memory into the network skb. Fix this by rejecting block lengths that cannot hold at least the NTB header plus one NDP. This will make block_len - opts->ndp_size and block_len - opts->dpe_size both well-defined. Commit 8d2b1a1ec9f5 ("CDC-NCM: avoid overflow in sanity checking") fixed a related class of issues on the host side of NCM.	5.5	More Details
CVE-2026-5937	Insufficient parameter verification leads to the occurrence of format errors in files, which will trigger an unhandled "std::invalid_argument" exception, ultimately causing the program to terminate.	5.5	More Details
CVE-2026-31616	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_phonet: fix skb frags[] overflow in pn_rx_complete() A broken/bored/mean USB host can overflow the skb_shared_info->frags[] array on a Linux gadget exposing a Phonet function by sending an unbounded sequence of full-page OUT transfers. pn_rx_complete() finalizes the skb only when req->actual < req->length, where req->length is set to PAGE_SIZE by the gadget. If the host always sends exactly PAGE_SIZE bytes per transfer, fp->rx.skb will never be reset and each completion will add another fragment via skb_add_rx_frag(). Once nr_frags exceeds MAX_SKB_FRAGS (default 17), subsequent frag stores overwrite memory adjacent to the shinfo on the heap. Drop the skb and account a length error when the frag limit is reached, matching the fix applied in t7xx by commit f0813bcd2d9d ("net: wwan: t7xx: fix potential skb->frags overflow in RX path").	5.5	More Details
CVE-2026-5938	Improper control flow management allows a crafted document action chain to cause modal dialog reentry on the main thread, resulting in UI freeze and denial of service.	5.5	More Details
CVE-2026-31615	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: renesas_usb3: validate endpoint index in standard request handlers The GET_STATUS and SET/CLEAR_FEATURE handlers extract the endpoint number from the host-supplied wIndex without any sort of validation. Fix this up by validating the number of endpoints actually match up with the number the device has before attempting to dereference a pointer based on this math. This is just like what was done in commit ee0d382feb44 ("usb: gadget: aspeed_udc: validate endpoint index for ast udc") for the aspeed driver.	5.5	More Details
CVE-2026-31591	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Lock all vCPUs when synchronzing VMSAs for SNP launch finish Lock all vCPUs when synchronizing and encrypting VMSAs for SNP guests, as allowing userspace to manipulate and/or run a vCPU while its state is being synchronized would at best corrupt vCPU state, and at worst crash the host kernel. Opportunistically assert that vcpu->mutex is held when synchronizing its VMSA (the SEV-ES path already locks vCPUs).	5.5	More Details
CVE-2026-5939	A crafted XFA PDF can trigger a use-after-free condition during calculate event processing, causing the application to crash and resulting in an arbitrary code execution.	5.5	More Details
CVE-2026-1845	The Real Estate Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Protect *all* of sev_mem_enc_register_region() with kvm->lock Take and hold kvm->lock for before checking sev_guest() in sev_mem_enc_register_region(), as sev_guest() isn't stable unless kvm->lock is held (or KVM can guarantee KVM_SEV_INIT{2} has completed and can't rollack state). If KVM_SEV_INIT{2} fails, KVM can end up trying to add to a not-yet-initialized sev->regions_list, e.g. triggering a #GP Oops: general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 110 UID: 0 PID: 72717 Comm: syz.15.11462 Tainted: G U W O 6.16.0-smp-DEV #1 NONE Tainted: [U]=USER, [W]=WARN, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 12.52.0-0 10/28/2024 RIP: 0010:sev_mem_enc_register_region+0x3f0/0x4f0 ../include/linux/list.h:83 Code: <41> 80 3c 04 00 74 08 4c 89 ff e8 f1 c7 a2 00 49 39 ed 0f 84 c6 00 RSP: 0018:ffff88838647fbb8 EFLAGS: 00010256 RAX: dfffc0000000000 RBX: 1ffff92015cf1e0b RCX: dfffc0000000000 RDX: 0000000000000000 RSI: 0000000000001000 RDI: ffff888367870000 RBP: ffffc900ae78f050 R08: ffffea000d9e0007 R09: 1ffffd4001b3c000 R10: dfffc0000000000 R11: fffff94001b3c001 R12: 0000000000000000 R13: ffff8982ab0bde00 R14: ffffc900ae78f058 R15: 0000000000000000 FS: 00007f34e9dc66c0(0000) GS:ffff89ee64d33000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fe180adef98 CR3:		

CVE-2026-31592	000000047210e000 CR4: 0000000000350ef0 Call Trace: <TASK> kvm_arch_vm_ioctl+0xa72/0x1240 ../arch/x86/kvm/x86.c:7371 kvm_vm_ioctl+0x649/0x990 ../virt/kvm/kvm_main.c:5363 __se_sys_ioctl+0x101/0x170 ../fs/ioctl.c:51 do_syscall_x64 ../arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x6f/0x1f0 ../arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f34e9f7e9a9 Code: <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f34e9dc6038 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007f34ea1a6080 RCX: 00007f34e9f7e9a9 RDX: 0000200000000280 RSI: 000000008010aebb RDI: 0000000000000007 RBP: 00007f34ea000d69 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f34ea1a6080 R15: 00007ffce77197a8 </TASK> with a syzlang reproducer that looks like: syz_kvm_add_vcpu$x86(0x0, &(0x7f0000000040)={0x0, &(0x7f0000000180)=ANY=[], 0x70}) (async) syz_kvm_add_vcpu$x86(0x0, &(0x7f0000000080)={0x0, &(0x7f0000000180)=ANY=[@ANYBLOB="..."], 0x4f}) (async) r0 = openat$kvm(0xffffffffffffff9c, &(0x7f0000000200), 0x0, 0x0) r1 = ioctl$KVM_CREATE_VM(r0, 0xae01, 0x0) r2 = openat$kvm(0xffffffffffffff9c, &(0x7f0000000240), 0x0, 0x0) r3 = ioctl$KVM_CREATE_VM(r2, 0xae01, 0x0) ioctl$KVM_SET_CLOCK(r3, 0xc008aeba, &(0x7f0000000040)={0x1, 0x8, 0x0, 0x5625e9b0}) (async) ioctl$KVM_SET_PIT2(r3, 0x8010aebb, &(0x7f0000000280)={[...], 0x5}) (async) ioctl$KVM_SET_PIT2(r1, 0x4070aea0, 0x0) (async) r4 = ioctl$KVM_CREATE_VM(0xffffffffffffffff, 0xae01, 0x0) openat$kvm(0xffffffffffffff9c, 0x0, 0x0, 0x0) (async) ioctl$KVM_SET_USER_MEMORY_REGION(r4, 0x4020ae46, &(0x7f0000000400)={0x0, 0x0, 0x0, 0x2000, &(0x7f0000001000/0x2000)=nil}) (async) r5 = ioctl$KVM_CREATE_VCPU(r4, 0xae41, 0x2) close(r0) (async) openat$kvm(0xffffffffffffff9c, &(0x7f0000000000), 0x8000, 0x0) (async) ioctl$KVM_SET_GUEST_DEBUG(r5, 0x4048ae9b, &(0x7f0000000300)={0x4376ea830d46549b, 0x0, [0x46, 0x0, 0x0, 0x0, 0x0, 0x0, 0x1000]}) (async) ioctl$KVM_RUN(r5, 0xae80, 0x0) Opportunistically use guard() to avoid having to define a new error label and goto usage.	5.5	More Details
CVE-2026-35339	The recursive mode (-R) of the chmod utility in uutils coreutils incorrectly handles exit codes when processing multiple files. The final return value is determined solely by the success or failure of the last file processed. This allows the command to return an exit code of 0 (success) even if errors were encountered on previous files, such as 'Operation not permitted'. Scripts relying on these exit codes may proceed under a false sense of success while sensitive files remain with restrictive or incorrect permissions.	5.5	More Details
CVE-2026-31540	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Check set_default_submission() before deferencing When the i915 driver firmware binaries are not present, the set_default_submission pointer is not set. This pointer is dereferenced during suspend anyways. Add a check to make sure it is set before dereferencing. [23.289926] PM: suspend entry (deep) [23.293558] Filesystems sync: 0.000 seconds [23.298010] Freezing user space processes [23.302771] Freezing user space processes completed (elapsed 0.000 seconds) [23.309766] OOM killer disabled. [23.313027] Freezing remaining freezable tasks [23.318540] Freezing remaining freezable tasks completed (elapsed 0.001 seconds) [23.342038] serial 00:05: disabled [23.345719] serial 00:02: disabled [23.349342] serial 00:01: disabled [23.353782] sd 0:0:0:0: [sda] Synchronizing SCSI cache [23.358993] sd 1:0:0:0: [sdb] Synchronizing SCSI cache [23.361635] ata1.00: Entering standby power mode [23.368863] ata2.00: Entering standby power mode [23.445187] BUG: kernel NULL pointer dereference, address: 0000000000000000 [23.452194] #PF: supervisor instruction fetch in kernel mode [23.457896] #PF: error_code(0x0010) - not-present page [23.463065] PGD 0 P4D 0 [23.465640] Oops: Oops: 0010 [#1] SMP NOPTI [23.469869] CPU: 8 UID: 0 PID: 211 Comm: kworker/u48:18 Tainted: G S W 6.19.0-rc4-00020-gf0b9d8eb98df #10 PREEMPT(voluntary) [23.482512] Tainted: [S]=CPU_OUT_OF_SPEC, [W]=WARN [23.496511] Workqueue: async async_run_entry_fn [23.501087] RIP: 0010:0x0 [23.503755] Code: Unable to access opcode bytes at 0xffffffffffffffd6. [23.510324] RSP: 0018:ffffb4a60065fca8 EFLAGS: 00010246 [23.515592] RAX: 0000000000000000 RBX: ffff9f428290e000 RCX: 000000000000000f [23.522765] RDX: 0000000000000000 RSI: 0000000000000282 RDI: ffff9f428290e000 [23.529937] RBP: ffff9f4282907070 R08: ffff9f4281130428 R09: 00000000ffffffff [23.537111] R10: 0000000000000000 R11: 0000000000000001 R12: ffff9f42829070f8 [23.544284] R13: ffff9f4282906028 R14: ffff9f4282900000 R15: ffff9f4282906b68 [23.551457] FS: 0000000000000000(0000) GS:ffff9f466b2cf000(0000) knlGS:0000000000000000 [23.559588] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [23.565365] CR2: ffffffffffffffd6 CR3: 000000031c230001 CR4: 0000000000f70ef0 [23.572539] PKRU: 55555554 [23.575281] Call Trace: [23.577770] <TASK> [23.579905] intel_engines_reset_default_submission+0x42/0x60 [23.585695] __intel_gt_unset_wedged+0x191/0x200 [23.590360] intel_gt_unset_wedged+0x20/0x40 [23.594675] gt_sanitize+0x15e/0x170 [23.598290] i915_gem_suspend_late+0x6b/0x180 [23.602692] i915_drm_suspend_late+0x35/0xf0 [23.607008] ? __pfx_pci_pm_suspend_late+0x10/0x10 [23.611843] dpm_run_callback+0x78/0x1c0 [23.615817] device_suspend_late+0xde/0x2e0 [23.620037] async_suspend_late+0x18/0x30 [23.624082] async_run_entry_fn+0x25/0xa0 [23.628129] process_one_work+0x15b/0x380 [23.632182] worker_thread+0x2a5/0x3c0 [23.635973] ? __pfx_worker_thread+0x10/0x10 [23.640279] kthread+0xf6/0x1f0 [23.643464] ? __pfx_kthread+0x10/0x10 [23.647263] ? __pfx_kthread+0x10/0x10 [23.651045] ret_from_fork+0x131/0x190 [23.654837] ? __pfx_kthread+0x10/0x10 [23.658634] ret_from_fork_asm+0x1a/0x30 [23.662597] </TASK> [23.664826] Modules linked in: [23.667914] CR2: 0000000000000000 [23.671271] ----------[cut here]---------- (cherry picked from commit daa199abc3d3d1740c9e3a2c3e9216ae5b447cad)	5.5	More Details
CVE-2026-31542	In the Linux kernel, the following vulnerability has been resolved: x86/platform/uv: Handle deconfigured sockets When a socket is deconfigured, it's mapped to SOCK_EMPTY (0xffff). This causes a panic while allocating UV hub info structures. Fix this by using NUMA_NO_NODE, allowing UV hub info structures to be allocated on valid nodes.	5.5	More Details
CVE-2026-31590	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Drop WARN on large size for KVM_MEMORY_ENCRYPT_REG_REGION Drop the WARN in sev_pin_memory() on npages overflowing an int, as the WARN is comically trivially to trigger from userspace, e.g. by doing: struct kvm_enc_region range = { .addr = 0, .size = -1ul, }; __vm_ioctl(vm, KVM_MEMORY_ENCRYPT_REG_REGION, &range); Note, the checks in sev_mem_enc_register_region() that presumably exist to verify the incoming address+size are completely worthless, as both "addr" and "size" are u64s and SEV is 64-bit only, i.e. they _can't_ be greater than ULONG_MAX. That wart will be cleaned up in the near future. if (range->addr > ULONG_MAX || range->size > ULONG_MAX) return -EINVAL; Opportunistically add a comment to explain why the code calculates the number of pages the "hard" way, e.g. instead of just shifting @ulen.	5.5	More Details
CVE-2026-	The sort utility in uutils coreutils is vulnerable to a process panic when using the --files0-from option with inputs containing non-UTF-8 filenames. The implementation enforces UTF-8 encoding and utilizes expect(), causing an immediate crash when	5.5	More

35348	encountering valid but non-UTF-8 paths. This diverges from GNU sort, which treats filenames as raw bytes. A local attacker can exploit this to crash the utility and disrupt automated pipelines.		Details
CVE-2026-31671	In the Linux kernel, the following vulnerability has been resolved: xfrm_user: fix info leak in build_report() struct xfrm_user_report is a __u8 proto field followed by a struct xfrm_selector which means there is three "empty" bytes of padding, but the padding is never zeroed before copying to userspace. Fix that up by zeroing the structure before setting individual member variables.	5.5	More Details
CVE-2026-31623	In the Linux kernel, the following vulnerability has been resolved: net: usb: cdc-phonet: fix skb frags[] overflow in rx_complete() A malicious USB device claiming to be a CDC Phonet modem can overflow the skb_shared_info->frags[] array by sending an unbounded sequence of full-page bulk transfers. Drop the skb and increment the length error when the frag limit is reached. This matches the same fix that commit f0813bcd2d9d ("net: wwan: t7xx: fix potential skb->frags overflow in RX path") did for the t7xx driver.	5.5	More Details
CVE-2026-31672	In the Linux kernel, the following vulnerability has been resolved: wifi: rt2x00usb: fix devres lifetime USB drivers bind to USB interfaces and any device managed resources should have their lifetime tied to the interface rather than parent USB device. This avoids issues like memory leaks when drivers are unbound without their devices being physically disconnected (e.g. on probe deferral or configuration changes). Fix the USB anchor lifetime so that it is released on driver unbind.	5.5	More Details
CVE-2026-31543	In the Linux kernel, the following vulnerability has been resolved: crash_dump: don't log dm-crypt key bytes in read_key_from_user_keying When debug logging is enabled, read_key_from_user_keying() logs the first 8 bytes of the key payload and partially exposes the dm-crypt key. Stop logging any key bytes.	5.5	More Details
CVE-2026-31621	In the Linux kernel, the following vulnerability has been resolved: bnge: return after auxiliary_device_uninit() in error path When auxiliary_device_add() fails, the error block calls auxiliary_device_uninit() but does not return. The uninit drops the last reference and synchronously runs bnge_aux_dev_release(), which sets bd->auxr_dev = NULL and frees the underlying object. The subsequent bd->auxr_dev->net = bd->netdev then dereferences NULL, which is not a good thing to have happen when trying to clean up from an error. Add the missing return, as the auxiliary bus documentation states is a requirement (seems that LLM tools read documentation better than humans do...)	5.5	More Details
CVE-2026-31643	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix key parsing memleak In rxrpc_preparse_xdr_yfs_rxgk(), the memory attached to token->rxgk can be leaked in a few error paths after it's allocated. Fix this by freeing it in the "reject_token:" case.	5.5	More Details
CVE-2026-31549	In the Linux kernel, the following vulnerability has been resolved: i2c: cp2615: fix serial string NULL-deref at probe The cp2615 driver uses the USB device serial string as the i2c adapter name but does not make sure that the string exists. Verify that the device has a serial number before accessing it to avoid triggering a NULL-pointer dereference (e.g. with malicious devices).	5.5	More Details
CVE-2026-31547	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix missing runtime PM reference in ccs_mode_store ccs_mode_store() calls xe_gt_reset() which internally invokes xe_pm_runtime_get_noresume(). That function requires the caller to already hold an outer runtime PM reference and warns if none is held: [46.891177] xe 0000:03:00.0: [drm] Missing outer runtime PM protection [46.891178] WARNING: drivers/gpu/drm/xe/xe_pm.c:885 at xe_pm_runtime_get_noresume+0x8b/0xc0 Fix this by protecting xe_gt_reset() with the scope-based guard(xe_pm_runtime)(xe), which is the preferred form when the reference lifetime matches a single scope. v2: - Use scope-based guard(xe_pm_runtime)(xe) (Shuicheng) - Update commit message accordingly (cherry picked from commit 7937ea733f79b3f25e802a0c8360bf7423856f36)	5.5	More Details
CVE-2026-31546	In the Linux kernel, the following vulnerability has been resolved: net: bonding: fix NULL deref in bond_debug_rlb_hash_show rlb_clear_slave intentionally keeps RLB hash-table entries on the rx_hashtbl_used_head list with slave set to NULL when no replacement slave is available. However, bond_debug_rlb_hash_show visites client_info->slave without checking if it's NULL. Other used-list iterators in bond_alb.c already handle this NULL-slave state safely: - rlb_update_client returns early on !client_info->slave - rlb_req_update_slave_clients, rlb_clear_slave, and rlb_rebalance compare slave values before visiting - lb_req_update_subnet_clients continues if slave is NULL The following NULL deref crash can be trigger in bond_debug_rlb_hash_show: [1.289791] BUG: kernel NULL pointer dereference, address: 0000000000000000 [1.292058] RIP: 0010:bond_debug_rlb_hash_show (drivers/net/bonding/bond_debugfs.c:41) [1.293101] RSP: 0018:ffffc900004a7d00 EFLAGS: 00010286 [1.293333] RAX: 0000000000000000 RBX: ffff888102b48200 RCX: ffff888102b48204 [1.293631] RDX: ffff888102b48200 RSI: ffffffff839daad5 RDI: ffff888102815078 [1.293924] RBP: ffff888102815078 R08: ffff888102b4820e R09: 0000000000000000 [1.294267] R10: 0000000000000000 R11: 0000000000000000 R12: ffff888100f929c0 [1.294564] R13: ffff888100f92a00 R14: 0000000000000001 R15: ffffc900004a7ed8 [1.294864] FS: 0000000001395380(0000) GS:ffff888196e75000(0000) knlGS:0000000000000000 [1.295239] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [1.295480] CR2: 0000000000000000 CR3: 0000000102adc004 CR4: 0000000000772ef0 [1.295897] Call Trace: [1.296134] seq_read_iter (fs/seq_file.c:231) [1.296341] seq_read (fs/seq_file.c:164) [1.296493] full_proxy_read (fs/debugfs/file.c:378 (discriminator 1)) [1.296658] vfs_read (fs/read_write.c:572) [1.296981] ksys_read (fs/read_write.c:717) [1.297132] do_syscall_64 (arch/x86/entry/syscall_64.c:63 (discriminator 1) arch/x86/entry/syscall_64.c:94 (discriminator 1)) [1.297325] entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Add a NULL check and print "(none)" for entries with no assigned slave.	5.5	More Details
CVE-2026-31545	In the Linux kernel, the following vulnerability has been resolved: NFC: nxp-nci: allow GPIOs to sleep Allow the firmware and enable GPIOs to sleep. This fixes a `WARN_ON' and allows the driver to operate GPIOs which are connected to I2C GPIO expanders. -- >8 -- kernel: WARNING: CPU: 3 PID: 2636 at drivers/gpio/gpiolib.c:3880 gpiod_set_value+0x88/0x98 -- >8 --	5.5	More Details
CVE-2026-31544	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix NULL dereference on notify error path Since commit b5daf93b809d1 ("firmware: arm_scmi: Avoid notifier registration for unsupported events") the call chains leading to the helper __scmi_event_handler_get_ops expect an ERR_PTR to be returned on failure to get an handler for the requested event key, while the current helper can still return a NULL when no handler could be found or created. Fix by forcing an ERR_PTR return value when the handler reference is NULL.	5.5	More Details

CVE-2026-42421	OpenClaw before 2026.4.8 contains a session management vulnerability where existing WebSocket sessions survive shared gateway token rotation. Attackers can maintain unauthorized access to WebSocket connections after token rotation by exploiting the failure to disconnect existing shared-token sessions.	5.4	More Details
CVE-2026-41909	OpenClaw before 2026.4.20 contains an improper authorization vulnerability in paired-device pairing management that allows limited-scope sessions to enumerate and act on pairing requests. Attackers with paired-device access can approve or operate on unrelated pending device requests within the same gateway scope.	5.4	More Details
CVE-2026-41233	Froxlor is open source server administration software. Prior to version 2.3.6, in `Domains.add()`, the `adminid` parameter is accepted from user input and used without validation when the calling reseller does not have the `customers_see_all` permission. This allows a reseller to attribute newly created domains to any other admin, bypassing their own domain quota (since the wrong admin's `domains_used` counter is incremented) and potentially exhausting another admin's quota. Version 2.3.6 fixes the issue.	5.4	More Details
CVE-2026-2951	The Gutentor – Gutenberg Blocks – Page Builder for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2026-41467	ProjeQtor versions 7.0 through 12.4.3 contain a stored cross-site scripting vulnerability in the file upload functionality where the checkValidFileName() function fails to restrict HTML and HTM file uploads. Authenticated attackers can upload HTML files containing arbitrary JavaScript through the image upload or attachment endpoints, and any user accessing the uploaded file URL will execute the embedded JavaScript in their browser.	5.4	More Details
CVE-2026-41916	OpenClaw before 2026.4.8 contains an authentication state management vulnerability where the resolvedAuth closure becomes stale after configuration reload. Newly accepted gateway connections continue using outdated resolved auth state, allowing attackers to bypass authentication controls through config reload operations.	5.4	More Details
CVE-2026-7145	A weakness has been identified in mettle sendportal up to 3.0.1. Affected is the function destroy of the file app/Http/Controllers/Workspaces/WorkspaceInvitationsController.php of the component Invitation Handler. This manipulation of the argument invitation causes authorization bypass. The attack may be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-7024	A flaw has been found in rawchen sims up to 004f783b1db5ecdfad81c8fdc3b34171211112de. Affected by this issue is some unknown functionality of the file sims-master/src/web/servlet/file/DeleteFileServlet.java of the component deleteFileServlet Endpoint. Executing a manipulation of the argument filename can lead to path traversal. The attack can be launched remotely. The exploit has been published and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-3007	Successful exploitation of the stored cross-site scripting (XSS) vulnerability could allow an attacker to execute arbitrary JavaScript on any user account that has access to Koollab LMS' courselet feature.	5.4	More Details
CVE-2026-41466	ProjeQtor versions 7.0 through 12.4.3 contain a stored cross-site scripting vulnerability in the checkValidHtmlText() function within Security.php that fails to properly sanitize user input by only detecting specific patterns while returning unsanitized strings without output encoding. Attackers can inject malicious payloads that bypass the filter using alternative syntax such as img tags with event handlers, which are stored and executed in the browsers of users viewing the affected content.	5.4	More Details
CVE-2026-6515	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed a user to use invalidated or incorrectly scoped credentials to access Virtual Registries under certain conditions.	5.4	More Details
CVE-2026-5306	The Check & Log Email WordPress plugin before 2.0.13 does not properly handle email replacement, which could allow unauthenticated users to perform Stored XSS attacks when the email encoder setting is enabled	5.4	More Details
CVE-2026-41406	OpenClaw before 2026.3.31 contains a sender allowlist bypass vulnerability that allows remote attackers to access restricted messages. Attackers can exploit fetched quoted, root, and thread context messages to bypass sender allowlist restrictions and retrieve unauthorized content.	5.4	More Details
CVE-2026-41425	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to 1.6.11, there is no CSRF protection on the cache feature in authlib.integrations.starlette_client.OAuth. This vulnerability is fixed in 1.6.11.	5.4	More Details
CVE-2026-41318	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to version 1.12.1, AnythingLLM's in-chat markdown renderer has an unsafe custom rule for images that interpolates the markdown image's `alt` text into an HTML `alt="..."` attribute without any HTML encoding. Every call-site in the app wraps `renderMarkdown(...)` with `DOMPurify.sanitize(...)` as defense-in-depth — except the `Chartable` component, which renders chart captions with no sanitization. The chart caption is the natural-language text the LLM emits around a `create-chart` tool call, so any attacker who can influence the LLM's output — most cheaply via indirect prompt injection in a shared workspace document, or directly if they can create a chart record in a multi-user workspace — can trigger stored DOM-level XSS in every other user's browser when they open that conversation. AnythingLLM chat history is loaded server-side via `GET /api/workspace/:slug/chats` and rendered directly into the chat UI. Version 1.12.1 contains a patch for this issue.	5.4	More Details
CVE-2026-41382	OpenClaw before 2026.3.31 contains an authorization bypass vulnerability in Discord voice ingress that allows attackers to bypass channel and member allowlist restrictions. Attackers can exploit stale-role validation gaps and improper channel name validation to gain unauthorized access to restricted voice channels.	5.4	More Details

CVE-2026-30368	A client-side authorization flaw in Lightspeed Classroom v5.1.2.1763770643 allows unauthenticated attackers to impersonate users by bypassing integrity checks and abusing client-generated authorization tokens, leading to unauthorized control and monitoring of student devices.	5.4	More Details
CVE-2026-41381	OpenClaw before 2026.3.31 contains an access control bypass vulnerability in the Discord voice manager that allows attackers to bypass channel-level member access allowlist restrictions. Attackers can send Discord voice ingress requests before channel allowlist authorization is performed, gaining unauthorized access to restricted voice channels.	5.4	More Details
CVE-2026-25720	A vulnerability exists in SenseLive X3050's web management interface due to improper session lifetime enforcement, allowing authenticated sessions to remain active for extended periods without requiring re-authentication. An attacker with access to a previously authenticated session could continue interacting with administrative functions long after legitimate user activity has ceased.	5.4	More Details
CVE-2026-41356	OpenClaw before 2026.3.31 fails to terminate active WebSocket sessions when rotating device tokens. Attackers with previously compromised credentials can maintain unauthorized access through existing WebSocket connections after token rotation.	5.4	More Details
CVE-2026-38948	Cross-Site Scripting (XSS) vulnerability exists in FUEL CMS v1.5.2 and before within the asset upload functionality. The application fails to properly sanitize uploaded SVG files, allowing a low-privileged authenticated user to upload a crafted SVG file containing malicious code.	5.4	More Details
CVE-2026-41348	OpenClaw before 2026.3.31 contains an authorization bypass vulnerability in Discord slash command and autocomplete paths that fail to enforce group DM channel allowlist restrictions. Authorized Discord users can bypass channel restrictions by invoking slash commands, allowing access to restricted group DM channels.	5.4	More Details
CVE-2026-41358	OpenClaw before 2026.4.2 fails to filter Slack thread context by sender allowlist, allowing non-allowlisted messages to enter agent context. Attackers can inject unauthorized thread messages through allowlisted user replies to bypass sender access controls and manipulate model context.	5.4	More Details
CVE-2026-41376	OpenClaw before 2026.3.31 contains an allowlist bypass vulnerability in Matrix thread root and reply context handling that fails to properly validate message senders. Attackers can fetch thread-root and reply context messages that should be filtered by sender allowlists, bypassing access controls.	5.4	More Details
CVE-2026-41344	OpenClaw before 2026.3.28 contains a privilege escalation vulnerability in the chat.send endpoint that allows write-scoped gateway callers to persist admin-only verboseLevel session overrides. Attackers can exploit the /verbose parameter to bypass access controls and expose sensitive reasoning or tool output intended to be restricted to administrators.	5.4	More Details
CVE-2026-41341	OpenClaw before 2026.3.31 contains a logic error in Discord component interaction routing that misclassifies group direct messages as direct messages in extensions/discord/src/monitor/agent-components-helpers.ts. Attackers can exploit this misclassification to bypass group DM policy enforcement or trigger incorrect session handling.	5.4	More Details
CVE-2026-41365	OpenClaw before 2026.3.31 contains a sender allowlist bypass vulnerability in MS Teams thread history fetched via Graph API. Attackers can retrieve thread messages that should be filtered by sender allowlists, bypassing message filtering restrictions.	5.4	More Details
CVE-2026-6848	A flaw was found in Red Hat Quay. When Red Hat Quay requests password re-verification for sensitive operations, such as token generation or robot account creation, the re-authentication prompt can be bypassed. This allows a user with a timed-out session, or an attacker with access to an idle authenticated browser session, to perform privileged actions without providing valid credentials. The vulnerability enables unauthorized execution of sensitive operations despite the user interface displaying an error for invalid credentials.	5.4	More Details
CVE-2026-42042	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, the Axios library's XSRF token protection logic uses JavaScript truthy/falsy semantics instead of strict boolean comparison for the withXSRFToken config property. When this property is set to any truthy non-boolean value (via prototype pollution or misconfiguration), the same-origin check (isURLSameOrigin) is short-circuited, causing XSRF tokens to be sent to all request targets including cross-origin servers controlled by an attacker. This vulnerability is fixed in 1.15.1 and 0.31.1.	5.4	More Details
CVE-2026-41459	Xerte Online Toolkits versions 3.15 and earlier contain an information disclosure vulnerability that allows unauthenticated attackers to retrieve the full server-side filesystem path of the application root. Attackers can send a GET request to the /setup page to access the exposed root_path value rendered in the HTML response, which enables exploitation of path-dependent vulnerabilities such as relative path traversal in connector.php.	5.3	More Details
CVE-2026-42427	OpenClaw before 2026.4.8 contains a remote code execution vulnerability caused by missing environment variable denylist entries for HGRCPATH, CARGO_BUILD_RUSTC_WRAPPER, RUSTC_WRAPPER, and MAKEFLAGS. Attackers can inject malicious build tool environment variables to influence host exec commands and achieve arbitrary code execution.	5.3	More Details
CVE-2026-33609	Incomplete escaping of LDAP queries when running with 8bit-dns enabled allows users to perform queries of internal domain subtrees.	5.3	More Details
CVE-2026-33595	A client can trigger excessive memory allocation by generating a lot of errors responses over a single DoQ and DoH3 connection, as some resources were not properly released until the end of the connection.	5.3	More Details
CVE-2026-33594	A client can trigger excessive memory allocation by generating a lot of queries that are routed to an overloaded DoH backend, causing queries to accumulate into a buffer that will not be released until the end of the connection.	5.3	More Details
CVE-2026-	OpenClaw before 2026.3.31 performs Discord audio preflight transcription before validating member authorization, allowing unauthenticated attackers to consume resources. Remote attackers can trigger audio preflight processing without member	5.3	More Details

41374	allowlist validation to cause resource exhaustion.		
CVE-2026-33254	An attacker can create a large number of concurrent DoQ or DoH3 connections, causing unlimited memory allocation in DNSdist and leading to a denial of service. DOQ and DoH3 are disabled by default.	5.3	More Details
CVE-2026-7132	A vulnerability was found in code-projects Online Lot Reservation System up to 1.0. This affects the function readfile of the file /download.php. The manipulation of the argument File results in path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used.	5.3	More Details
CVE-2026-41182	LangSmith Client SDKs provide SDK's for interacting with the LangSmith platform. Prior to version 0.5.19 of the JavaScript SDK and version 0.7.31 of the Python SDK, the LangSmith SDK's output redaction controls (hideOutputs in JS, hide_outputs in Python) do not apply to streaming token events. When an LLM run produces streaming output, each chunk is recorded as a new_token event containing the raw token value. These events bypass the redaction pipeline entirely — prepareRunCreateOrUpdateInputs (JS) and _hide_run_outputs (Python) only process the inputs and outputs fields on a run, never the events array. As a result, applications relying on output redaction to prevent sensitive LLM output from being stored in LangSmith will still leak the full streamed content via run events. Version 0.5.19 of the JavaScript SDK and version 0.7.31 of the Python SDK fix the issue.	5.3	More Details
CVE-2026-34066	nimiq-blockchain provides persistent block storage for Nimiq's Rust implementation. Prior to version 1.3.0, `HistoryStore::put_historic_txns` uses an `assert!` to enforce invariants about `HistoricTransaction.block_number` (must be within the macro block being pushed and within the same epoch). During history sync, a peer can influence the `history: &[HistoricTransaction]` input passed into `Blockchain::push_history_sync`, and a malformed history list can violate these invariants and trigger a panic. `extend_history_sync` calls `this.history_store.add_to_history(..)` before comparing the computed history root against the macro block header (`block.history_root()`), so the panic can happen before later rejection checks run. The patch for this vulnerability is included as part of v1.3.0. No known workarounds are available.	5.3	More Details
CVE-2026-7135	A security flaw has been discovered in GPAC up to 26.03-DEV-rev105-g8f39a1eb3-master. Affected by this vulnerability is the function elng_box_read of the file src/isomedia/box_code_base.c of the component MP4Box. Performing a manipulation of the argument elng results in out-of-bounds read. The attack needs to be approached locally. The exploit has been released to the public and may be used for attacks. The patch is named cf6ac48c972eaaee2af270adc3f36615325deb3e. The affected component should be upgraded.	5.3	More Details
CVE-2026-34064	nimiq-account contains account primitives to be used in Nimiq's Rust implementation. Prior to version 1.3.0, `VestingContract::can_change_balance` returns `AccountError::InsufficientFunds` when `new_balance < min_cap`, but it constructs the error using `balance: self.balance - min_cap`. `Coin::sub` panics on underflow, so if an attacker can reach a state where `min_cap > balance`, the node crashes while trying to return an error. The `min_cap > balance` precondition is attacker-reachable because the vesting contract creation data (32-byte format) allows encoding `total_amount` without validating `total_amount <= transaction.value` (the real contract balance). After creating such a vesting contract, the attacker can broadcast an outgoing transaction to trigger the panic during mempool admission and block processing. The patch for this vulnerability is included as part of v1.3.0. No known workarounds are available.	5.3	More Details
CVE-2026-41391	OpenClaw before 2026.3.31 fails to properly sanitize PIP_INDEX_URL and UV_INDEX_URL environment variables in host execution contexts, allowing attackers to redirect Python package-index traffic. Attackers can exploit this bypass to intercept or manipulate package management operations by injecting malicious index URLs through unsanitized environment variables.	5.3	More Details
CVE-2026-34062	nimiq-libp2p is a Nimiq network implementation based on libp2p. Prior to version 1.3.0, `MessageCodec::read_request` and `read_response` call `read_to_end()` on inbound substreams, so a remote peer can send only a partial frame and keep the substream open. because `Behaviour::new` also sets `with_max_concurrent_streams(1000)`, the node exposes a much larger stalled-slot budget than the library default. The patch for this vulnerability is formally released as part of v1.3.0. No known workarounds are available.	5.3	More Details
CVE-2026-7109	A vulnerability was detected in code-projects Invoice System in Laravel 1.0. This impacts an unknown function of the file /item of the component API Endpoint. Performing a manipulation results in improper authorization. It is possible to initiate the attack remotely. The exploit is now public and may be used.	5.3	More Details
CVE-2026-41168	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions prior to 6.10.1 can craft a PDF which leads to long runtimes. This requires cross-reference streams with wrong large `/Size` values or object streams with wrong large `/N` values. This has been fixed in pypdf 6.10.1. As a workaround, one may apply the changes from the patch manually.	5.3	More Details
CVE-2026-7071	A security vulnerability has been detected in CodeAstro Online Job Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /users/user-cvs/. The manipulation leads to file and directory information exposure. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2026-7059	A vulnerability was found in 666ghj MiroFish up to 0.1.2. This affects the function get_simulation_posts of the file backend/app/api/simulation.py of the component Query Parameter Handler. Performing a manipulation of the argument Platform results in path traversal. The attack can be initiated remotely. The exploit has been made public and could be used.	5.3	More Details
CVE-2026-35345	A vulnerability in the tail utility of uutils coreutils allows for the exfiltration of sensitive file contents when using the --follow=name option. Unlike GNU tail, the uutils implementation continues to monitor a path after it has been replaced by a symbolic link, subsequently outputting the contents of the link's target. In environments where a privileged user (e.g., root) monitors a log directory, a local attacker with write access to that directory can replace a log file with a symlink to a sensitive system file (such as /etc/shadow), causing tail to disclose the contents of the sensitive file.	5.3	More Details
CVE-2026-	OpenClaw before 2026.3.31 lacks a shared pre-auth concurrency budget on the public LINE webhook path, allowing attackers to cause transient availability loss. Remote attackers can flood the webhook endpoint with concurrent requests	5.3	More Details

41343	before signature verification to exhaust resources and degrade service availability.		
CVE-2026-33260	An attacker can send a web request that causes unlimited memory allocation in the internal web server, leading to a denial of service. The internal web server is disabled by default.	5.3	More Details
CVE-2026-41345	OpenClaw before 2026.3.31 contains a credential exposure vulnerability in media download functionality that forwards Authorization headers across cross-origin redirects. Attackers can exploit this by crafting malicious cross-origin redirect chains to intercept sensitive authorization credentials intended for legitimate requests.	5.3	More Details
CVE-2026-42034	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, for stream request bodies, maxBodyLength is bypassed when maxRedirects is set to 0 (native http/https transport path). Oversized streamed uploads are sent fully even when the caller sets strict body limits. This vulnerability is fixed in 1.15.1 and 0.31.1.	5.3	More Details
CVE-2026-41346	OpenClaw 2026.2.26 before 2026.3.31 enforces pending pairing-request caps per channel file instead of per account, allowing attackers to exhaust the shared pending window. Remote attackers can submit pairing requests from other accounts to block new pairing challenges on unaffected accounts, causing denial of service.	5.3	More Details
CVE-2026-33258	By publishing and querying a crafted zone an attacker can cause allocation of large entries in the negative and aggressive NSEC(3) caches.	5.3	More Details
CVE-2026-41351	OpenClaw before 2026.3.31 contains a replay detection bypass vulnerability in webhook signature handling that treats Base64 and Base64URL encoded signatures as distinct requests. Attackers can re-encode Telnyx webhook signatures to bypass replay detection while maintaining valid signature verification.	5.3	More Details
CVE-2026-33257	An attacker can send a web request that causes unlimited memory allocation in the internal web server, leading to a denial of service. The internal web server is disabled by default.	5.3	More Details
CVE-2026-33256	An attacker can send a web request that causes unlimited memory allocation in the internal web server, leading to a denial of service. The internal web server is disabled by default.	5.3	More Details
CVE-2026-7217	A security vulnerability has been detected in Deepractice PromptX up to 2.4.0. The affected element is the function read_docx/read_xlsx/read_pptx/list_xlsx_sheets/read_pdf of the file packages/mcp-office/src/index.ts of the component Document File Handler. Such manipulation of the argument path leads to absolute path traversal. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-40431	A vulnerability exists in SenseLive X3050’s web management interface due to its reliance on unencrypted HTTP for all administrative communication. Because management traffic, including authentication attempts and configuration data, is transmitted in cleartext, an attacker with access to the same network segment could intercept or observe sensitive operational information.	5.3	More Details
CVE-2026-42036	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, when responseType: 'stream' is used, Axios returns the response stream without enforcing maxContentLength. This bypasses configured response-size limits and allows unbounded downstream consumption. This vulnerability is fixed in 1.15.1 and 0.31.1.	5.3	More Details
CVE-2026-6966	Improper verification of cryptographic signature uniqueness in delegated role validation in awslabs/tough before tough-v0.22.0 allows remote authenticated users to bypass the TUF signature threshold requirement by duplicating a valid signature, causing the client to accept forged delegated role metadata. We recommend you upgrade to tough-v0.22.0 / tuftool-v0.15.0.	5.3	More Details
CVE-2026-32952	go-ntlmssp is a Go package that provides NTLM/Negotiate authentication over HTTP. Prior to version 0.1.1, a malicious NTLM challenge message can causes an slice out of bounds panic, which can crash any Go process using `ntlmssp.Negotiator` as an HTTP transport. Version 0.1.1 patches the issue.	5.3	More Details
CVE-2026-2028	The MaxiBlocks Builder plugin for WordPress is vulnerable to arbitrary media file deletion due to insufficient file ownership validation on the 'maxi_remove_custom_image_size' AJAX action in all versions up to, and including, 2.1.8. This makes it possible for authenticated attackers, with Author-level access and above, to delete arbitrary files in the wp-content/uploads directory, including files uploaded by other users and administrators.	5.3	More Details
CVE-2026-42037	Axios is a promise based HTTP client for the browser and Node.js. From 1.0.0 to before 1.15.1, the FormDataPart constructor in lib/helpers/formDataToStream.js interpolates value.type directly into the Content-Type header of each multipart part without sanitizing CRLF (\r\n) sequences. An attacker who controls the .type property of a Blob/File-like object (e.g., via a user-uploaded file in a Node.js proxy service) can inject arbitrary MIME part headers into the multipart form-data body. This bypasses Node.js v18+ built-in header protections because the injection targets the multipart body structure, not HTTP request headers. This vulnerability is fixed in 1.15.1.	5.3	More Details
CVE-2026-5488	The ExactMetrics – Google Analytics Dashboard for WordPress plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 9.1.2. This is due to missing capability checks in the get_ads_access_token() and reset_experience() AJAX handlers. While the mi-admin-nonce is localized on all admin pages (including profile.php which subscribers can access), and while other similar AJAX endpoints in the same class properly check for the exactmetrics_save_settings capability, these two endpoints only verify the nonce. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve valid Google Ads access tokens and reset Google Ads integration settings.	5.3	More Details
	The HM Books Gallery plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 4.8.0. This is due to the absence of capability checks and nonce verification in the admin_init hook that handles the permalink settings		

CVE-2026-5347	update at line 205-209 of wp-books-gallery.php. The vulnerable code checks only for the presence of the 'permalink_structure' POST parameter before updating the 'wbg_cpt_slug' option, without verifying that the request comes from an authenticated administrator. This makes it possible for unauthenticated attackers to modify the custom post type slug for the books gallery, which changes the URL structure for all book entries and can break existing links and SEO rankings.	5.3	More Details
CVE-2026-41418	4ga Boards is a boards system for realtime project management. Prior to 3.3.5, 4ga Boards is vulnerable to user enumeration via a timing side-channel in the login endpoint (POST /api/access-tokens). When an invalid username/email is provided, the server responds immediately (~17ms average). When a valid username/email is provided with an incorrect password, the server first performs a bcrypt.compareSync() operation (~74ms average) before responding. This ~4.4× timing difference is trivially detectable even over a network — a single request suffices. This vulnerability is fixed in 3.3.5.	5.3	More Details
CVE-2026-6810	The Booking Calendar Contact Form plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2.63 via the dex_bccf_admin_int_calendar_list.inc.php file due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to takeover other user's calendars and view user data associated with the calendar.	5.3	More Details
CVE-2026-4117	The CalJ plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.5. This is due to a missing capability check in the CalJSettingsPage class constructor, which processes the 'save-obtained-key' operation directly from POST data without verifying that the requesting user has the 'manage_options' capability, and without any nonce verification. The plugin bootstrap file (calj.php) instantiates CalJSettingsPage whenever is_admin() returns true, which is the case for any authenticated user making requests to wp-admin URLs (including admin-ajax.php). This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's API key setting and clear the Shabbat cache, effectively taking control of the plugin's API integration.	5.3	More Details
CVE-2026-3569	The Liaison Site Prober plugin for WordPress is vulnerable to Information Exposure in all versions up to and including 1.2.1 via the /wp-json/site-prober/v1/logs REST API endpoint. The permissions_read() permission callback unconditionally returns true (via __return_true()) instead of checking for appropriate capabilities. This makes it possible for unauthenticated attackers to retrieve sensitive audit log data including IP addresses, user IDs, usernames, login/logout events, failed login attempts, and detailed activity descriptions.	5.3	More Details
CVE-2026-31052	An issue in Hostbill v.2025-11-24 and 2025-12-01 allows a remote attacker to cause a denial of service via the Checkout Authentication Flow component	5.3	More Details
CVE-2026-7235	A security vulnerability has been detected in ErlichLiu claude-agent-sdk-master up to b185aa7ff0d864581257008077b4010fca1747bf. Affected by this vulnerability is an unknown functionality of the file app/api/agent-output/route.ts. The manipulation of the argument outputFile leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-4911	The Booking Package plugin for WordPress is vulnerable to Price Manipulation in versions up to, and including, 1.7.06 This is due to the intentForStripe() function passing user-controlled $_POST['amount'] directly to the Stripe PaymentIntent API without validation, and the commitStripe() function ignoring the server-calculated amount when confirming the payment. While the server correctly calculates the booking cost via getAmount() based on services, guests, taxes, and coupons, this calculated amount is never validated against or used to update the PaymentIntent because the critical code in CreditCard.php that would include the calculated amount in the PaymentIntent update is commented out. This makes it possible for unauthenticated attackers to book services at arbitrary prices (e.g., $0.01 instead of $500.00) by manipulating the amount parameter during PaymentIntent creation and completing the booking with the fraudulent payment.	5.3	More Details
CVE-2026-6985	A weakness has been identified in Cesanta Mongoose up to 7.20. This vulnerability affects the function handle_opt of the file /src/net_builtin.c of the component TCP Option Handler. This manipulation of the argument optlen causes infinite loop. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 7.21 is able to resolve this issue. Upgrading the affected component is advised. VulDB has contacted the vendor early and they confirmed quickly, that this issue got fixed already.	5.3	More Details
CVE-2026-41337	OpenClaw before 2026.3.31 contains a callback origin mutation vulnerability in Plivo voice-call replay that allows attackers to mutate in-process callback origin before replay rejection. Attackers with captured valid callbacks for live calls can exploit this to manipulate callback origins during the replay process.	5.3	More Details
CVE-2026-4106	The HT Mega Addons for Elementor WordPress plugin before 3.0.7 contains an unauthenticated AJAX action returning some PII (such as full name, city, state and country) of customers who placed orders in the last 7 days	5.3	More Details
CVE-2025-60887	An issue was discovered in Cista v0.15 and below. Insecure deserialization of untrusted input under certain conditions may lead to leaking of stack/heap addresses which may be used to bypass ASLR. Classes with pointer-like mechanics under the cista::raw namespace are prone to reference tampering, where Cista does not perform sufficient checks to safeguard against self-referencing pointers and referencing other data within the payload. The leak occurs if the deserialized values are observable by the attacker.	5.3	More Details
CVE-2026-41915	OpenClaw before 2026.4.8 fails to remove git plumbing environment variables from the execution environment before host exec operations. Attackers can exploit this by setting GIT_DIR and related variables to redirect git operations and compromise repository integrity.	5.3	More Details
CVE-2026-40182	OpenTelemetry dotnet is a dotnet telemetry framework. From 1.13.1 to before 1.15.2, When exporting telemetry to a back-end/collector over gRPC or HTTP using OpenTelemetry Protocol format (OTLP), if the request results in a unsuccessful request (i.e. HTTP 4xx or 5xx), the response is read into memory with no upper-bound on the number of bytes consumed. This could cause memory exhaustion in the consuming application if the configured back-end/collector endpoint is attacker-	5.3	More Details

	controlled (or a network attacker can MitM the connection) and an extremely large body is returned by the response. This vulnerability is fixed in 1.15.2.		
CVE-2026-40891	OpenTelemetry dotnet is a dotnet telemetry framework. From 1.13.1 to before 1.15.2, When exporting telemetry over gRPC using the OpenTelemetry Protocol (OTLP), the exporter may parse a server-provided grpc-status-details-bin trailer during retry handling. Prior to the fix, a malformed trailer could encode an extremely large length-delimited protobuf field which was used directly for allocation, allowing excessive memory allocation and potential denial of service (DoS). This vulnerability is fixed in 1.15.2.	5.3	More Details
CVE-2026-7271	A vulnerability was detected in DV0x creative-ad-agent up to 751b9e5146604dc65049bd0f62dcbdad6212f8a3. Impacted is an unknown function of the file server/sdk-server.ts of the component creative-ad-agent-server. Performing a manipulation of the argument req.params results in path traversal. Remote exploitation of the attack is possible. The exploit is now public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The patch is named 3d255865a957f3740b8724dd914502c0f44d4970. Applying a patch is the recommended action to fix this issue.	5.3	More Details
CVE-2026-40894	OpenTelemetry dotnet is a dotnet telemetry framework. In OpenTelemetry.Api 0.5.0-beta.2 to 1.15.2 and OpenTelemetry.Extensions.Propagators 1.3.1 to 1.15.2, The implementation details of the baggage, B3 and Jaeger processing code in the OpenTelemetry.Api and OpenTelemetry.Extensions.Propagators NuGet packages can allocate excessive memory when parsing which could create a potential denial of service (DoS) in the consuming application. This vulnerability is fixed in 1.15.3.	5.3	More Details
CVE-2026-32655	Dell Alienware Command Center (AWCC), versions prior to 6.13.8.0, contain a Least Privilege Violation vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	5.3	More Details
CVE-2026-41400	OpenClaw before 2026.3.31 contains an incomplete fix for CVE-2026-32062 where the voice-call component parses large WebSocket frames before start validation. Remote attackers can send oversized pre-start WebSocket frames to cause resource consumption and denial of service.	5.3	More Details
CVE-2026-41136	free5GC AMF provides Access & Mobility Management Function (AMF) for free5GC, an an open-source project for 5th generation (5G) mobile core networks. Prior to version 1.4.3, the `HTTPUEContextTransfer` handler in `internal/sbi/api_communication.go` does not include a `default` case in the `Content-Type` switch statement. When a request arrives with an unsupported `Content-Type`, the deserialization step is silently skipped, `err` remains `nil`, and the processor is invoked with a completely uninitialized `UeContextTransferRequest` object. Version 1.4.3 contains a fix.	5.3	More Details
CVE-2026-41606	Uncontrolled Recursion vulnerability in Apache Thrift. This issue affects Apache Thrift: before 0.23.0. Users are recommended to upgrade to version 0.23.0, which fixes the issue.	5.3	More Details
CVE-2026-7179	A security vulnerability has been detected in OSPG binwalk up to 2.4.3. This vulnerability affects the function read_null_terminated_string of the file src/binwalk/plugins/winceextract.py of the component WinCE Extraction Plugin. Such manipulation of the argument self.file_name leads to path traversal. The attack can only be performed from a local environment. The exploit has been disclosed publicly and may be used. The project maintainer confirms this issue: "I accept the existence of the Path Traversal vulnerability. However, as stated in the Github link, it reached EOL and as a result no actions should be expected." The GitHub repository mentions, that "[u]sers and contributors should migrate to binwalk v3." This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-7183	A vulnerability has been found in aligungr UERANSIM up to 3.2.7. The affected element is the function rls::DecodeRlsMessage in the library src/lib/rls/rls_pdu.cpp of the component Radio Link Simulation Layer. The manipulation of the argument pduLength leads to uncaught exception. The attack may be initiated remotely. Upgrading to version 3.2.8 is sufficient to fix this issue. The identifier of the patch is ca1a66fffe282767bb08618af9f848e3b68ea47b. It is suggested to upgrade the affected component. This behavior is related to CVE-2024-37877. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	5.3	More Details
CVE-2026-22748	Vulnerability in Spring Spring Security. When an application configures JWT decoding with NimbusJwtDecoder or NimbusReactiveJwtDecoder, it must configure an OAuth2TokenValidator<Jwt> separately, for example by calling setJwtValidator.This issue affects Spring Security: from 6.3.0 through 6.3.14, from 6.4.0 through 6.4.14, from 6.5.0 through 6.5.9, from 7.0.0 through 7.0.4.	5.3	More Details
CVE-2026-40448	Potential Integer overflow in tensor allocation size calculation could lead to insufficient memory allocation for large tensors in Samsung Open Source ONE. Affected version is prior to commit 1.30.0.	5.3	More Details
CVE-2026-41363	OpenClaw versions 2026.2.6 through 2026.3.24 contain a path traversal vulnerability in the Feishu extension resolveUploadInput function that bypasses file-system sandbox restrictions. Attackers can exploit improper path resolution during upload_image operations to read arbitrary files outside configured localRoots boundaries.	5.3	More Details
CVE-2026-41332	OpenClaw before 2026.3.28 contains an environment variable sanitization vulnerability where GIT_TEMPLATE_DIR and AWS_CONFIG_FILE are not blocked in the host-env blocklist. Attackers can exploit approved exec requests to redirect git or AWS CLI behavior through attacker-controlled configuration files to execute untrusted code or load malicious credentials.	5.3	More Details
CVE-2026-6993	A security flaw has been discovered in go-kratos kratos up to 2.9.2. This impacts the function NewServer of the file transport/http/server.go of the component http.DefaultServeMux Fallback Handler. The manipulation results in unintended intermediary. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The patch is identified as 0284a5bcf92b5a7ee015300ce3051baf7ae4718d. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-	@astrojs/node allows Astro to deploy your SSR site to Node targets. Prior to 10.0.5, requesting a static js/css resources from _astro path with an incorrect/malformed if-match header returns a 500 error with a one year cache lifetime instead of 412		More

2026-41322	in some cases. This has the effect that all subsequent requests to that file, regardless of if-match header will be served a 5xx error instead of the file until the cache expires. This vulnerability is fixed in 10.0.5.	5.3	Details
CVE-2026-41335	OpenClaw before 2026.3.31 contains an information disclosure vulnerability in the Control Interface bootstrap JSON that exposes version and assistant agent identifiers. Attackers can extract sensitive fingerprinting information from the Control UI bootstrap payload to identify system versions and agent configurations.	5.3	More Details
CVE-2026-41469	Beghelli Sicuro24 SicuroWeb does not enforce a Content Security Policy, allowing unrestricted loading of external JavaScript resources from attacker-controlled origins. When chained with the template injection and sandbox escape vulnerabilities present in the same application, the absence of CSP removes the browser-enforced restriction that would otherwise block external script execution, enabling attackers to load arbitrary remote payloads into operator browser sessions.	5.2	More Details
CVE-2026-42371	uriparser before 1.0.1 has numeric truncation in text range comparison, if an application accepts URIs with a length in gigabytes.	5.1	More Details
CVE-2025-10549	EfficientLab Controlio before v1.3.95 contains a DLL hijacking vulnerability caused by weak folder permissions in the installation directory. A local attacker can place a specially crafted DLL in this directory and achieve arbitrary code execution with highest privileges, because the affected service runs as NT AUTHORITY\SYSTEM.	5.1	More Details
CVE-2026-41131	OpenFGA is an authorization/permission engine built for developers. Prior to version 1.14.1, in specific scenarios, models using conditions with caching enabled can result in two different check requests producing the same cache key. This could result in OpenFGA reusing an earlier cached result for a subsequent request. The preconditions for vulnerability are the model having relations which rely on condition evaluation and the user having caching enabled. OpenFGA v1.14.1 contains a fix.	5.0	More Details
CVE-2026-41232	Froxlor is open source server administration software. Prior to version 2.3.6, in `EmailSender::add()`, the domain ownership validation for full email sender aliases uses the wrong array index when splitting the email address, passing the local part instead of the domain to `validateLocalDomainOwnership()`. This causes the ownership check to always pass for non-existent "domains," allowing any authenticated customer to add sender aliases for email addresses on domains belonging to other customers. Postfix's `sender_login_maps` then authorizes the attacker to send emails as those addresses. Version 2.3.6 fixes the issue.	5.0	More Details
CVE-2026-41338	OpenClaw before 2026.3.31 contains a time-of-check-time-of-use vulnerability in sandbox file operations that allows attackers to bypass fd-based defenses. Attackers can exploit check-then-act patterns in apply_patch, remove, and mkdir operations to manipulate files between validation and execution.	5.0	More Details
CVE-2026-41367	OpenClaw versions 2026.2.14 through 2026.3.24 fail to consistently apply guild and channel policy gates to Discord button and component interactions. Attackers can trigger privileged component actions from blocked contexts by bypassing channel policy enforcement.	5.0	More Details
CVE-2026-40971	When configured to use an SSL bundle, Spring Boot's RabbitMQ auto-configuration does not perform hostname verification when connecting to the RabbitMQ broker. Affected: Spring Boot 4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14) per vendor advisory.	5.0	More Details
CVE-2026-40970	When configured to use an SSL bundle, Spring Boot's Elasticsearch auto-configuration does not perform hostname verification when connecting to the Elasticsearch server. Affected: Spring Boot 4.0.0–4.0.5; upgrade to 4.0.6 or later per vendor advisory.	5.0	More Details
CVE-2026-35372	A logic error in the ln utility of uutils coreutils allows the utility to dereference a symbolic link target even when the --no-dereference (or -n) flag is explicitly provided. The implementation previously only honored the "no-dereference" intent if the --force (overwrite) mode was also enabled. This flaw causes ln to follow a symbolic link that points to a directory and create new links inside that target directory instead of treating the symbolic link itself as the destination. In environments where a privileged user or system script uses ln -n to update a symlink, a local attacker could manipulate existing symbolic links to redirect file creation into sensitive directories, potentially leading to unauthorized file creation or system misconfiguration.	5.0	More Details
CVE-2026-6845	A flaw was found in binutils, specifically within the `readelf` utility. This vulnerability allows a local attacker to cause a Denial of Service (DoS) by tricking a user into processing a specially crafted Executable and Linkable Format (ELF) file. The exploitation of this flaw can lead to the system becoming unresponsive due to excessive resource consumption or a program crash.	5.0	More Details
CVE-2026-33259	Having many concurrent transfers of the same RPZ can lead to inconsistent RPZ data, use after free and/or a crash of the recursor. Normally concurrent transfers of the same RPZ zone can only occur with a malfunctioning RPZ provider.	5.0	More Details
CVE-2026-7085	A vulnerability was determined in HBAI-Ltd Toonflow-app up to 1.1.1. This vulnerability affects the function z.url of the file src/routes/setting/about/downloadApp.ts of the component downloadApp Endpoint. This manipulation of the argument url causes path traversal. It is possible to initiate the attack remotely. The attack is considered to have high complexity. It is stated that the exploitability is difficult. The exploit has been publicly disclosed and may be utilized. The real existence of this vulnerability is still doubted at the moment. The vendor explains in a reply to the issue report, that "[t]his interface is used for online updates, and the update URL has been statically compiled in the official code repository. Unless users modify the code, the requested address will be the official source address."	5.0	More Details
CVE-2026-7317	A vulnerability was found in Grav CMS up to 1.7.49.5/2.0.0-beta.1. Affected by this vulnerability is the function FileCache::doGet of the file system/src/Grav/Framework/Cache/Adapter/FileCache.php of the component Cache Value Handler. The manipulation results in deserialization. The attack may be launched remotely. The attack requires a high level of complexity. The exploitation appears to be difficult. The exploit has been made public and could be used. Upgrading to version 2.0.0-beta.2 addresses this issue. The patch is identified as c66dfeb5f. The affected component should be upgraded.	5.0	More Details

CVE-2026-40974	Spring Boot's Cassandra auto-configuration does not perform hostname verification when establishing an SSL connection to Cassandra. Affected: Spring Boot 4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14), 3.4.0–3.4.15 (fix 3.4.16), 3.3.0–3.3.18 (fix 3.3.19), 2.7.0–2.7.32 (fix 2.7.33); Cassandra SSL auto-configuration. Versions that are no longer supported are also affected per vendor advisory.	5.0	More Details
CVE-2026-4917	IBM Guardium Data Protection 12.1 could allow an administrative user to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to write arbitrary files on the system.	4.9	More Details
CVE-2026-1274	IBM Guardium Data Protection 12.0, 12.1, and 12.2 is vulnerable to a Bypass Business Logic vulnerability in the access management control panel.	4.9	More Details
CVE-2026-31050	Cross Site Scripting vulnerability in Hostbill v.2025-11-24 and 2025-12-01 allows a remote attacker to execute arbitrary code	4.9	More Details
CVE-2026-31955	Xibo is an open source digital signage platform with a web content management system and Windows display player software. An authenticated Server-Side Request Forgery (SSRF) vulnerability in versions prior to 4.4.1 allows users with DataSet permissions to make arbitrary HTTP requests from the CMS server to internal or external network resources. This can be exploited to scan internal infrastructure, access local cloud metadata endpoints (e.g., AWS IMDS), interact with internal services that lack authentication, or exfiltrate data. Exploitation of the vulnerability is possible on behalf of an authorized user who has both of the following privileges, which are not granted to non-admins as standard: Include "Add DataSet" button to allow for additional DataSets to be created independently to Layouts. Users should upgrade to version 4.4.1 which fixes this issue. Upgrading to a fixed version is necessary to remediate. Users unable to upgrade should revoke such privileges from users they do not trust.	4.9	More Details
CVE-2026-1789	A vulnerability in the browser-based remote management interface may allow an administrator to access sensitive information on the device via crafted requests, affecting certain production printers and office/small office multifunction printers.	4.9	More Details
CVE-2026-40975	Values produced by ${random.value} are not suitable for use as secrets. ${random.uuid} is not affected. ${random.int} and ${random.long} should never be used for secrets as they are numeric values with a predictable range. Affected: Spring Boot 4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14), 3.4.0–3.4.15 (fix 3.4.16), 3.3.0–3.3.18 (fix 3.3.19), 2.7.0–2.7.32 (fix 2.7.33); random value property source / weak PRNG for secrets. Versions that are no longer supported are also affected per vendor advisory.	4.8	More Details
CVE-2026-33598	A cached crafted response can cause an out-of-bounds read if custom Lua code calls getDomainListByAddress() or getAddressListByDomain() on a packet cache.	4.8	More Details
CVE-2025-10539	Due to improper TLS certificate validation in the DeskTime Time Tracking App before version 1.3.674, attackers who can position themselves in the network path between the client and the DeskTime update servers can return a malicious executable in response to an update request. This allows the attacker to achieve user-level remote code execution on the affected client.	4.8	More Details
CVE-2026-41393	OpenClaw before 2026.3.31 contains a wide-area discovery vulnerability allowing arbitrary tailnet peers to be accepted as DNS authorities. Attackers with same-tailnet position and CA-trusted endpoint access can exfiltrate operator credentials through DNS steering manipulation.	4.8	More Details
CVE-2026-1726	IBM Guardium Key Lifecycle Manager 4.1, 4.1.1, 4.2, 4.2.1, 5.0, and 5.1	4.8	More Details
CVE-2026-42041	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, the Axios library is vulnerable to a Prototype Pollution "Gadget" attack that allows any Object.prototype pollution to silently suppress all HTTP error responses (401, 403, 500, etc.), causing them to be treated as successful responses. This completely bypasses application-level authentication and error handling. The root cause is that validateStatus is the only config property using the mergeDirectKeys merge strategy, which uses JavaScript's in operator — an operator that inherently traverses the prototype chain. When Object.prototype.validateStatus is polluted with () => true, all HTTP status codes are accepted as success. This vulnerability is fixed in 1.15.1 and 0.31.1.	4.8	More Details
CVE-2026-4919	IBM Guardium Data Protection 12.1 is vulnerable to cross-site scripting. This vulnerability allows an administrative user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2026-7028	A security flaw has been discovered in CodeAstro Online Job Portal 1.0. The affected element is an unknown function of the file /admin/jobs-admins/delete-jobs.php of the component All Jobs Page. Performing a manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-31523	In the Linux kernel, the following vulnerability has been resolved: nvme-pci: ensure we're polling a polled queue A user can change the polled queue count at run time. There's a brief window during a reset where a hipri task may try to poll that queue before the block layer has updated the queue maps, which would race with the now interrupt driven queue and may cause double completions.	4.7	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: smb: client: make use of smbdirect_socket.recv_io.credits.available The logic off managing recv credits by counting posted recv_io and granted credits is racy. That's because the peer might already consumed a credit, but between receiving the incoming recv at the		More

2026-31535	hardware and processing the completion in the 'recv_done' functions we likely have a window where we grant credits, which don't really exist. So we better have a decicated counter for the available credits, which will be incremented when we posted new recv buffers and drained when we grant the credits to the peer.	4.7	Details
CVE-2026-7238	A flaw has been found in code-projects Online Music Site 1.0. This affects an unknown part of the file /Administrator/PHP/AdminUpdateAlbum.php. This manipulation of the argument txtimage causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used.	4.7	More Details
CVE-2026-7083	A vulnerability has been found in likeadmin-likeshop likeadmin_php up to 1.9.6. Affected by this issue is the function queryResult of the file server\app\adminapi\lists\tools\DataTableLists.php of the component dataTable Admin API. The manipulation leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-7133	A vulnerability was determined in code-projects Online Lot Reservation System 1.0. This impacts an unknown function of the file /activity.php. This manipulation of the argument directory causes unrestricted upload. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-7293	A vulnerability was detected in SourceCodester Pizzafy Ecommerce System 1.0. Affected is the function delete_category of the file /admin/ajax.php?action=delete_category. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	4.7	More Details
CVE-2025-59308	In Mahara before 24.04.10 and 25 before 25.04.1, an institution administrator or institution support administrator on a multi-tenanted site can masquerade as an institution member in an institution for which they are not an administrator, if they also have the 'Site staff' role.	4.7	More Details
CVE-2026-35359	A Time-of-Check to Time-of-Use (TOCTOU) vulnerability in the cp utility of uutils coreutils allows an attacker to bypass no-dereference intent. The utility checks if a source path is a symbolic link using path-based metadata but subsequently opens it without the O_NOFOLLOW flag. An attacker with concurrent write access can swap a regular file for a symbolic link during this window, causing a privileged cp process to copy the contents of arbitrary sensitive files into a destination controlled by the attacker.	4.7	More Details
CVE-2026-6978	A vulnerability was detected in JiZhiCMS up to 2.5.6. The impacted element is the function htmlspecialchars_decode of the file /index.php/admins/Sys/addcache.html. The manipulation of the argument sqls results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-7282	A vulnerability was identified in SourceCodester Pharmacy Sales and Inventory System 1.0. This affects the function delete_expired of the file /ajax.php?action=delete_expired. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-31572	In the Linux kernel, the following vulnerability has been resolved: i2c: designware: amdisp: Fix resume-probe race condition issue Identified resume-probe race condition in kernel v7.0 with the commit 38fa29b01a6a ("i2c: designware: Combine the init functions"),but this issue existed from the beginning though not detected. The amdisp i2c device requires ISP to be in power-on state for probe to succeed. To meet this requirement, this device is added to genpd to control ISP power using runtime PM. The pm_runtime_get_sync() called before i2c_dw_probe() triggers PM resume, which powers on ISP and also invokes the amdisp i2c runtime resume before the probe completes resulting in this race condition and a NULL dereferencing issue in v7.0 Fix this race condition by using the genpd APIs directly during probe: - Call dev_pm_genpd_resume() to Power ON ISP before probe - Call dev_pm_genpd_suspend() to Power OFF ISP after probe - Set the device to suspended state with pm_runtime_set_suspended() - Enable runtime PM only after the device is fully initialized	4.7	More Details
CVE-2026-35357	The cp utility in uutils coreutils is vulnerable to an information disclosure race condition. Destination files are initially created with umask-derived permissions (e.g., 0644) before being restricted to their final mode (e.g., 0600) later in the process. A local attacker can race to open the file during this window; once obtained, the file descriptor remains valid and readable even after the permissions are tightened, exposing sensitive or private file contents.	4.7	More Details
CVE-2026-40977	When an application is configured to use `ApplicationPidFileWriter`, a local attacker with write access to the PID file's location can corrupt one file on the host each time the application is started. Affected: Spring Boot 4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14), 3.4.0–3.4.15 (fix 3.4.16), 3.3.0–3.3.18 (fix 3.3.19), 2.7.0–2.7.32 (fix 2.7.33); PID file / symlink behavior (`ApplicationPidFileWriter`). Versions that are no longer supported are also affected per vendor advisory.	4.7	More Details
CVE-2025-66286	An API design flaw in WebKitGTK and WPE WebKit allows untrusted web content to unexpectedly perform IP connections, DNS lookups, and HTTP requests. Applications expect to use the WebPage::send-request signal handler to approve or reject all network requests. However, certain types of HTTP requests bypass this signal handler.	4.7	More Details
CVE-2026-41244	Mojic is a CLI tool to transform readable C code into an unrecognizable chaotic stream of emojis. Prior to 2.1.4, the CipherEngine uses a standard equality operator (!==) to verify the HMAC-SHA256 integrity seal during the decryption phase. This creates an Observable Timing Discrepancy (CWE-208), allowing a potential attacker to bypass the file integrity check via a timing attack. This vulnerability is fixed in 2.1.4.	4.7	More Details
CVE-2026-35354	A Time-of-Check to Time-of-Use (TOCTOU) vulnerability exists in the mv utility of uutils coreutils during cross-device moves. The extended attribute (xattr) preservation logic uses multiple path-based system calls that perform fresh path-to-inode lookups for each operation. A local attacker with write access to the directory can exploit this race to swap files between calls, causing the destination file to receive an inconsistent mix of security xattrs, such as SELinux labels or file capabilities.	4.7	More Details
CVE-2026-7134	A vulnerability was identified in code-projects Online Lot Reservation System 1.0. Affected is an unknown function of the file /edithousepic.php. Such manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit is publicly available and might be used.	4.7	More Details

CVE-2026-7283	A security flaw has been discovered in SourceCodester Pharmacy Sales and Inventory System 1.0. This impacts the function save_expired of the file /ajax.php?action=save_expired. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-6984	A security flaw has been discovered in AstrBotDevs AstrBot up to 4.22.1. This affects the function create_template of the file astrbot/dashboard/routes/t2i.py of the component Dashboard API. The manipulation results in improper neutralization of special elements used in a template engine. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-6983	A vulnerability was identified in pagekit up to 1.0.18. Affected by this issue is some unknown functionality of the file /index.php/admin/system/update/download. The manipulation of the argument url leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-41398	OpenClaw before 2026.4.2 contains an improper access control vulnerability in the iOS A2UI bridge that treats generic local-network pages as trusted origins. Attackers can inject unauthorized agent.request runs by loading attacker-controlled pages from local-network or tailnet hosts, polluting session state and consuming budget.	4.6	More Details
CVE-2026-31620	In the Linux kernel, the following vulnerability has been resolved: ALSA: usx2y: us144mkii: fix NULL deref on missing interface 0 A malicious USB device with the TASCAM US-144MKII device id can have a configuration containing bInterfaceNumber=1 but no interface 0. USB configuration descriptors are not required to assign interface numbers sequentially, so usb_ifnum_to_if(dev, 0) returns will NULL, which will then be dereferenced directly. Fix this up by checking the return value properly.	4.6	More Details
CVE-2026-41377	OpenClaw before 2026.3.31 contains a fail-open vulnerability in the plugin installation flow where security scan failures do not block installation. Attackers can exploit scan failures to install untrusted plugins when operators proceed despite visible scan warnings.	4.6	More Details
CVE-2026-35376	A Time-of-Check to Time-of-Use (TOCTOU) vulnerability exists in the chcon utility of uutils coreutils during recursive operations. The implementation resolves recursive targets using a fresh path lookup (via fts_accpath) rather than binding the traversal and label application to the specific directory state encountered during traversal. Because these operations are not anchored to file descriptors, a local attacker with write access to a directory tree can exploit timing-sensitive rename or symbolic link races to redirect a privileged recursive relabeling operation to unintended files or directories. This vulnerability breaks the hardening expectations for SELinux administration workflows and can lead to the unauthorized modification of security labels on sensitive system objects.	4.5	More Details
CVE-2026-7026	A vulnerability was determined in D-Link DGS-3420 1.50.018. This issue affects some unknown processing of the component System Information Settings Page. This manipulation of the argument System Name causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	4.5	More Details
CVE-2026-2719	The Private WP suite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Exceptions' setting in all versions up to, and including, 0.4.1. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-3362	The Short Comment Filter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Minimum Count' settings field in all versions up to and including 2.2. This is due to insufficient input sanitization (no sanitize callback on register_setting) and missing output escaping (no esc_attr() on the echoed value in the input's value attribute). The option value is stored via update_option() and rendered unescaped in an HTML attribute context. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in the settings page that will execute whenever a user accesses that page. This is particularly impactful in WordPress multisite installations or when DISALLOW_UNFILTERED_HTML is set, where administrators are not granted the unfiltered_html capability.	4.4	More Details
CVE-2026-35901	A handling issue in the RTSP service of the Mercury MIPC252W 1.0.5 Build 230306 Rel.79931n allows an authenticated attacker to trigger session termination by repeatedly sending SETUP requests for the same media track within a single RTSP session. This causes the server to reset the RTSP connection, leading to a denial-of-service condition.	4.4	More Details
CVE-2026-2714	The Institute Management plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Enquiry Form Title' setting in all versions up to, and including, 5.5. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1379	The HTTP Headers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.19.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-33600	An RPZ sent by a malicious authoritative server can result in a null pointer dereference, caused by a missing consistency check and leading to a denial of service.	4.4	More Details
CVE-2026-	The Sentence To SEO (keywords, description and tags) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Permanent keywords' field in all versions up to and including 1.0. This is due to insufficient input sanitization and output escaping. The plugin reads user input via filter_input_array(INPUT_POST) which applies no HTML sanitization (FILTER_DEFAULT), stores it unsanitized to the WordPress options table via update_option(), and then outputs the stored	4.4	More

4142	value directly into a textarea element without any escaping using PHP short echo tags (<?= ?>). An attacker can break out of the textarea element using a closing </textarea> tag and inject arbitrary HTML/JavaScript. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the plugin's settings page.		Details
CVE-2026-35366	The printenv utility in uutils coreutils fails to display environment variables containing invalid UTF-8 byte sequences. While POSIX permits arbitrary bytes in environment strings, the uutils implementation silently skips these entries rather than printing the raw bytes. This vulnerability allows malicious environment variables (e.g., adversarial LD_PRELOAD values) to evade inspection by administrators or security auditing tools, potentially allowing library injection or other environment-based attacks to go undetected.	4.4	More Details
CVE-2026-35358	The cp utility in uutils coreutils, when performing recursive copies (-R), incorrectly treats character and block device nodes as stream sources rather than preserving them. Because the implementation reads bytes into regular files at the destination instead of using mknod, device semantics are destroyed (e.g., /dev/null becomes a regular file). This behavior can lead to runtime denial of service through disk exhaustion or process hangs when reading from unbounded device nodes.	4.4	More Details
CVE-2026-6041	The Buzz Comments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Custom Buzz Avatar' (buzz_comments_avatar_image) setting in all versions up to, and including, 0.9.4. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the plugin settings page.	4.4	More Details
CVE-2026-35370	The id utility in uutils coreutils miscalculates the groups= section of its output. The implementation uses a user's real GID instead of their effective GID to compute the group list, leading to potentially divergent output compared to GNU coreutils. Because many scripts and automated processes rely on the output of id to make security-critical access-control or permission decisions, this discrepancy can lead to unauthorized access or security misconfigurations.	4.4	More Details
CVE-2026-35347	The comm utility in uutils coreutils incorrectly consumes data from non-regular file inputs before performing comparison operations. The are_files_identical function opens and reads from both input paths to compare content without first verifying if the paths refer to regular files. If an input path is a FIFO or a pipe, this pre-read operation drains the stream, leading to silent data loss before the actual comparison logic is executed. Additionally, the utility may hang indefinitely if it attempts to pre-read from infinite streams like /dev/zero.	4.4	More Details
CVE-2026-29051	melange allows users to build apk packages using declarative pipelines. Starting in version 0.32.0 and prior to version 0.43.4, `melange lint --persist-lint-results` (opt-in flag, also usable via `melange build --persist-lint-results`) constructs output file paths by joining `--out-dir` with the `arch` and `pkgname` values read from the `.PKGINFO` control file of the APK being linted. In affected versions these values were not validated for path separators or `..` sequences, so an attacker who can supply an APK to a melange-based lint/build pipeline (e.g. CI that lints third-party APKs, or build-as-a-service) could cause melange to write `lint-<pkgname>-<pkgver>-r<epoch>.json` to an arbitrary `.json` path reachable by the melange process. The written file is a JSON lint report whose content is partially attacker-influenced. There is no direct code-execution path, but the write can clobber other JSON artifacts on the filesystem. The issue only affects deployments that explicitly pass `--persist-lint-results`; the flag is off by default. The issue is fixed in melange v0.43.4 by validating `arch` and `pkgname` for `..`, `/`, and `filepath.Separator` before path construction in `pkg/linter/results.go` (commit 84f3b45). As a workaround, do not pass `--persist-lint-results` when linting or building APKs whose `.PKGINFO` contents are not fully trusted. Running melange as a low-privileged user and confining writes to an isolated directory also limits impact.	4.4	More Details
CVE-2026-33601	If you use the zoneToCache function with a malicious authoritative server, an attacker can send a zone that result in a null pointer dereference, caused by a missing consistency check and leading to a denial of service.	4.4	More Details
CVE-2026-6393	The BetterDocs plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 4.3.11. This is due to a missing capability check in the generate_openai_content_callback() function, which relies solely on a nonce rather than verifying user permissions. This makes it possible for authenticated attackers, with subscriber-level access and above, to trigger OpenAI API calls using the site's configured API key with arbitrary user-controlled prompts, leading to unauthorized consumption of the site owner's paid AI API quota.	4.3	More Details
CVE-2026-4118	The Call To Action Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.3. This is due to missing nonce validation in the cbox_options_page() function which handles saving, creating, and deleting plugin settings. The form rendered on the settings page does not include a wp_nonce_field(), and the save handler does not call wp_verify_nonce() or check_admin_referer() before processing settings updates via $wpdb->update(). This makes it possible for unauthenticated attackers to modify plugin settings such as call-to-action box title, content, link URL, image URL, colors, and other configuration options via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-41908	OpenClaw before 2026.4.20 contains a scope enforcement bypass vulnerability in the assistant-media route that allows trusted-proxy callers without operator.read scope to access protected assistant-media files and metadata. Attackers can bypass identity-bearing HTTP auth path scope validation to retrieve sensitive media content within allowed media roots.	4.3	More Details
CVE-2025-11762	The HubSpot All-In-One Marketing - Forms, Popups, Live Chat plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 11.3.32 via the leadin/public/admin/class-adminconstants.php file. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract a list of all installed plugins and their versions which can be leveraged for reconnaissance and further attacks.	4.3	More Details
CVE-2026-4121	The Kcaptcha plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 1.0.1. This is due to missing nonce validation in the plugin's settings page handler (admin/setting.php). The settings form does not include a wp_nonce_field() and the form processing code does not call wp_verify_nonce() or check_admin_referer() before saving settings to the database via $wpdb->update(). This makes it possible for unauthenticated attackers to modify the plugin's CAPTCHA settings (enabling or disabling CAPTCHA on login, registration, lost password, and comment forms) via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	4.3	More Details

CVE-2026-7144	A security flaw has been discovered in 1000 Projects Portfolio Management System MCA 1.0. This impacts an unknown function of the file update_passwd_process.php. The manipulation of the argument temp_user results in authorization bypass. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	4.3	More Details
CVE-2026-41339	OpenClaw before 2026.4.2 exposes configPath and stateDir metadata in Gateway connect success snapshots to non-admin authenticated clients. Non-admin clients can recover host-specific filesystem paths and deployment details, enabling host fingerprinting and facilitating chained attacks.	4.3	More Details
CVE-2026-7230	A vulnerability was found in SourceCodester Safety Anger Pad 1.0. The affected element is an unknown function. The manipulation of the argument angerDisplay results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used.	4.3	More Details
CVE-2026-7200	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this issue is some unknown functionality of the file /index.php?page=types. Executing a manipulation of the argument ID can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2026-41910	OpenClaw before 2026.4.8 omits owner-only enforcement for cross-channel allowlist writes in the /allowlist endpoint. An authorized non-owner sender can bypass access controls to perform allowlist modifications against different channels, violating the intended trust model.	4.3	More Details
CVE-2026-41350	OpenClaw before 2026.3.31 contains a session visibility bypass vulnerability where the session_status function fails to enforce configured tools.sessions.visibility restrictions for unsandboxed invocations. Attackers can invoke session_status without sandbox constraints to bypass session-policy controls and access restricted session information.	4.3	More Details
CVE-2026-41362	OpenClaw versions 2026.2.19 before 2026.3.31 contain an improper cache isolation vulnerability in the Zalo webhook replay-dedupe mechanism that is shared across authenticated webhook targets. Attackers controlling one authenticated Zalo webhook path in multi-account deployments can suppress legitimate events on different accounts by matching event_name and message_id parameters.	4.3	More Details
CVE-2026-4126	The Table Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.0 via the 'table_manager' shortcode. The shortcode handler `tablemanager_render_table_shortcode()` takes a user-controlled `table` attribute, applies only `sanitize_key()` for sanitization, and concatenates the value with `$wpdb->prefix` to form a full database table name. It then executes `DESC` and `SELECT *` queries against this table and renders all rows and columns to the frontend. There is no allowlist check to ensure only plugin-created tables can be accessed — the `tablemanager_created_tables` option is only referenced in admin functions, never in the shortcode handler. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data from arbitrary WordPress database tables.	4.3	More Details
CVE-2026-1930	The Emailchef plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the page_options_ajax_disconnect() function in all versions up to, and including, 3.5.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the plugin's settings via the 'emailchef_disconnect' AJAX action.	4.3	More Details
CVE-2026-4128	The TP Restore Categories And Taxonomies plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0.1. The delete_term() function, which handles the 'tpmcattt_delete_term' AJAX action, does not perform any capability check (e.g., current_user_can()) to verify the user has sufficient permissions. While it does verify a nonce via check_ajax_referer(), this nonce is generated for all authenticated users via the admin_enqueue_scripts hook and exposed on any wp-admin page (including profile.php, which subscribers can access). This makes it possible for authenticated attackers, with Subscriber-level access and above, to permanently delete taxonomy term records from the plugin's trash/backup tables by sending a crafted AJAX request with a valid nonce and an arbitrary term_id.	4.3	More Details
CVE-2026-29197	In versions <8.4.0, <8.3.2, <8.2.2, <8.1.3, <8.0.4, <7.13.6, <7.12.7, <7.11.7, and <7.10.10, the endpoints /api/apps/logs and /api/apps/:id/logs have a typo in the required permission check, allowing authenticated users without the proper permissions to read apps-engine logs.	4.3	More Details
CVE-2026-4133	The TextP2P Texting Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 1.7. This is due to missing nonce validation in the imTextP2POptionPage() function which processes settings updates. The form at line 314 does not include a wp_nonce_field(), and the POST handler at line 7 does not call check_admin_referer() or wp_verify_nonce() before processing settings changes. This makes it possible for unauthenticated attackers to update all plugin settings including chat widget titles, messages, API credentials, colors, and reCAPTCHA configuration via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	4.3	More Details
CVE-2026-31956	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to version 4.4.1, any authenticated user can manually construct a URL to preview campaigns/regions, and export saved reports belonging to other users. Exploitation of the vulnerability is possible on behalf of an authorized user who has any of the following privileges: Page which shows all Layouts that have been created for the purposes of Layout Management; page which shows all Campaigns that have been created for the purposes of Campaign Management; and page which shows all Reports that have been Saved. Users should upgrade to version 4.4.1 which fixes this issue. Upgrading to a fixed version is necessary to remediate.	4.3	More Details
CVE-2026-4138	The DX Unanswered Comments plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.7. This is due to missing nonce validation on the plugin's settings form in the dxuc-unanswered-comments-admin-page.php file. This makes it possible for unauthenticated attackers to modify plugin settings (dxuc_authors_list and dxuc_comment_count) via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
	The mCatFilter plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 0.5.2. This is due to the complete absence of nonce verification and capability checks in the compute_post() function, which		

CVE-2026-4139	processes settings updates. The compute_post() function is called in the plugin constructor on every page load via the plugins_loaded hook, and it directly processes $_POST data to modify plugin settings via update_option() without any CSRF token validation. This makes it possible for unauthenticated attackers to modify all plugin settings, including category exclusion rules, feed exclusion flags, and tag page exclusion flags, via a forged POST request, granted they can trick a site administrator into performing an action such as clicking a link.	4.3	More Details
CVE-2026-6396	The Fast & Fancy Filter – 3F plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.2.2. This is due to missing nonce verification in the saveFields() function, which handles the fff_save_settins AJAX action. This makes it possible for unauthenticated attackers to modify plugin filter settings, update arbitrary options, or create new filter posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-6294	The Google PageRank Display plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.4. This is due to missing nonce validation in the gpdisplay_option() function, which handles the plugin settings page. The settings form does not include a wp_nonce_field(), and the form handler does not call check_admin_referer() or wp_verify_nonce() before processing the POST request. This makes it possible for unauthenticated attackers to trick a logged-in administrator into submitting a crafted request that changes the plugin's settings (stored via update_option()), such as the display style used to render the PageRank badge.	4.3	More Details
CVE-2026-4140	The Ni WooCommerce Order Export plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 3.1.6. This is due to missing nonce validation in the ni_order_export_action() AJAX handler function. The handler processes settings updates when the 'page' parameter is set to 'nioe-order-settings', delegating to Ni_Order_Setting::page_ajax() which calls update_option('ni_order_export_option', $_REQUEST) without verifying any nonce or checking user capabilities. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	4.3	More Details
CVE-2026-41408	OpenClaw before 2026.3.31 contains a resource exhaustion vulnerability in media downloads that bypasses core safety limits for file size, count, and cleanup operations. Attackers can exhaust disk space by downloading media files without triggering intended safety restrictions, causing availability impact.	4.3	More Details
CVE-2026-30462	A path traversal vulnerability in the Blocks module of Daylight Studio FuelCMS v1.5.2 allows attackers to execute a directory traversal.	4.3	More Details
CVE-2026-7095	A vulnerability was identified in code-projects Employee Management System 1.0. This affects an unknown part of the file 370project/edit.php. The manipulation of the argument ID leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-40690	The asset dependency graph did not restrict nodes by the viewer's DAG read permissions: a user with read access to at least one DAG could browse the asset graph for any other asset in the deployment and learn the existence and names of DAGs and assets outside their authorized scope. Users are recommended to upgrade to version 3.2.1, which fixes this issue.	4.3	More Details
CVE-2026-5377	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.11 before 18.11.1 that could have allowed an authenticated user to access titles of confidential or private issues in public projects due to improper access control in the issue description rendering process.	4.3	More Details
CVE-2026-7116	A security flaw has been discovered in code-projects Employee Management System 1.0. This issue affects some unknown processing of the file 370project/mark.php. Performing a manipulation results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	4.3	More Details
CVE-2026-7129	A vulnerability was detected in SourceCodester Pharmacy Sales and Inventory System 1.0. Impacted is an unknown function of the file /index.php?page=categories. Performing a manipulation of the argument ID results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-7089	A security vulnerability has been detected in code-projects Home Service System 1.0. The impacted element is an unknown function of the file /booking.php of the component Appointment Booking. The manipulation of the argument fname/lname leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-6874	A vulnerability was determined in ericc-ch copilot-api up to 0.7.0. This impacts an unknown function of the file /token of the component Header Handler. Executing a manipulation of the argument Host can lead to reliance on reverse dns resolution. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-30346	An open redirect in the /api/google/authorize endpoint of hunvreus DevPush v0.3.2 allows attackers to redirect users to malicious sites via supplying a crafted URL.	4.3	More Details
CVE-2025-58922	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada allows Cross Site Request Forgery.This issue affects Avada: from n/a before 7.13.2.	4.3	More Details
CVE-2026-3565	The Taqnix plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.3. This is due to a missing nonce verification in the taqnix_delete_my_account() function, where the check_ajax_referer() call is explicitly commented out on line 883. This makes it possible for unauthenticated attackers to trick a logged-in non-administrator user into deleting their own account via a forged request granted they can trick the user into performing an action such as clicking a link or visiting a malicious page.	4.3	More Details
CVE-2026-	A security vulnerability has been detected in code-projects Invoice System in Laravel 1.0. This affects an unknown function. Such manipulation leads to cross-site request forgery. The attack may be performed from remote. The exploit has been	4.3	More Details

7108	disclosed publicly and may be used.		
CVE-2026-41079	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. Prior to 2.4.17, a network-adjacent attacker can send a crafted SNMP response to the CUPS SNMP backend that causes an out-of-bounds read of up to 176 bytes past a stack buffer. The leaked memory is converted from UTF-16 to UTF-8 and stored as printer supply description strings, which are subsequently visible to authenticated users via IPP Get-Printer-Attributes responses and the CUPS web interface. This vulnerability is fixed in 2.4.17.	4.3	More Details
CVE-2026-7086	A vulnerability was identified in HBAI-Ltd Toonflow-app up to 1.1.1. This issue affects the function updateStoryboardUrl of the file replaceUrl.ts of the component Storyboard Export. Such manipulation of the argument url leads to path traversal. It is possible to launch the attack remotely. The exploit is publicly available and might be used. It is still unclear if this vulnerability genuinely exists. The vendor explains in a reply to the issue report, that "[t]he URL of this interface is designed to only be a local address or a trusted domain address configured in docker, and will not contain malicious links, unless the user modifies the code causing unexpected situations."	4.3	More Details
CVE-2026-42420	OpenClaw before 2026.4.8 contains improper input validation in base64 decode paths that allocate memory before enforcing decoded-size limits. Attackers can exploit multiple code paths to cause memory exhaustion or denial of service through crafted base64-encoded input.	4.3	More Details
CVE-2026-7309	A flaw was found in the OpenShift Container Platform build system. A user with the `edit` ClusterRole can inject arbitrary environment variables, such as `LD_PRELOAD` or `http_proxy`, into `docker-build` containers through the `buildconfigs/instantiate` API. This incomplete fix for a previous vulnerability allows for information disclosure, specifically impacting the confidentiality of build traffic.	4.3	More Details
CVE-2025-62104	Missing Authorization vulnerability in Navneil Naicker ACF Galerie 4 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ACF Galerie 4: from n/a through 1.4.2.	4.3	More Details
CVE-2026-41126	BigBlueButton is an open-source virtual classroom. Versions prior to 3.0.24 have an Open Redirect through bigbluebutton/api/join via get-parameter "logoutURL." Version 3.0.24 has adjusted the handling of requests with incorrect checksum so that the default logoutURL is used. No known workarounds are available.	4.3	More Details
CVE-2026-38743	The authenticated /ui/dags endpoint did not enforce per-DAG access control on embedded Human-in-the-Loop (HITL) and TaskInstance records: a logged-in Airflow user with read access to at least one DAG could retrieve HITL prompts (including their request parameters) and full TaskInstance details for DAGs outside their authorized scope. Because HITL prompts and TaskInstance fields routinely carry operator parameters and free-form context attached to a task, the leak widens visibility of DAG-run data beyond the intended per-DAG RBAC boundary for every authenticated user. Users are recommended to upgrade to version 3.2.1 , which fixes this issue.	4.3	More Details
CVE-2026-41402	OpenClaw before 2026.3.31 contains a scope bypass vulnerability in webhook replay cache deduplication that allows authenticated attackers to replay messages across sibling targets using the same messageId. Attackers can exploit overly broad cache keying to bypass replay protection and deliver duplicate webhook messages to unintended targets.	4.2	More Details
CVE-2026-35351	The mv utility in uutils coreutils fails to preserve file ownership during moves across different filesystem boundaries. The utility falls back to a copy-and-delete routine that creates the destination file using the caller's UID/GID rather than the source's metadata. This flaw breaks backups and migrations, causing files moved by a privileged user (e.g., root) to become root-owned unexpectedly, which can lead to information disclosure or restricted access for the intended owners.	4.2	More Details
CVE-2026-40968	When an authenticated user is denied access to a gRPC method, their authenticated identity remains bound to the gRPC worker thread and can be inherited by a subsequent unauthenticated request on the same thread. This may allow the subsequent user to gain escalated permissions. Affected versions: Spring gRPC: 1.0.0 - 1.0.2 (fixed in 1.0.3). Older, unsupported versions are also affected.	4.2	More Details
CVE-2026-40254	FreeRDP is a free implementation of the Remote Desktop Protocol. Versions prior to 3.25.0 have an off-by-one in the path traversal filter in `channels/drive/client/drive_file.c`. The `contains_dotdot()` function catches `../` and `..\` mid-path but misses `..` when it's the last component with no trailing separator. A rogue RDP server can read, list, or write files one directory above the client's shared folder through RDPDR requests. This requires the victim to connect with drive redirection enabled. Version 3.25.0 patches the issue.	4.2	More Details
CVE-2026-42254	Hickory DNS hickory-recursor 0.1 through 0.25.2 allows cross-zone poisoning because cached data is not directly associated with a query that triggered a response.	4.0	More Details
CVE-2026-42095	bookserver in KDE Arianna before 26.04.1 allows attackers to read files over a socket connection by guessing a URL.	4.0	More Details
CVE-2026-41990	Libgcrypt before 1.12.2 mishandles Dilithium signing. Writes to a static array lack a bounds check but do not use attacker-controlled data.	4.0	More Details
CVE-2026-31051	An issue in Hostbill v.2025-11-24 and 2025-12-01 allows a remote attacker to cause a denial of service via the Client Balance component	3.8	More Details
CVE-2026-6986	A security vulnerability has been detected in Cesanta Mongoose up to 7.20. This issue affects the function mg_aes_gcm_decrypt of the file /src/tls_aes128.c of the component GCM Authentication Tag Handler. Such manipulation leads to improper verification of cryptographic signature. The attack may be performed from remote. A high complexity level is associated with this attack. The exploitability is assessed as difficult. The exploit has been disclosed publicly and may be used. Upgrading to version 7.21 is capable of addressing this issue. It is advisable to upgrade the affected	3.7	More Details

	component. VulDB has contacted the vendor early and they confirmed quickly, that this issue got fixed already.		
CVE-2026-41354	OpenClaw before 2026.4.2 contains an insufficient scope vulnerability in Zalo webhook replay dedupe keys that allows legitimate events from different conversations or senders to collide. Attackers can exploit weak deduplication scoping to cause silent message suppression and disrupt bot workflows across chat sessions.	3.7	More Details
CVE-2026-7103	A vulnerability was determined in code-projects Chat System 1.0. Affected is an unknown function of the file update_user.php of the component MD5 Hash Handler. This manipulation of the argument Password causes use of weak hash. The attack is possible to be carried out remotely. The attack's complexity is rated as high. The exploitability is told to be difficult. The exploit has been publicly disclosed and may be utilized.	3.7	More Details
CVE-2026-22746	Vulnerability in Spring Spring Security. If an application is using the UserDetails#isEnabled, #isAccountNonExpired, or #isAccountNonLocked user attributes, to enable, expire, or lock users, then DaoAuthenticationProvider's timing attack defense can be bypassed for users who are disabled, expired, or locked.This issue affects Spring Security: from 5.7.0 through 5.7.22, from 5.8.0 through 5.8.24, from 6.3.0 through 6.3.15, from 6.5.0 through 6.5.9, from 7.0.0 through 7.0.4.	3.7	More Details
CVE-2026-41913	OpenClaw before 2026.4.4 contains a race condition vulnerability in shared-secret authentication that allows concurrent asynchronous requests to bypass the per-key rate-limit budget. Attackers can exploit this by sending multiple simultaneous authentication attempts to circumvent intended rate-limiting protections on Tailscale-capable paths.	3.7	More Details
CVE-2026-33597	PRSD detection denial of service	3.7	More Details
CVE-2026-42040	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, the encode() function in lib/helpers/AxiosURLSearchParams.js contains a character mapping (charMap) at line 21 that reverses the safe percent-encoding of null bytes. After encodeURIComponent('\x00') correctly produces the safe sequence %00, the charMap entry '%00': '\x00' converts it back to a raw null byte. Primary impact is limited because the standard axios request flow is not affected. This vulnerability is fixed in 1.15.1 and 0.31.1.	3.7	More Details
CVE-2026-7041	A vulnerability was detected in 666ghj MiroFish up to 0.1.2. The impacted element is an unknown function of the file /console of the component Werkzeug Debugger PIN Handler. Performing a manipulation of the argument SECRET results in information disclosure. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is regarded as difficult. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.7	More Details
CVE-2026-2708	A request smuggling vulnerability exists in libsoup's HTTP/1 header parsing logic. The soup_message_headers_append_common() function in libsoup/soup-message-headers.c unconditionally appends each header value without validating for duplicate or conflicting Content-Length fields. This allows an attacker to send HTTP requests containing multiple Content-Length headers with differing values.	3.7	More Details
CVE-2026-40969	The raw message of every server-side AuthenticationException is returned to the unauthenticated remote caller in the gRPC status description. This allows an attacker to obtain information about the authentication failure, which may be useful for further attacks. Affected versions: Spring gRPC: 1.0.0 - 1.0.2 (fixed in 1.0.3). Older, unsupported versions are also affected.	3.7	More Details
CVE-2026-7303	A security flaw has been discovered in Xuxueli xxl-job up to 3.3.2. Impacted is the function logDetailCat of the file xxl-job-admin/src/main/java/com/xxl/job/admin/controller/biz/JobLogController.java of the component Execution Log Handler. The manipulation of the argument logId results in improper control of resource identifiers. The attack may be performed from remote. This attack is characterized by high complexity. The exploitability is considered difficult. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.4.0 is recommended to address this issue. The patch is identified as d24e4ccd6073cc75305e1d3b9c29bc8db7437e7a. It is suggested to upgrade the affected component.	3.7	More Details
CVE-2026-41407	OpenClaw before 2026.4.2 contains a timing side channel vulnerability in shared-secret comparison call sites that use early length-mismatch checks instead of fixed-length comparison helpers. Attackers can measure timing differences to leak secret-length information, weakening constant-time handling for shared secrets.	3.7	More Details
CVE-2026-41333	OpenClaw before 2026.3.31 contains an authentication rate limiting bypass vulnerability that allows attackers to circumvent shared authentication protections using fake device tokens. Attackers can exploit the mixed WebSocket authentication flow to bypass rate limiting controls and conduct brute force attacks against weak shared passwords.	3.7	More Details
CVE-2026-35362	The safe_traversal module in uutils coreutils, which provides protection against Time-of-Check to Time-of-Use (TOCTOU) symlink races using file-descriptor-relative syscalls, is incorrectly limited to Linux targets. On other Unix-like systems such as macOS and FreeBSD, the utility fails to utilize these protections, leaving directory traversal operations vulnerable to symlink race conditions.	3.6	More Details
CVE-2026-3254	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.11 before 18.11.1 that under certain conditions could have allowed an authenticated user to load unauthorized content into another user's browser due to improper input validation in the Mermaid sandbox.	3.5	More Details
CVE-2026-7110	A flaw has been found in code-projects Invoice System in Laravel 1.0. Affected is an unknown function of the file /item. Executing a manipulation of the argument item name/description can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	3.5	More Details
CVE-2026-7222	A vulnerability was determined in code-projects Coaching Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /cims/modules/student/complaint.php of the component Complaint Form Page. This manipulation of the argument Complaint causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	3.5	More Details
CVE-2026-	A vulnerability was found in projeto-siga siga 11.0.3.18. The affected element is an unknown function of the file /sigawf/app/responsavel/novo. Performing a manipulation of the argument Nome/Descrição results in cross site scripting.	3.5	More

6990	The attack can be initiated remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.		Details
CVE-2026-4512	The reCaptcha by WebDesignBy WordPress plugin before 2.0 does not sanitize or escape the Site Key setting before outputting it in a JavaScript string context via the grecaptcha_js() function. This allows administrators on multisite installations (who do not have the unfiltered_html capability) to inject arbitrary JavaScript that executes for all visitors to the WordPress login page.	3.5	More Details
CVE-2026-7021	A weakness has been identified in SmythOS sre up to 0.0.15. This impacts an unknown function of the file packages/sdk/src/LLM/utils.ts of the component Connector Service. This manipulation of the argument baseURL causes information disclosure. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-35361	The mknod utility in uutils coreutils fails to handle security labels atomically by creating device nodes before setting the SELinux context. If labeling fails, the utility attempts cleanup using std::fs::remove_dir, which cannot remove device nodes or FIFOs. This leaves mislabeled nodes behind with incorrect default contexts, potentially allowing unauthorized access to device nodes that should have been restricted by mandatory access controls.	3.4	More Details
CVE-2026-7233	A vulnerability was determined in Artifex MuPDF up to 1.28.0. The impacted element is the function fz_subset_cff_for_gids of the file subset-cff.c of the component CFF Index Handler. This manipulation causes out-of-bounds read. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through a bug report but has not responded yet.	3.3	More Details
CVE-2026-41357	OpenClaw before 2026.3.31 contains an environment variable leakage vulnerability in SSH-based sandbox backends that pass unsanitized process.env to child processes. Attackers can exploit this by leveraging non-default SSH environment forwarding configurations to leak sensitive environment variables from parent processes to SSH child processes.	3.3	More Details
CVE-2026-35343	The cut utility in uutils coreutils incorrectly handles the -s (only-delimited) option when a newline character is specified as the delimiter. The implementation fails to verify the only_delimited flag in the cut_fields_newline_char_delim function, causing the utility to print non-delimited lines that should have been suppressed. This can lead to unexpected data being passed to downstream scripts that rely on strict output filtering.	3.3	More Details
CVE-2026-35379	A logic error in the tr utility of uutils coreutils causes the program to incorrectly define the [:graph:] and [:print:] character classes. The implementation mistakenly includes the ASCII space character (0x20) in the [:graph:] class and excludes it from the [:print:] class, effectively reversing the standard behavior established by POSIX and GNU coreutils. This vulnerability leads to unintended data modification or loss when the utility is used in automated scripts or data-cleaning pipelines that rely on standard character class semantics. For example, a command executed to delete all graphical characters while intending to preserve whitespace will incorrectly delete all ASCII spaces, potentially resulting in data corruption or logic failures in downstream processing.	3.3	More Details
CVE-2026-35342	The mktemp utility in uutils coreutils fails to properly handle an empty TMPDIR environment variable. Unlike GNU mktemp, which falls back to /tmp when TMPDIR is an empty string, the uutils implementation treats the empty string as a valid path. This causes temporary files to be created in the current working directory (CWD) instead of the intended secure temporary directory. If the CWD is more permissive or accessible to other users than /tmp, it may lead to unintended information disclosure or unauthorized access to temporary data.	3.3	More Details
CVE-2026-35344	The dd utility in uutils coreutils suppresses errors during file truncation operations by unconditionally calling Result::ok() on truncation attempts. While intended to mimic GNU behavior for special files like /dev/null, the uutils implementation also hides failures on regular files and directories caused by full disks or read-only file systems. This can lead to silent data corruption in backup or migration scripts, as the utility may report a successful operation even when the destination file contains old or garbage data.	3.3	More Details
CVE-2026-35346	The comm utility in uutils coreutils silently corrupts data by performing lossy UTF-8 conversion on all output lines. The implementation uses String::from_utf8_lossy(), which replaces invalid UTF-8 byte sequences with the Unicode replacement character (U+FFFD). This behavior differs from GNU comm, which processes raw bytes and preserves the original input. This results in corrupted output when the utility is used to compare binary files or files using non-UTF-8 legacy encodings.	3.3	More Details
CVE-2026-35353	The mkdir utility in uutils coreutils incorrectly applies permissions when using the -m flag by creating a directory with umask-derived permissions (typically 0755) before subsequently changing them to the requested mode via a separate chmod system call. In multi-user environments, this introduces a brief window where a directory intended to be private is accessible to other users, potentially leading to unauthorized data access.	3.3	More Details
CVE-2026-35367	The nohup utility in uutils coreutils creates its default output file, nohup.out, without specifying explicit restricted permissions. This causes the file to inherit umask-based permissions, typically resulting in a world-readable file (0644). In multi-user environments, this allows any user on the system to read the captured stdout/stderr output of a command, potentially exposing sensitive information. This behavior diverges from GNU coreutils, which creates nohup.out with owner-only (0600) permissions.	3.3	More Details
CVE-2026-35371	The id utility in uutils coreutils exhibits incorrect behavior in its "pretty print" output when the real UID and effective UID differ. The implementation incorrectly uses the effective GID instead of the effective UID when performing a name lookup for the effective user. This results in misleading diagnostic output that can cause automated scripts or system administrators to make incorrect decisions regarding file permissions or access control.	3.3	More Details
CVE-2026-35373	A logic error in the ln utility of uutils coreutils causes the program to reject source paths containing non-UTF-8 filename bytes when using target-directory forms (e.g., ln SOURCE... DIRECTORY). While GNU ln treats filenames as raw bytes and creates the links correctly, the uutils implementation enforces UTF-8 encoding, resulting in a failure to stat the file and a non-zero exit code. In environments where automated scripts or system tasks process valid but non-UTF-8 filenames common on Unix filesystems, this divergence causes the utility to fail, leading to a local denial of service for those specific operations.	3.3	More Details

CVE-2026-35375	A logic error in the split utility of uutils coreutils causes the corruption of output filenames when provided with non-UTF-8 prefix or suffix inputs. The implementation utilizes to_string_lossy() when constructing chunk filenames, which automatically rewrites invalid byte sequences into the UTF-8 replacement character (U+FFFD). This behavior diverges from GNU split, which preserves raw pathname bytes intact. In environments utilizing non-UTF-8 encodings, this vulnerability leads to the creation of files with incorrect names, potentially causing filename collisions, broken automation, or the misdirection of output data.	3.3	More Details
CVE-2026-35377	A logic error in the env utility of uutils coreutils causes a failure to correctly parse command-line arguments when utilizing the -S (split-string) option. In GNU env, backslashes within single quotes are treated literally (with the exceptions of \\ and \'). However, the uutils implementation incorrectly attempts to validate these sequences, resulting in an "invalid sequence" error and an immediate process termination with an exit status of 125 when encountering valid but unrecognized sequences like \a or \x. This divergence from GNU behavior breaks compatibility for automated scripts and administrative workflows that rely on standard split-string semantics, leading to a local denial of service for those operations.	3.3	More Details
CVE-2026-35378	A logic error in the expr utility of uutils coreutils causes the program to evaluate parenthesized subexpressions during the parsing phase rather than at the execution phase. This implementation flaw prevents the utility from performing proper short-circuiting for logical OR (|) and AND (&) operations. As a result, arithmetic errors (such as division by zero) occurring within "dead" branches, branches that should be ignored due to short-circuiting, are raised as fatal errors. This divergence from GNU expr behavior can cause guarded expressions within shell scripts to fail with hard errors instead of returning expected boolean results, leading to premature script termination and breaking GNU-compatible shell control flow.	3.3	More Details
CVE-2026-35381	A logic error in the cut utility of uutils coreutils causes the utility to ignore the -s (only-delimited) flag when using the -z (null-terminated) and -d '' (empty delimiter) options together. The implementation incorrectly routes this specific combination through a specialized newline-delimiter code path that fails to check the record suppression status. Consequently, uutils cut emits the entire record plus a NUL byte instead of suppressing it. This divergence from GNU coreutils behavior creates a data integrity risk for automated pipelines that rely on cut -s to filter out undelimited data.	3.3	More Details
CVE-2026-7038	A weakness has been identified in tufantunc ssh-mcp up to 1.5.0. Impacted is an unknown function of the file src/index.ts of the component Command Line Handler. This manipulation causes insufficiently protected credentials. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-41988	uuid before 14.0.0 can make unexpected writes when external output buffers are used, and the UUID version is 3, 5, or 6. In particular, UUID version 4, which is very commonly used, is unaffected by this issue.	3.2	More Details
CVE-2026-33596	A client might theoretically be able to cause a mismatch between queries sent to a backend and the received responses by sending a flood of perfectly timed queries that are routed to a TCP-only or DNS over TLS backend.	3.1	More Details
CVE-2026-34067	nimiq-transaction provides the transaction primitive to be used in Nimiq's Rust implementation. Prior to version 1.3.0, `HistoryTreeProof::verify` panics on a malformed proof where `history.len() != positions.len()` due to `assert_eq!(history.len(), positions.len())`. The proof object is derived from untrusted p2p responses (`ResponseTransactionsProof.proof`) and is therefore attacker-controlled at the network boundary until validated. A malicious peer could trigger a crash by returning a crafted inclusion proof with a length mismatch. The patch for this vulnerability is included as part of v1.3.0. No known workarounds are available.	3.1	More Details
CVE-2026-33599	A rogue backend can send a crafted SVCB response to a Discovery of Designated Resolvers request, when requested via either the autoUpgrade (Lua) option to newServer or auto_upgrade (YAML) settings. DDR upgrade is not enabled by default.	3.1	More Details
CVE-2026-41488	LangChain is a framework for building agents and LLM-powered applications. Prior to 1.1.14, langchain-openai's _url_to_size() helper (used by get_num_tokens_from_messages for image token counting) validated URLs for SSRF protection and then fetched them in a separate network operation with independent DNS resolution. This left a TOCTOU / DNS rebinding window: an attacker-controlled hostname could resolve to a public IP during validation and then to a private/localhost IP during the actual fetch.	3.1	More Details
CVE-2026-41403	OpenClaw before 2026.3.31 misclassifies proxied remote requests as loopback connections in the diffs viewer when allowRemoteViewer is disabled, allowing unauthorized access. Attackers can bypass access controls by sending proxied requests that are incorrectly identified as local loopback traffic, circumventing intended remote viewer restrictions.	2.9	More Details
CVE-2025-9957	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.2 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that under certain conditions could have allowed an authenticated user with project owner permissions to bypass group fork prevention settings due to improper authorization checks.	2.7	More Details
CVE-2026-6392	Tanium addressed an information disclosure vulnerability in Threat Response.	2.7	More Details
CVE-2026-6408	Tanium addressed an information disclosure vulnerability in Tanium Server.	2.7	More Details
CVE-2026-6416	Tanium addressed an uncontrolled resource consumption vulnerability in Interact.	2.7	More Details
CVE-2026-1272	IBM Guardium Data Protection 12.0, 12.1, and 12.2 is vulnerable to Security Misconfiguration vulnerability in the user access control panel.	2.7	More Details

CVE-2026-6842	A flaw was found in nano. In environments with permissive umask settings, a local attacker can exploit incorrect directory permissions (0777 instead of 0700) for the `~/.local` directory. This allows the attacker to inject a malicious `.desktop` launcher, which could lead to unintended actions or information disclosure if the launcher is subsequently processed.	2.5	More Details
CVE-2026-7016	A vulnerability was found in MaxSite CMS up to 109.3. Impacted is an unknown function of the component ushki Plugin. Performing a manipulation of the argument f_ushka_new/f_ushk results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been made public and could be used. Upgrading to version 109.4 is recommended to address this issue. The patch is named 8a3946bd0a54bfb72a4d57179fcd253f2c550cd7. Upgrading the affected component is recommended. The vendor was informed early about this issue. They classify it as a "Self-XSS". They deployed a countermeasure: "Nevertheless, we consider this a violation of secure coding standards. The lack of filtering via `htmlspecialchars()` has already been fixed in the latest patch to prevent incorrect data display."	2.4	More Details
CVE-2026-7027	A vulnerability was identified in D-Link DSL-2740R EU_01.15. Impacted is an unknown function of the component Wireless Setup Section. Such manipulation of the argument Wireless Network Name leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used.	2.4	More Details
CVE-2026-7295	A vulnerability has been found in SourceCodester Pizzafy Ecommerce System 1.0. Affected by this issue is the function save_menu of the file /admin/ajax.php?action=save_menu. Such manipulation of the argument Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2026-7090	A vulnerability was detected in code-projects Chat System 1.0. This affects an unknown function of the file /admin/send_message.php of the component Chat Interface. The manipulation of the argument msg results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2026-7014	A flaw has been found in MaxSite CMS up to 109.3. This vulnerability affects unknown code of the component down_count Plugin. This manipulation of the argument f_file/f_prefix causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used. Upgrading to version 109.4 is able to resolve this issue. Patch name: 8a3946bd0a54bfb72a4d57179fcd253f2c550cd7. The affected component should be upgraded. The vendor was informed early about this issue. They classify it as a "Self-XSS". They deployed a countermeasure: "Nevertheless, we consider this a violation of secure coding standards. The lack of filtering via `htmlspecialchars()` has already been fixed in the latest patch to prevent incorrect data display."	2.4	More Details
CVE-2026-6999	A flaw has been found in BIVOCOM TR321 21.1.1.50. Affected by this vulnerability is an unknown functionality of the component Wireless Setting. This manipulation of the argument Network Name SSID causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-6998	A vulnerability was detected in BDCOM P3310D 0.4.2 10.1.0F Build 86345. Affected is an unknown function of the component New RMON Statistics Page. The manipulation of the argument Owner results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-6997	A security vulnerability has been detected in BDCOM P3310D 0.4.2 10.1.0F Build 86345. This impacts an unknown function of the component New RMON History Page. The manipulation of the argument Owner leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-6996	A weakness has been identified in BDCOM P3310D 0.4.2 10.1.0F Build 86345. This affects an unknown function of the component rmon event Tab. Executing a manipulation of the argument Description can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-6995	A security flaw has been discovered in BDCOM P3310D 0.4.2 10.1.0F Build 86345. The impacted element is an unknown function of the file /index.asp of the component New User Page. Performing a manipulation of the argument User name results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-7015	A vulnerability has been found in MaxSite CMS up to 109.3. This issue affects some unknown processing of the component Guestbook Plugin. Such manipulation of the argument f_text/f_slug/f_limit/f_email leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 109.4 is capable of addressing this issue. The name of the patch is 8a3946bd0a54bfb72a4d57179fcd253f2c550cd7. It is suggested to upgrade the affected component. The vendor was informed early about this issue. They classify it as a "Self-XSS". They deployed a countermeasure: "Nevertheless, we consider this a violation of secure coding standards. The lack of filtering via `htmlspecialchars()` has already been fixed in the latest patch to prevent incorrect data display."	2.4	More Details
CVE-2026-7294	A flaw has been found in SourceCodester Pizzafy Ecommerce System 1.0. Affected by this vulnerability is the function save_settings of the file /admin/index.php?page=save_settings. This manipulation of the argument Name causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2026-7296	A vulnerability was found in SourceCodester Pizzafy Ecommerce System 1.0. This affects the function save_order of the file /admin/ajax.php?action=save_order. Performing a manipulation of the argument first_name results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2.4	More Details
CVE-2026-7297	A vulnerability was determined in SourceCodester Pizzafy Ecommerce System 1.0. This vulnerability affects the function save_user of the file /admin/ajax.php?action=save_user. Executing a manipulation of the argument Name can lead to cross site scripting. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-	A security vulnerability has been detected in MaxSite CMS up to 109.3. Affected by this issue is some unknown functionality of the component mail_send Plugin. The manipulation of the argument f_subject/f_files/f_from leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 109.4		

2026-7013	can resolve this issue. The identifier of the patch is 8a3946bd0a54bfb72a4d57179fcd253f2c550cd7. It is advisable to upgrade the affected component. The vendor was informed early about this issue. They classify it as a "Self-XSS". They deployed a countermeasure: "Nevertheless, we consider this a violation of secure coding standards. The lack of filtering via `htmlspecialchars()` has already been fixed in the latest patch to prevent incorrect data display."	2.4	More Details
CVE-2026-7012	A vulnerability was detected in MaxSite CMS up to 109.3. This affects an unknown part of the component Redirect Plugin. The manipulation of the argument f_all/f_all404 results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used. Upgrading to version 109.4 is able to mitigate this issue. The patch is identified as 8a3946bd0a54bfb72a4d57179fcd253f2c550cd7. You should upgrade the affected component. The vendor was informed early about this issue. They classify it as a "Self-XSS". They deployed a countermeasure: "Nevertheless, we consider this a violation of secure coding standards. The lack of filtering via `htmlspecialchars()` has already been fixed in the latest patch to prevent incorrect data display."	2.4	More Details
CVE-2026-7000	A vulnerability has been found in Datacom DM4100 1.3.6.1.4.1.3709. Affected by this issue is some unknown functionality of the component VLAN Page. Such manipulation of the argument VLAN Name leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-7011	A weakness has been identified in MaxSite CMS up to 109.3. Affected by this vulnerability is an unknown functionality of the file /admin/plugin_antispam of the component Antispam Plugin. Executing a manipulation of the argument f_logging_file can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 109.4 addresses this issue. This patch is called 8a3946bd0a54bfb72a4d57179fcd253f2c550cd7. Upgrading the affected component is advised. The vendor was informed early about this issue. They classify it as a "Self-XSS". They deployed a countermeasure: "Nevertheless, we consider this a violation of secure coding standards. The lack of filtering via `htmlspecialchars()` has already been fixed in the latest patch to prevent incorrect data display."	2.4	More Details
CVE-2026-7001	A vulnerability was found in Datacom DM4100 1.3.6.1.4.1.3709. This affects an unknown part of the component Ethernet Configuration Page. Performing a manipulation of the argument Name results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-7269	A vulnerability was found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected is an unknown function of the file /index.php?page=product. Performing a manipulation of the argument ID results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2.4	More Details
CVE-2026-7281	A vulnerability was determined in SourceCodester Pharmacy Sales and Inventory System 1.0. The impacted element is the function supplier of the file /index.php?page=supplier. Executing a manipulation of the argument Name can lead to cross site scripting. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-2026-41321	@astrojs/cloudflare is an SSR adapter for use with Cloudflare Workers targets. Prior to 13.1.10, the fetch() call for remote images in packages/integrations/cloudflare/src/utils/image-binding-transform.ts uses the default redirect: 'follow' behavior. This allows the Cloudflare Worker to follow HTTP redirects to arbitrary URLs, bypassing the isRemoteAllowed() domain allowlist check which only validates the initial URL. This vulnerabiity is caused by an incomplete fix for CVE-2025-58179. This vulnerability is fixed in 13.1.10.	2.2	More Details
CVE-2026-41144	F´ (F Prime) is a framework that enables development and deployment of spaceflight and other embedded software applications. Prior to version 4.2.0, the bounds check byteOffset + dataSize > fileSize uses U32 addition that wraps around on overflow. An attacker-crafted DataPacket with byteOffset=0xFFFFFF9C and dataSize=100 overflows to 0, bypassing the check entirely. The subsequent file write proceeds at the original ~4GB offset. Additionally, Svc/FileUplink/File.cpp:20-31 performs no sanitization on the destination file path. Combined, these allow writing arbitrary data to any file at any offset. The impact is arbitrary file write leading to remote code execution on embedded targets. Note that this is a logic bug. ASAN does not detect it because all memory accesses are within valid buffers — the corruption occurs in file I/O. Version 4.2.0 contains a patch. No known workarounds are available.	0.0	More Details
CVE-2026-37750	A reflected Cross-Site Scripting (XSS) vulnerability in School Management System by mahmoudai1 allows unauthenticated remote attackers to execute arbitrary JavaScript in victim's browsers via the unsanitized type parameter in register.php.	N/A	More Details
CVE-2026-7359	Use after free in ANGLE in Google Chrome prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7360	Insufficient validation of untrusted input. in Compositing in Google Chrome prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7361	Use after free in iOS in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	N/A	More Details
CVE-2026-41446	Snap One WattBox 800 and 820 series firmware versions prior to 2.10.0.0 contain undisclosed diagnostic HTTP endpoints that require only the device MAC address and service tag for authentication, both of which are printed in plaintext on the physical device label. Attackers with access to the device label or documentation containing these values can authenticate to the several endpoints and execute arbitrary commands as root on the device.	N/A	More Details
CVE-2026-7358	Use after free in Animation in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details

CVE-2026-7355	Use after free in Media in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2026-7349	Use after free in Cast in Google Chrome prior to 147.0.7727.138 allowed an attacker on the local network segment to execute arbitrary code inside a sandbox via malicious network traffic. (Chromium security severity: High)	N/A	More Details
CVE-2026-7352	Use after free in Media in Google Chrome on Android prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7357	Use after free in GPU in Google Chrome prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7356	Use after free in Navigation in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7353	Heap buffer overflow in Skia in Google Chrome prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7345	Insufficient validation of untrusted input in Feedback in Google Chrome prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-38949	Cross-Site Scripting (XSS) vulnerability exists in HTMLy version 3.1.1 in the content creation functionality at the /add/content?type=image endpoint. The application fails to properly sanitize user input, allowing injection of arbitrary code	N/A	More Details
CVE-2026-7335	Use after free in media in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7346	Inappropriate implementation in Tint in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7343	Use after free in Views in Google Chrome on Windows prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	N/A	More Details
CVE-2026-7342	Use after free in WebView in Google Chrome on Android prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7341	Use after free in WebRTC in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7340	Integer overflow in ANGLE in Google Chrome on Windows prior to 147.0.7727.138 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2026-7339	Heap buffer overflow in WebRTC in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2026-7338	Use after free in Cast in Google Chrome prior to 147.0.7727.138 allowed an attacker on the local network segment to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: High)	N/A	More Details
CVE-2026-7337	Type Confusion in V8 in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7336	Use after free in WebRTC in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7334	Use after free in Views in Google Chrome on Mac prior to 147.0.7727.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7354	Out of bounds read and write in Angle in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-			

2026-7333	Use after free in GPU in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-5822	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-7347	Use after free in Chromoting in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: High)	N/A	More Details
CVE-2026-7351	Race in MHTML in Google Chrome prior to 147.0.7727.138 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: High)	N/A	More Details
CVE-2025-60889	Insecure deserialization of untrusted input in StellarGroup HPX 1.11.0 under certain conditions may allow attackers to execute arbitrary code or other unspecified impacts.	N/A	More Details
CVE-2026-5794	A vulnerability affecting the detailed versions of Cryptobox allows a legitimate user to prevent another to login by triggering an account lockout via sending a specially crafted request.	N/A	More Details
CVE-2026-40556	GNU nano creates the user's ~/.local directory with overly permissive permissions when the directory does not exist yet. On first use of features requiring Cross-Desktop Group (XDG) data storage, nano explicitly requests directory mode 0777, making the directory world-writable in environments where the process umask does not sufficiently restrict permissions. In systems with a relaxed or zero umask, such as container environments, CI/CD runners, embedded systems, or user shells configured with umask 000, this results in ~/.local being created as world-writable. A local attacker can exploit a race window between nano's creation of ~/.local and its subsequent creation of more restrictive subdirectories to write attacker-controlled files into the victim's XDG directory hierarchy. This problem was fixed in nano version 9.0	N/A	More Details
CVE-2026-7344	Use after free in Accessibility in Google Chrome on Windows prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	N/A	More Details
CVE-2026-7348	Use after free in Codecs in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-7350	Use after free in WebMIDI in Google Chrome prior to 147.0.7727.138 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-31599	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: fix NULL pointer dereference in vidtv_channel_pmt_match_sections syzbot reported a general protection fault in vidtv_psi_desc_assign [1]. vidtv_psi_pmt_stream_init() can return NULL on memory allocation failure, but vidtv_channel_pmt_match_sections() does not check for this. When tail is NULL, the subsequent call to vidtv_psi_desc_assign(&tail->descriptor, desc) dereferences a NULL pointer offset, causing a general protection fault. Add a NULL check after vidtv_psi_pmt_stream_init(). On failure, clean up the already-allocated stream chain and return. [1] Oops: general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:vidtv_psi_desc_assign+0x24/0x90 drivers/media/test-drivers/vidtv/vidtv_psi.c:629 Call Trace: <TASK> vidtv_channel_pmt_match_sections drivers/media/test-drivers/vidtv/vidtv_channel.c:349 [inline] vidtv_channel_si_init+0x1445/0x1a50 drivers/media/test-drivers/vidtv/vidtv_channel.c:479 vidtv_mux_init+0x526/0xbe0 drivers/media/test-drivers/vidtv/vidtv_mux.c:519 vidtv_start_streaming drivers/media/test-drivers/vidtv/vidtv_bridge.c:194 [inline] vidtv_start_feed+0x33e/0x4d0 drivers/media/test-drivers/vidtv/vidtv_bridge.c:239	N/A	More Details
CVE-2026-40552	mpGabinet is vulnerable to Remote Command Execution. An authorized user with access to the application and direct access to the backend database can achieve system command execution by uploading an attachment and modifying its storage path in the database to reference an attacker-controlled remote network resource. Alternatively, it is possible to use a previously uploaded file and change its reference. When the application processes the attachment, and a user tries to open it, the referenced resource is executed by the system. Critically, this vulnerability can be exploited by any unauthenticated attacker by chaining it with CVE-2026-40550 and CVE-2026-40551, which allows obtaining database access, and logging onto any account. This issue affects mpGabinet version 23.12.19 and below.	N/A	More Details
CVE-2026-3837	An authenticated attacker can persist crafted values in multiple field types and trigger client-side script execution when another user opens the affected document in Desk. The vulnerable formatter implementations interpolate stored values into raw HTML attributes and element content without escaping This issue affects Frappe: 16.10.0.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mm/pagewalk: fix race between concurrent split and refault The splitting of a PUD entry in walk_pud_range() can race with a concurrent thread refaulting the PUD leaf entry causing it to try walking a PMD range that has disappeared. An example and reproduction of this is to try reading numa_maps of a process while VFIO-PCI is setting up DMA (specifically the vfio_pin_pages_remote call) on a large BAR for that process. This will trigger a kernel BUG: vfio-pci 0000:03:00.0: enabling device (0000 -> 0002) BUG: unable to handle page fault for address: ffffa23980000000 PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI ... RIP: 0010:walk_pgd_range+0x3b5/0x7a0 Code: 8d 43 ff 48 89 44 24 28 4d 89 ce 4d 8d a7 00 00 20 00 48 8b 4c 24 28 49 81 e4 00 00 e0 ff 49 8d 44 24 ff 48 39 c8 4c 0f 43 e3 <49> f7 06 9f ff ff ff 75 3b 48 8b 44 24 20 48 8b 40 28 48 85 c0 74 RSP: 0018:ffffac23e1ecf808 EFLAGS: 00010287 RAX: 00007f44c01fffff RBX: 00007f4500000000 RCX: 00007f44ffffffff RDX: 0000000000000000 RSI: 000fffffffffff000 RDI: ffffffff93378fe0 RBP: ffffac23e1ecf918 R08: 0000000000000004 R09: ffffa23980000000 R10: 0000000000000020 R11: 0000000000000004 R12: 00007f44c0200000 R13: 00007f44c0000000		

CVE-2026-31456	R14: ffffa23980000000 R15: 00007f44c0000000 FS: 00007fe884739580(0000) GS:ffff9b7d7a9c0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffa23980000000 CR3: 000000c0650e2005 CR4: 0000000000770ef0 PKRU: 55555554 Call Trace: <TASK> __walk_page_range+0x195/0x1b0 walk_page_vma+0x62/0xc0 show_numa_map+0x12b/0x3b0 seq_read_iter+0x297/0x440 seq_read+0x11d/0x140 vfs_read+0xc2/0x340 ksys_read+0x5f/0xe0 do_syscall_64+0x68/0x130 ? get_page_from_freelist+0x5c2/0x17e0 ? mas_store_prealloc+0x17e/0x360 ? vma_set_page_prot+0x4c/0xa0 ? __alloc_pages_noprof+0x14e/0x2d0 ? __mod_memcg_lruvec_state+0x8d/0x140 ? __lruvec_stat_mod_folio+0x76/0xb0 ? __folio_mod_stat+0x26/0x80 ? do_anonymous_page+0x705/0x900 ? __handle_mm_fault+0xa8d/0x1000 ? __count_memcg_events+0x53/0xf0 ? handle_mm_fault+0xa5/0x360 ? do_user_addr_fault+0x342/0x640 ? arch_exit_to_user_mode_prepare.constprop.0+0x16/0xa0 ? irqentry_exit_to_user_mode+0x24/0x100 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fe88464f47e Code: c0 e9 b6 fe ff ff 50 48 8d 3d be 07 0b 00 e8 69 01 02 00 66 0f 1f 84 00 00 00 00 00 64 8b 04 25 18 00 00 00 85 c0 75 14 0f 05 <48> 3d 00 f0 ff ff 77 5a c3 66 0f 1f 84 00 00 00 00 00 48 83 ec 28 RSP: 002b:00007ffe6cd9a9b8 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 RAX: ffffffffffffffda RBX: 0000000000020000 RCX: 00007fe88464f47e RDX: 0000000000020000 RSI: 00007fe884543000 RDI: 0000000000000003 RBP: 00007fe884543000 R08: 00007fe884542010 R09: 0000000000000000 R10: ffffffffffffbc5 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000003 R14: 0000000000020000 R15: 0000000000020000 </TASK> Fix this by validating the PUD entry in walk_pmd_range() using a stable snapshot (pudp_get()). If the PUD is not present or is a leaf, retry the walk via ACTION_AGAIN instead of descending further. This mirrors the retry logic in walk_pte_range(), which lets walk_pmd_range() retry if the PTE is not being got by pte_offset_map_lock().	N/A	More Details
CVE-2026-31457	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: check contexts->nr in repeat_call_fn damon_sysfs_repeat_call_fn() calls damon_sysfs_upd_tuned_intervals(), damon_sysfs_upd_schemes_stats(), and damon_sysfs_upd_schemes_effective_quotas() without checking contexts->nr. If nr_contexts is set to 0 via sysfs while DAMON is running, these functions dereference contexts_arr[0] and cause a NULL pointer dereference. Add the missing check. For example, the issue can be reproduced using DAMON sysfs interface and DAMON user-space tool (damo) [1] like below. $ sudo damo start --refresh_interval 1s $ echo 0 | sudo tee \ /sys/kernel/mm/damon/admin/kdamonds/0/contexts/nr_contexts	N/A	More Details
CVE-2026-31458	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: check contexts->nr before accessing contexts_arr[0] Multiple sysfs command paths dereference contexts_arr[0] without first verifying that kdamond->contexts->nr == 1. A user can set nr_contexts to 0 via sysfs while DAMON is running, causing NULL pointer dereferences. In more detail, the issue can be triggered by privileged users like below. First, start DAMON and make contexts directory empty (kdamond->contexts->nr == 0). # damo start # cd /sys/kernel/mm/damon/admin/kdamonds/0 # echo 0 > contexts/nr_contexts Then, each of below commands will cause the NULL pointer dereference. # echo update_schemes_stats > state # echo update_schemes_tried_regions > state # echo update_schemes_tried_bytes > state # echo update_schemes_effective_quotas > state # echo update_tuned_intervals > state Guard all commands (except OFF) at the entry point of damon_sysfs_handle_cmd().	N/A	More Details
CVE-2026-31459	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: fix param_ctx leak on damon_sysfs_new_test_ctx() failure Patch series "mm/damon/sysfs: fix memory leak and NULL dereference issues", v4. DAMON_SYSFS can leak memory under allocation failure, and do NULL pointer dereference when a privileged user make wrong sequences of control. Fix those. This patch (of 3): When damon_sysfs_new_test_ctx() fails in damon_sysfs_commit_input(), param_ctx is leaked because the early return skips the cleanup at the out label. Destroy param_ctx before returning.	N/A	More Details
CVE-2026-31460	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: check if ext_caps is valid in BL setup LVDS connectors don't have extended backlight caps so check if the pointer is valid before accessing it. (cherry picked from commit 3f797396d7f4eb9bb6eded184bbc6f033628a6f6)	N/A	More Details
CVE-2026-31461	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix drm_edid leak in amdgpu_dm [WHAT] When a sink is connected, aconnector->drm_edid was overwritten without freeing the previous allocation, causing a memory leak on resume. [HOW] Free the previous drm_edid before updating it. (cherry picked from commit 52024a94e7111366141cfc5d888b2ef011f879e5)	N/A	More Details
CVE-2026-31462	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: prevent immediate PASID reuse case PASID resue could cause interrupt issue when process immediately runs into hw state left by previous process exited with the same PASID, it's possible that page faults are still pending in the IH ring buffer when the process exits and frees up its PASID. To prevent the case, it uses idr cyclic allocator same as kernel pid's. (cherry picked from commit 8f1de51f49be692de137c8525106e0fce2d1912d)	N/A	More Details
CVE-2026-31465	In the Linux kernel, the following vulnerability has been resolved: writeback: don't block sync for filesystems with no data integrity guarantees Add a SB_I_NO_DATA_INTEGRITY superblock flag for filesystems that cannot guarantee data persistence on sync (eg fuse). For superblocks with this flag set, sync kicks off writeback of dirty inodes but does not wait for the flusher threads to complete the writeback. This replaces the per-inode AS_NO_DATA_INTEGRITY mapping flag added in commit f9a49aa302a0 ("fs/writeback: skip AS_NO_DATA_INTEGRITY mappings in wait_sb_inodes()"). The flag belongs at the superblock level because data integrity is a filesystem-wide property, not a per-inode one. Having this flag at the superblock level also allows us to skip having to iterate every dirty inode in wait_sb_inodes() only to skip each inode individually. Prior to this commit, mappings with no data integrity guarantees skipped waiting on writeback completion but still waited on the flusher threads to finish initiating the writeback. Waiting on the flusher threads is unnecessary. This commit kicks off writeback but does not wait on the flusher threads. This change properly addresses a recent report [1] for a suspend-to-RAM hang seen on fuse-overlayfs that was caused by waiting on the flusher threads to finish: Workqueue: pm_fs_sync pm_fs_sync_work_fn Call Trace: <TASK> __schedule+0x457/0x1720 schedule+0x27/0xd0 wb_wait_for_completion+0x97/0xe0 sync_inodes_sb+0xf8/0x2e0 __iterate_supers+0xdc/0x160 ksys_sync+0x43/0xb0 pm_fs_sync_work_fn+0x17/0xa0 process_one_work+0x193/0x350 worker_thread+0x1a1/0x310 kthread+0xfc/0x240 ret_from_fork+0x243/0x280 ret_from_fork_asm+0x1a/0x30 </TASK> On fuse this is problematic because there are paths that may cause the flusher thread to block (eg if systemd freezes the user session cgroups first, which freezes the fuse daemon, before invoking the kernel suspend. The kernel suspend triggers ->write_node() which on fuse issues a	N/A	More Details

	synchronous setattr request, which cannot be processed since the daemon is frozen. Or if the daemon is buggy and cannot properly complete writeback, initiating writeback on a dirty folio already under writeback leads to writeback_get_folio() -> folio_prepare_writeback() -> unconditional wait on writeback to finish, which will cause a hang). This commit restores fuse to its prior behavior before tmp folios were removed, where sync was essentially a no-op. [1] https://lore.kernel.org/linux-fsdevel/CAJnrk1a-asuvfrbKXbEwwDSctvemF+6zfhdnuzO65Pt8HsFSRw@mail.gmail.com/T/#m632c4648e9cafc4239299887109ebd880ac6c5c1		
CVE-2026-31466	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: fix folio isn't locked in softleaf_to_folio() On arm64 server, we found folio that get from migration entry isn't locked in softleaf_to_folio(). This issue triggers when mTHP splitting and zap_nonpresent_ptes() races, and the root cause is lack of memory barrier in softleaf_to_folio(). The race is as follows: CPU0 CPU1 deferred_split_scan() zap_nonpresent_ptes() lock folio split_folio() unmap_folio() change ptes to migration entries __split_folio_to_order() softleaf_to_folio() set flags(including PG_locked) for tail pages folio = pfn_folio(softleaf_to_pfn(entry)) smp_wmb() VM_WARN_ON_ONCE(!folio_test_locked(folio)) prep_compound_page() for tail pages In __split_folio_to_order(), smp_wmb() guarantees page flags of tail pages are visible before the tail page becomes non-compound. smp_wmb() should be paired with smp_rmb() in softleaf_to_folio(), which is missed. As a result, if zap_nonpresent_ptes() accesses migration entry that stores tail pfn, softleaf_to_folio() may see the updated compound_head of tail page before page->flags. This issue will trigger VM_WARN_ON_ONCE() in pfn_swap_entry_folio() because of the race between folio split and zap_nonpresent_ptes() leading to a folio incorrectly undergoing modification without a folio lock being held. This is a BUG_ON() before commit 93976a20345b ("mm: eliminate further swapops predicates"), which in merged in v6.19-rc1. To fix it, add missing smp_rmb() if the softleaf entry is migration entry in softleaf_to_folio() and softleaf_to_page(). [tujinjiang@huawei.com: update function name and comments]	N/A	More Details
CVE-2026-5749	Inadequate access control in the registration process in Fullstep V5, which could allow unauthenticated users to obtain a valid JWT token with which to interact with authenticated API resources. Successful exploitation of this vulnerability could allow an unauthenticated attacker to compromise the confidentiality of the affected resource, provided they have a valid token with which to interact with the API.	N/A	More Details
CVE-2026-5750	An insecure direct object reference (IDOR) vulnerability in the Fullstep V5 registration process allows authenticated users to access data belonging to other registered users through various vulnerable authenticated resources in the application. The vulnerable endpoints result from: '/api/suppliers/v1/suppliers//false' to list user information; and '/#/supplier-registration/supplier-registration//2' to update your user information (personal details, documents, etc.).	N/A	More Details
CVE-2026-35382	Rejected reason: Voluntarily withdrawn	N/A	More Details
CVE-2026-3673	An authenticated attacker can store a crafted tag value in _user_tags and trigger JavaScript execution when a victim opens the list/report view where tags are rendered. The vulnerable renderer interpolates tag content into HTML attributes and element content without escaping. This issue affects Frappe: 16.10.10.	N/A	More Details
CVE-2026-6019	http.cookies.Morsel.js_output() returns an inline <script> snippet and only escapes " for JavaScript string context. It does not neutralize the HTML parser-sensitive sequence </script> inside the generated script element. Mitigation base64-encodes the cookie value to disallow escaping using cookie value.	N/A	More Details
CVE-2026-41134	Kiota is an OpenAPI based HTTP Client code generator. Versions prior to 1.31.1 are affected by a code-generation literal injection vulnerability in multiple writer sinks (for example: serialization/deserialization keys, path/query parameter mappings, URL template metadata, enum/property metadata, and default value emission). When malicious values from an OpenAPI description are emitted into generated source without context-appropriate escaping, an attacker can break out of string literals and inject additional code into generated clients. This issue is only practically exploitable when the OpenAPI description used for generation is from an untrusted source, or a normally trusted OpenAPI description has been compromised/tampered with. Only generating from trusted, integrity-protected API descriptions significantly reduces the risk. To remediate the issue, upgrade Kiota to 1.31.1 or later and regenerate/refresh existing generated clients as a precaution. Refreshing generated clients ensures previously generated vulnerable code is replaced with hardened output.	N/A	More Details
CVE-2026-31452	In the Linux kernel, the following vulnerability has been resolved: ext4: convert inline data to extents when truncate exceeds inline size Add a check in ext4_setattr() to convert files from inline data storage to extent-based storage when truncate() grows the file size beyond the inline capacity. This prevents the filesystem from entering an inconsistent state where the inline data flag is set but the file size exceeds what can be stored inline. Without this fix, the following sequence causes a kernel BUG_ON(): 1. Mount filesystem with inode that has inline flag set and small size 2. truncate(file, 50MB) - grows size but inline flag remains set 3. sendfile() attempts to write data 4. ext4_write_inline_data() hits BUG_ON(write_size > inline_capacity) The crash occurs because ext4_write_inline_data() expects inline storage to accommodate the write, but the actual inline capacity (~60 bytes for i_block + ~96 bytes for xattrs) is far smaller than the file size and write request. The fix checks if the new size from setattr exceeds the inode's actual inline capacity (EXT4_I(inode)->i_inline_size) and converts the file to extent-based storage before proceeding with the size change. This addresses the root cause by ensuring the inline data flag and file size remain consistent during truncate operations.	N/A	More Details
CVE-2026-41170	Squidex is an open source headless content management system and content management hub. Prior to version 7.23.0, the `RestoreController.PostRestoreJob` endpoint allows an administrator to supply an arbitrary URL for downloading backup archives. This URL is fetched using the "Backup" `HttpClient` without any SSRF protection. A malicious or compromised admin can use this endpoint to probe internal network services, access cloud metadata endpoints, or perform internal reconnaissance. The vulnerability is authenticated (Admin-only) but highly impactful, allowing potential access to sensitive internal resources. Version 7.23.0 contains a fix.	N/A	More Details
CVE-2026-41171	Squidex is an open source headless content management system and content management hub. Versions prior to 7.23.0 have a Server-Side Request Forgery (SSRF) vulnerability due to missing SSRF protection on the `Jint` HTTP client used by scripting engine functions (`getJSON`, `request`, etc.). An authenticated user with low privileges (e.g., schema editing permissions) can force the server to make arbitrary outbound HTTP requests to attacker-controlled or internal endpoints. This allows access to internal services and cloud metadata endpoints (e.g., IMDS), potentially leading to credential exposure and lateral movement. Version 7.23.0 contains a fix.	N/A	More Details

CVE-2026-41172	Squidex is an open source headless content management system and content management hub. Prior to version 7.23.0, an SSRF vulnerability allows a user with asset upload permission to force the server to fetch arbitrary URLs, including localhost/private network targets, and persist the response as an asset. Version 7.23.0 contains a fix.	N/A	More Details
CVE-2026-4049	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-32679	The installers of LiveOn Meet Client for Windows (Downloader5Installer.exe and Downloader5InstallerForAdmin.exe) and the installers of Canon Network Camera Plugin (CanonNWCamPlugin.exe and CanonNWCamPluginForAdmin.exe) insecurely load Dynamic Link Libraries (DLLs). If a malicious DLL is placed at the same directory, the affected installer may load that DLL and execute its code with the privilege of the user invoking the installer.	N/A	More Details
CVE-2026-40062	A path Traversal vulnerability exists in Ziostation2 v2.9.8.7 and earlier. A remote unauthenticated attacker may get sensitive information on the operating system.	N/A	More Details
CVE-2026-41196	Luanti (formerly Minetest) is an open source voxel game-creation platform. Starting in version 5.0.0 and prior to version 5.15.2, a malicious mod can trivially escape the sandboxed Lua environment to execute arbitrary code and gain full filesystem access on the user's device. This applies to the server-side mod, async and mapgen as well as the client-side (CSM) environments. This vulnerability is only exploitable when using LuaJIT. Version 5.15.2 contains a patch. On release versions, one can also patch this issue without recompiling by editing `builtin/init.lua` and adding the line `getfenv = nil` at the end. Note that this will break mods relying on this function (which is not inherently unsafe).	N/A	More Details
CVE-2026-41197	Noir is a Domain Specific Language for SNARK proving systems that is designed to use any ACIR compatible proving system, and Brillig is the bytecode ACIR uses for non-determinism. Noir programs can invoke external functions through foreign calls. When compiling to Brillig bytecode, the SSA instructions are processed block-by-block in `BrilligBlock::compile_block()`. When the compiler encounters an `Instruction::Call` with a `Value::ForeignFunction` target, it invokes `codegen_call()` in `brillig_call/code_gen_call.rs`, which dispatches to `convert_ssa_foreign_call()`. Before emitting the foreign call opcode, the compiler must pre-allocate memory for any array results the call will return. This happens through `allocate_external_call_results()`, which iterates over the result types. For `Type::Array` results, it delegates to `allocate_foreign_call_result_array()` to recursively allocate memory on the heap for nested arrays. The `BrilligArray` struct is the internal representation of a Noir array in Brillig IR. Its `size` field represents the semi-flattened size, the total number of memory slots the array occupies, accounting for the fact that composite types like tuples consume multiple slots per element. This size is computed by `compute_array_length()` in `brillig_block_variables.rs`. For the outer array, `allocate_external_call_results()` correctly uses `define_variable()`, which internally calls `allocate_value_with_type()`. This function applies the formula above, producing the correct semi-flattened size. However, for nested arrays, `allocate_foreign_call_result_array()` contains a bug. The pattern `Type::Array(_, nested_size)` discards the inner types with `_` and uses only `nested_size`, the semantic length of the nested array (the number of logical elements), not the semi-flattened size. For simple element types this works correctly, but for composite element types it under-allocates. Foreign calls returning nested arrays of tuples or other composite types corrupt the Brillig VM heap. Version 1.0.0-beta.19 fixes this issue.	N/A	More Details
CVE-2026-41200	STIG Manager is an API and web client for managing Security Technical Implementation Guides (STIG) assessments of Information Systems. Versions 1.5.10 through 1.6.7 have a reflected Cross-Site Scripting (XSS) vulnerability in the OIDC authentication error handling code in `src/init.js` and `public/reauth.html`. During the OIDC redirect flow, the `error` and `error_description` query parameters returned by the OIDC provider are written directly to the DOM via `innerHTML` without HTML escaping. An attacker who can craft a malicious redirect URL and convince a user to follow it can execute arbitrary JavaScript in the application's origin context. The vulnerability is most severe when the targeted user has an active STIG Manager session running in another browser tab — injected code executes in the same origin and can communicate with the SharedWorker managing the active access token, enabling authenticated API requests on behalf of the victim including reading and modifying collection data. The vulnerability is patched in version 1.6.8. There is no workaround short of upgrading. Deployments behind a web application firewall that filters reflected XSS payloads in query parameters may have partial mitigation, but this is not a substitute for patching.	N/A	More Details
CVE-2026-41206	PySpector is a static analysis security testing (SAST) Framework engineered for modern Python development workflows. The plugin security validator in PySpector uses AST-based static analysis to prevent dangerous code from being loaded as plugins. Prior to version 0.1.8, the blocklist implemented in `PluginSecurity.validate_plugin_code` is incomplete and can be bypassed using several Python constructs that are not checked. An attacker who can supply a plugin file can achieve arbitrary code execution within the PySpector process when that plugin is installed and executed. Version 0.1.8 fixes the issue.	N/A	More Details
CVE-2026-41211	Vite+ is a unified toolchain and entry point for web development. Prior to version 0.1.17, `downloadPackageManager()` accepts an untrusted `version` string and uses it directly in filesystem paths. A caller can supply `../` segments or an absolute path to escape the `VP_HOME/package_manager/<pm>/` cache root and make Vite+ delete, replace, and populate directories outside the intended cache location. Version 0.1.17 contains a patch.	N/A	More Details
CVE-2026-41243	OpenLearn is open-source educational forum software. Prior to commit 844b2a40a69d0c4911580fe501923f0b391313ab, when `safeMode` is enabled, unapproved forum posts are hidden from the public list, but the direct post-read procedure still returns the full post to anyone with the post UUID. Commit 844b2a40a69d0c4911580fe501923f0b391313ab fixes the issue.	N/A	More Details
CVE-2026-40529	CMS ALAYA provided by KANATA Limited contains an SQL injection vulnerability. Information stored in the database may be obtained or altered by an attacker with access to the administrative interface.	N/A	More Details
CVE-2026-	IP Setting Software contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with administrative privileges.	N/A	More Details

34488			
CVE-2026-31455	In the Linux kernel, the following vulnerability has been resolved: xfs: stop reclaim before pushing AIL during unmount The unmount sequence in xfs_unmount_flush_inodes() pushed the AIL while background reclaim and inodegc are still running. This is broken independently of any use-after-free issues - background reclaim and inodegc should not be running while the AIL is being pushed during unmount, as inodegc can dirty and insert inodes into the AIL during the flush, and background reclaim can race to abort and free dirty inodes. Reorder xfs_unmount_flush_inodes() to stop inodegc and cancel background reclaim before pushing the AIL. Stop inodegc before cancelling m_reclaim_work because the inodegc worker can re-queue m_reclaim_work via xfs_inodegc_set_reclaimable.	N/A	More Details
CVE-2026-31451	In the Linux kernel, the following vulnerability has been resolved: ext4: replace BUG_ON with proper error handling in ext4_read_inline_folio Replace BUG_ON() with proper error handling when inline data size exceeds PAGE_SIZE. This prevents kernel panic and allows the system to continue running while properly reporting the filesystem corruption. The error is logged via ext4_error_inode(), the buffer head is released to prevent memory leak, and -EFSCORRUPTED is returned to indicate filesystem corruption.	N/A	More Details
CVE-2026-40551	mpGabinet performs client-side authentication. An attacker with access to any application instance connected to the backend server can bypass the login verification process by manipulating the application binary and authenticate as an arbitrary user. This issue affects mpGabinet version 23.12.19 and below.	N/A	More Details
CVE-2010-20117	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2026-41128	Craft CMS is a content management system (CMS). In versions 5.6.0 through 5.9.14, the `actionSavePermissions()` endpoint allows a user with only `viewUsers` permission to remove arbitrary users from all user groups. While `_saveUserGroups()` enforces per-group authorization for additions, it performs no equivalent authorization check for removals, so submitting an empty `groups` value removes all existing group memberships. Version 5.9.15 contains a patch.	N/A	More Details
CVE-2026-41129	Craft CMS is a content management system (CMS). Versions on the 4.x branch through 4.17.8 and the 5.x branch through 5.9.14 are vulnerable to Server-Side Request Forgery. The exploitation requires a few permissions to be enabled in the used GraphQL schema: "Edit assets in the <VolumeName> volume" and "Create assets in the <VolumeName> volume." Versions 4.17.9 and 5.9.15 patch the issue.	N/A	More Details
CVE-2026-41130	Craft CMS is a content management system (CMS). In versions on the 4.x branch through 4.17.8 and the 5.x branch through 5.9.14, the `resource-js` endpoint in Craft CMS allows unauthenticated requests to proxy remote JavaScript resources. When `trustedHosts` is not explicitly restricted (default configuration), the application trusts the client-supplied Host header. This allows an attacker to control the derived `baseUrl`, which is used in prefix validation inside `actionResourceJs()`. By supplying a malicious Host header, the attacker can make the server issue arbitrary HTTP requests, leading to Server-Side Request Forgery (SSRF). Versions 4.17.9 and 5.9.15 patch the issue.	N/A	More Details
CVE-2026-41146	facil.io is a C micro-framework for web applications. Prior to commit 5128747363055201d3ecf0e29bf0a961703c9fa0, `fio_json_parse` can enter an infinite loop when it encounters a nested JSON value starting with `i` or `I`. The process spins in user space and pegs one CPU core at ~100% instead of returning a parse error. Because `iodine` vendors the same parser code, the issue also affects `iodine` when it parses attacker-controlled JSON. The smallest reproducer I found is `[i`. The quoted-value form that originally exposed the issue, `[""i`, reaches the same bug because the parser tolerates missing commas and then treats the trailing `i` as the start of another value. Commit 5128747363055201d3ecf0e29bf0a961703c9fa0 fixes the issue.	N/A	More Details
CVE-2026-41457	OwnTone Server versions 28.4 through 29.0 contain a SQL injection vulnerability in DAAP query and filter handling that allows attackers to inject arbitrary SQL expressions by supplying malicious values through the query= and filter= parameters for integer-mapped DAAP fields. Attackers can exploit insufficient sanitization of these parameters to bypass filters and gain unauthorized access to media library data.	N/A	More Details
CVE-2026-41458	OwnTone Server versions 28.4 through 29.0 contain a race condition vulnerability in the DAAP login handler that allows unauthenticated attackers to crash the server by exploiting unsynchronized access to the global DAAP session list. Attackers can flood the DAAP /login endpoint with concurrent requests to trigger a remote denial of service condition without requiring authentication.	N/A	More Details
CVE-2026-40451	DeepL Chrome browser extension versions from v1.22.0 to v.1.23.0 contain a cross-site scripting vulnerability, which allows an attacker to execute arbitrary script in a user's browser, and inject malicious HTML into web pages viewed by the user.	N/A	More Details
CVE-2000-5001	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2005-20001	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2008-20002	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2008-20003	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details

CVE-2009-20012	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2010-20110	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2010-20116	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2010-20118	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2026-31445	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: avoid use of half-online-committed context One major usage of damon_call() is online DAMON parameters update. It is done by calling damon_commit_ctx() inside the damon_call() callback function. damon_commit_ctx() can fail for two reasons: 1) invalid parameters and 2) internal memory allocation failures. In case of failures, the damon_ctx that attempted to be updated (commit destination) can be partially updated (or, corrupted from a perspective), and therefore shouldn't be used anymore. The function only ensures the damon_ctx object can safely deallocated using damon_destroy_ctx(). The API callers are, however, calling damon_commit_ctx() only after asserting the parameters are valid, to avoid damon_commit_ctx() fails due to invalid input parameters. But it can still theoretically fail if the internal memory allocation fails. In the case, DAMON may run with the partially updated damon_ctx. This can result in unexpected behaviors including even NULL pointer dereference in case of damos_commit_dests() failure [1]. Such allocation failure is arguably too small to fail, so the real world impact would be rare. But, given the bad consequence, this needs to be fixed. Avoid such partially-committed (maybe-corrupted) damon_ctx use by saving the damon_commit_ctx() failure on the damon_ctx object. For this, introduce damon_ctx->maybe_corrupted field. damon_commit_ctx() sets it when it is failed. kdamond_call() checks if the field is set after each damon_call_control->fn() is executed. If it is set, ignore remaining callback requests and return. All kdamond_call() callers including kdamond_fn() also check the maybe_corrupted field right after kdamond_call() invocations. If the field is set, break the kdamond_fn() main loop so that DAMON sill doesn't use the context that might be corrupted. [sj@kernel.org: let kdamond_call() with cancel regardless of maybe_corrupted]	N/A	More Details
CVE-2010-20124	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2011-10031	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2013-10041	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2013-10045	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2013-10056	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2014-125120	Rejected reason: This CVE has the been REJECTED and will not be published by the CNA.	N/A	More Details
CVE-2026-0539	Incorrect Default Permissions in pcvisit service binary on Windows allows a low-privileged local attacker to escalate their privileges by overwriting the service binary with arbitrary contents. This service binary is automatically launched with NT\SYSTEM privileges on boot. This issue affects all versions after 22.6.22.1329 and was fixed in 25.12.3.1745.	N/A	More Details
CVE-2026-31434	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix leak of kobject name for sub-group space_info When create_space_info_sub_group() allocates elements of space_info->sub_group[], kobject_init_and_add() is called for each element via btrfs_sysfs_add_space_info_type(). However, when check_removing_space_info() frees these elements, it does not call btrfs_sysfs_remove_space_info() on them. As a result, kobject_put() is not called and the associated kobj->name objects are leaked. This memory leak is reproduced by running the blktests test case zbd/009 on kernels built with CONFIG_DEBUG_KMEMLEAK. The kmemleak feature reports the following error: unreferenced object 0xffff888112877d40 (size 16): comm "mount", pid 1244, jiffies 4294996972 hex dump (first 16 bytes): 64 61 74 61 2d 72 65 6c 6f 63 00 c4 c6 a7 cb 7f data-reloc..... backtrace (crc 53ffde4d): __kmalloc_node_track_caller_noprof+0x619/0x870 kstrdup+0x42/0xc0 kobject_set_name_vargs+0x44/0x110 kobject_init_and_add+0xcf/0x150 btrfs_sysfs_add_space_info_type+0xfc/0x210 [btrfs] create_space_info_sub_group.constprop.0+0xfb/0x1b0 [btrfs] create_space_info+0x211/0x320 [btrfs] btrfs_init_space_info+0x15a/0x1b0 [btrfs] open_ctree+0x33c7/0x4a50 [btrfs] btrfs_get_tree.cold+0x9f/0x1ee [btrfs] vfs_get_tree+0x87/0x2f0 vfs_cmd_create+0xbd/0x280 __do_sys_fsconfig+0x3df/0x990 do_syscall_64+0x136/0x1540 entry_SYSCALL_64_after_hwframe+0x76/0x7e To avoid the leak, call btrfs_sysfs_remove_space_info() instead of kfree() for the elements.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix NULL pointer dereference in netfs_unbuffered_write() on retry When a write subrequest is marked NETFS_SREQ_NEED_RETRY, the retry path in		

CVE-2026-31437	netfs_unbuffered_write() unconditionally calls stream->prepare_write() without checking if it is NULL. Filesystems such as 9P do not set the prepare_write operation, so stream->prepare_write remains NULL. When get_user_pages() fails with -EFAULT and the subrequest is flagged for retry, this results in a NULL pointer dereference at fs/netfs/direct_write.c:189. Fix this by mirroring the pattern already used in write_retry.c: if stream->prepare_write is NULL, skip renegotiation and directly reissue the subrequest via netfs_reissue_write(), which handles iterator reset, IN_PROGRESS flag, stats update and reissue internally.	N/A	More Details
CVE-2026-31438	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix kernel BUG in netfs_limit_iter() for ITER_KVEC iterators When a process crashes and the kernel writes a core dump to a 9P filesystem, __kernel_write() creates an ITER_KVEC iterator. This iterator reaches netfs_limit_iter() via netfs_unbuffered_write(), which only handles ITER_FOLIOQ, ITER_BVEC and ITER_XARRAY iterator types, hitting the BUG() for any other type. Fix this by adding netfs_limit_kvec() following the same pattern as netfs_limit_bvec(), since both kvec and bvec are simple segment arrays with pointer and length fields. Dispatch it from netfs_limit_iter() when the iterator type is ITER_KVEC.	N/A	More Details
CVE-2026-31439	In the Linux kernel, the following vulnerability has been resolved: dmaengine: xilinx: xdma: Fix regmap init error handling devm_regmap_init_mmio returns an ERR_PTR() upon error, not NULL. Fix the error check and also fix the error message. Use the error code from ERR_PTR() instead of the wrong value in ret.	N/A	More Details
CVE-2026-31440	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix leaking event log memory During the device remove process, the device is reset, causing the configuration registers to go back to their default state, which is zero. As the driver is checking if the event log support was enabled before deallocating, it will fail if a reset happened before. Do not check if the support was enabled, the check for 'idxd->evl' being valid (only allocated if the HW capability is available) is enough.	N/A	More Details
CVE-2026-31441	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix memory leak when a wq is reset idxd_wq_disable_cleanup() which is called from the reset path for a workqueue, sets the wq type to NONE, which for other parts of the driver mean that the wq is empty (all its resources were released). Only set the wq type to NONE after its resources are released.	N/A	More Details
CVE-2026-31443	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix crash when the event log is disabled If reporting errors to the event log is not supported by the hardware, and an error that causes Function Level Reset (FLR) is received, the driver will try to restore the event log even if it was not allocated. Also, only try to free the event log if it was properly allocated.	N/A	More Details
CVE-2026-41040	GROWI provided by GROWI, Inc. is vulnerable to a regular expression denial of service (ReDoS) via a crafted input string.	N/A	More Details
CVE-2026-3259	A Generation of Error Message Containing Sensitive Information vulnerability in the Materialized View Refresh mechanism in Google BigQuery on Google Cloud Platform allows an authenticated user to potentially disclose sensitive data using a crafted materialized view that triggers a runtime error during the refresh process. This vulnerability was patched on 29 January 2026, and no customer action is needed.	N/A	More Details
CVE-2026-3960	A critical remote code execution vulnerability exists in the unauthenticated REST API endpoint /99/ImportSQLTable in H2O-3 version 3.46.0.9 and prior. The vulnerability arises due to insufficient security controls in the parameter blacklist mechanism, which only targets MySQL JDBC driver-specific dangerous parameters. An attacker can bypass these controls by switching the JDBC URL protocol to jdbc:postgresql: and exploiting PostgreSQL JDBC driver-specific parameters such as socketFactory and socketFactoryArg. This allows unauthenticated attackers to execute arbitrary code on the H2O-3 server with the privileges of the H2O-3 process. The issue is resolved in version 3.46.0.10.	N/A	More Details
CVE-2026-31686	In the Linux kernel, the following vulnerability has been resolved: mm/kasan: fix double free for kasan pXds kasan_free_pxd() assumes the page table is always struct page aligned. But that's not always the case for all architectures. E.g. In case of powerpc with 64K pagesize, PUD table (of size 4096) comes from slab cache named pgtable-2^9. Hence instead of page_to_virt(pxd_page()) let's just directly pass the start of the pxd table which is passed as the 1st argument. This fixes the below double free kasan issue seen with PMEM: radix-mmu: Mapped 0x0000047d10000000-0x0000047f90000000 with 2.00 MiB pages == BUG: KASAN: double-free in kasan_remove_zero_shadow+0x9c4/0xa20 Free of addr c0000003c38e0000 by task ndctl/2164 CPU: 34 UID: 0 PID: 2164 Comm: ndctl Not tainted 6.19.0-rc1-00048-gea1013c15392 #157 VOLUNTARY Hardware name: IBM,9080-HEX POWER10 (architected) 0x800200 0xf000006 of:IBM,FW1060.00 (NH1060_012) hv:phyp pSeries Call Trace: dump_stack_lvl+0x88/0xc4 (unreliable) print_report+0x214/0x63c kasan_report_invalid_free+0xe4/0x110 check_slab_allocation+0x100/0x150 kmem_cache_free+0x128/0x6e0 kasan_remove_zero_shadow+0x9c4/0xa20 memunmap_pages+0x2b8/0x5c0 devm_action_release+0x54/0x70 release_nodes+0xc8/0x1a0 devres_release_all+0xe0/0x140 device_unbind_cleanup+0x30/0x120 device_release_driver_internal+0x3e4/0x450 unbind_store+0xfc/0x110 drv_attr_store+0x78/0xb0 sysfs_kf_write+0x114/0x140 kernfs_fop_write_iter+0x264/0x3f0 vfs_write+0x3bc/0x7d0 ksys_write+0xa4/0x190 system_call_exception+0x190/0x480 system_call_vectored_common+0x15c/0x2ec ---- interrupt: 3000 at 0x7fff93b3d3f4 NIP: 00007fff93b3d3f4 LR: 00007fff93b3d3f4 CTR: 0000000000000000 REGS: c0000003f1b07e80 TRAP: 3000 Not tainted (6.19.0-rc1-00048-gea1013c15392) MSR: 800000000280f033 <SF,VEC,VSX,EE,PR,FP,ME,IR,DR,RI,LE> CR: 48888208 XER: 00000000 <...> NIP [00007fff93b3d3f4] 0x7fff93b3d3f4 LR [00007fff93b3d3f4] 0x7fff93b3d3f4 ---- interrupt: 3000 The buggy address belongs to the object at c0000003c38e0000 which belongs to the cache pgtable-2^9 of size 4096 The buggy address is located 0 bytes inside of 4096-byte region [c0000003c38e0000, c0000003c38e1000) The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x3c38c head: order:2 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0 memcg:c0000003bfd63e01 flags: 0x63ffff800000040(head|node=6|zone=0|lastcpupid=0x7ffff) page_type: f5(slab) raw: 063ffff800000040 c000000140058980 5deadbeef0000122 0000000000000000 raw: 0000000000000000 0000000080200020 00000000f5000000 c0000003bfd63e01 head: 063ffff800000040 c000000140058980 5deadbeef0000122 0000000000000000 head: 0000000000000000 0000000080200020 00000000f5000000 c0000003bfd63e01 head:	N/A	More Details

	063ffff800000002 c00c000000f0e301 00000000ffffffff 00000000ffffffff head: ffffffffffffffff 0000000000000000 00000000ffffffff 0000000000000004 page dumped because: kasan: bad access detected [138.953636] [T2164] Memory state around the buggy address: [138.953643] [T2164] c0000003c38dff00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [138.953652] [T2164] c0000003c38dff80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [138.953661] [T2164] >c0000003c38e0000: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [138.953669] [T2164] ^ [138.953675] [T2164] c0000003c38e0080: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [138.953684] [T2164] c0000003c38e0100: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [138.953692] [T2164] == [138.953701] [T2164] Disabling lock debugging due to kernel taint		
CVE-2026-31684	In the Linux kernel, the following vulnerability has been resolved: net: sched: act_csum: validate nested VLAN headers tcf_csum_act() walks nested VLAN headers directly from skb->data when an skb still carries in-payload VLAN tags. The current code reads vlan->h_vlan_encapsulated_proto and then pulls VLAN_HLEN bytes without first ensuring that the full VLAN header is present in the linear area. If only part of an inner VLAN header is linearized, accessing h_vlan_encapsulated_proto reads past the linear area, and the following skb_pull(VLAN_HLEN) may violate skb invariants. Fix this by requiring pskb_may_pull(skb, VLAN_HLEN) before accessing and pulling each nested VLAN header. If the header still is not fully available, drop the packet through the existing error path.	N/A	More Details
CVE-2026-33277	An OS command Injection issue exists in LogonTracer prior to v2.0.0. An arbitrary OS command may be executed by a logged-in user.	N/A	More Details
CVE-2026-33566	There is a cypher injection issue in LogonTracer prior to v2.0.0. If specially crafted Windows event log data is loaded, the contents of the database may be altered.	N/A	More Details
CVE-2026-3867	An improper ownership management vulnerability has been identified in Moxa’s Secure Router. Because of improper ownership management, a low-privileged authenticated user may access a configuration file containing the hashed password of the administrative account. Successful exploitation of this vulnerability could allow an attacker to obtain sensitive information. Exploitation is only possible under a specific condition — when the configuration file has been exported. This vulnerability does not impact the integrity or availability of the affected product, and no confidentiality, integrity, or availability impact to the subsequent system has been identified.	N/A	More Details
CVE-2026-3868	An improper handling of the length parameter inconsistency vulnerability has been identified in Moxa’s Secure Router. Because of improper validation of length parameters in the HTTPS management interface, an unauthenticated remote attacker could send specially crafted requests that trigger a buffer overflow condition, causing the web service to become unresponsive. Successful exploitation may result in a denial-of-service condition requiring a device reboot to restore normal operation. While successful exploitation can severely impact the availability of the affected device, no impact to the confidentiality or integrity of the affected product has been identified. Additionally, no confidentiality, integrity, or availability impact to the subsequent system has been identified.	N/A	More Details
CVE-2026-22077	OPPO Wallet APP contains a trusted domain validation flaw that allows attackers to bypass protected interface access restrictions, which may lead to account token hijacking and sensitive information disclosure.	N/A	More Details
CVE-2025-15626	Authenticated user can bypass authorization in Ribblr - Crochet & Knitting iOS application	N/A	More Details
CVE-2026-32688	Allocation of Resources Without Limits or Throttling vulnerability in elixir-plug plug_cowboy allows unauthenticated remote denial of service via atom table exhaustion. Plug.Cowboy.Conn.conn/1 in lib/plug/cowboy/conn.ex calls String.to_atom/1 on the value returned by :cowboy_req.scheme/1. For HTTP/2 connections, cowlib passes the client-supplied :scheme pseudo-header value through verbatim without validation. Each unique value permanently allocates a new entry in the BEAM atom table. Since atoms are never garbage-collected and the atom table has a fixed limit (default 1,048,576), an unauthenticated attacker can exhaust the table by sending HTTP/2 requests with unique :scheme values, causing the Erlang VM to abort with system_limit and taking down the entire node. This vulnerability does not affect HTTP/1.1, where cowboy derives the scheme from the listener type rather than from a client-supplied header. This issue affects plug_cowboy: from 2.0.0 before 2.8.1.	N/A	More Details
CVE-2026-40557	Improper Certificate Validation via Global SSL Context Downgrade in Apache Storm Prometheus Reporter Versions Affected: from 2.6.3 to 2.8.6 Description: In production deployments where an administrator enables storm.daemon.metrics.reporter.plugin.prometheus.skip_tls_validation (by default it is disabled) intending to affect only the Prometheus reporter, the undocumented global side effect creates an attack surface across every TLS-protected communication channel in the Storm daemon. The PrometheusPreparableReporter class implements an INSECURE_TRUST_MANAGER that accepts all SSL certificates without validation, with empty checkClientTrusted and checkServerTrusted methods. Most critically, when the storm.daemon.metrics.reporter.plugin.prometheus.skip_tls_validation configuration option is enabled (default = disabled) for HTTPS Prometheus PushGateway connections, the INSECURE_CONNECTION_FACTORY calls SSLContext.setDefault(sslContext), which globally replaces the JVM's default SSL context rather than applying the insecure context only to the Prometheus connection. This payload flows through storm.yaml configuration → PrometheusPreparableReporter.prepare() → INSECURE_CONNECTION_FACTORY → SSLContext.setDefault(), resulting in a JVM-wide TLS security downgrade. All subsequent HTTPS connections in the process - including ZooKeeper, Thrift, Netty, and UI connections - silently trust all certificates, including self-signed, expired, and attacker-generated ones, enabling man-in-the-middle interception of cluster state, topology submissions, tuple data, and administrative credentials. Mitigation: 2.x users should upgrade to 2.8.7 if the Prometheus Metrics Reporter is used. Prometheus Metrics Reporter Users who cannot upgrade immediately should remove the storm.daemon.metrics.reporter.plugin.prometheus.skip_tls_validation: true setting from their storm.yaml configuration and instead configure a proper truststore containing the PushGateway's certificate.	N/A	More Details

CVE-2026-6265	Insecure preserved inherited permissions vulnerability in Cerberus FTP Server on Windows allows Privilege Escalation.This issue has been resolved in Cerberus FTP Server: 2026.1	N/A	More Details
CVE-2026-6337	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-6357	pip prior to version 26.1 would run self-update check functionality after installing wheel files which required importing well-known Python modules names. These module imports were intentionally deferred to increase startup time of the pip CLI. The patch changes self-update functionality to run before wheels are installed to prevent newly-installed modules from being imported shortly after the installation of a wheel package. Users should still review package contents prior to installation.	N/A	More Details
CVE-2025-54505	A transient execution vulnerability within AMD CPUs may allow a local user-privileged attacker to leak data via the floating point divisor unit, potentially resulting in loss of confidentiality.	N/A	More Details
CVE-2026-6970	authd prior to version 0.6.4 contains a logic error in primary group ID assignment that can lead to local privilege escalation. When a user's primary group ID (GID) differs from their UID, either because the account was created with authd prior to version 0.5.4 or because the primary group was manually changed via the `authctl group set-gid` command, and the user's identity provider record is updated, authd incorrectly resets the user's primary group ID to their UID upon next login. This causes newly created files and directories to be owned by the wrong group, causing denial of service issues, and potentially granting unintended access to other local users and allowing local privilege escalation.	N/A	More Details
CVE-2026-31687	In the Linux kernel, the following vulnerability has been resolved: gpio: omap: do not register driver in probe() Commit 11a78b794496 ("ARM: OMAP: MPUIO wake updates") registers the omap_mpuio_driver from omap_mpuio_init(), which is called from omap_gpio_probe(). However, it neither makes sense to register drivers from probe() callbacks of other drivers, nor does the driver core allow registering drivers with a device lock already being held. The latter was revealed by commit dc23806a7c47 ("driver core: enforce device_lock for driver_match_device()") leading to a potential deadlock condition described in [1]. Additionally, the omap_mpuio_driver is never unregistered from the driver core, even if the module is unloaded. Hence, register the omap_mpuio_driver from the module initcall and unregister it in module_exit().	N/A	More Details
CVE-2026-35225	An unauthenticated remote attacker is able to exhaust all available TCP connections in the CODESYS EtherNet/IP adapter stack, preventing legitimate clients from establishing new connections.	N/A	More Details
CVE-2026-31688	In the Linux kernel, the following vulnerability has been resolved: driver core: enforce device_lock for driver_match_device() Currently, driver_match_device() is called from three sites. One site (__device_attach_driver) holds device_lock(dev), but the other two (bind_store and __driver_attach) do not. This inconsistency means that bus match() callbacks are not guaranteed to be called with the lock held. Fix this by introducing driver_match_device_locked(), which guarantees holding the device lock using a scoped guard. Replace the unlocked calls in bind_store() and __driver_attach() with this new helper. Also add a lock assertion to driver_match_device() to enforce this guarantee. This consistency also fixes a known race condition. The driver_override implementation relies on the device_lock, so the missing lock led to the use-after-free (UAF) reported in Bugzilla for buses using this field. Stress testing the two newly locked paths for 24 hours with CONFIG_PROVE_LOCKING and CONFIG_LOCKDEP enabled showed no UAF recurrence and no lockdep warnings.	N/A	More Details
CVE-2026-31689	In the Linux kernel, the following vulnerability has been resolved: EDAC/mc: Fix error path ordering in edac_mc_alloc() When the mci->pvt_info allocation in edac_mc_alloc() fails, the error path will call put_device() which will end up calling the device's release function. However, the init ordering is wrong such that device_initialize() happens *after* the failed allocation and thus the device itself and the release function pointer are not initialized yet when they're called: MCE: In-kernel MCE decoding enabled. ------------[cut here]------------ kobject: '(null)': is not initialized, yet kobject_put() is being called. WARNING: lib/kobject.c:734 at kobject_put, CPU#22: systemd-udevd CPU: 22 UID: 0 PID: 538 Comm: systemd-udevd Not tainted 7.0.0-rc1+ #2 PREEMPT(full) RIP: 0010:kobject_put Call Trace: <TASK> edac_mc_alloc+0xbe/0xe0 [edac_core] amd64_edac_init+0x7a4/0xff0 [amd64_edac] ? __pfx_amd64_edac_init+0x10/0x10 [amd64_edac] do_one_initcall ... Reorder the calling sequence so that the device is initialized and thus the release function pointer is properly set before it can be used. This was found by Claude while reviewing another EDAC patch.	N/A	More Details
CVE-2026-31690	In the Linux kernel, the following vulnerability has been resolved: firmware: thead: Fix buffer overflow and use standard endian macros Addresses two issues in the TH1520 AON firmware protocol driver: 1. Fix a potential buffer overflow where the code used unsafe pointer arithmetic to access the 'mode' field through the 'resource' pointer with an offset. This was flagged by Smatch static checker as: "buffer overflow 'data' 2 <= 3" 2. Replace custom RPC_SET_BE* and RPC_GET_BE* macros with standard kernel endianness conversion macros (cpu_to_be16, etc.) for better portability and maintainability. The functionality was re-tested with the GPU power-up sequence, confirming the GPU powers up correctly and the driver probes successfully. [12.702370] powervr ffef400000.gpu: [drm] loaded firmware powervr/rogue_36.52.104.182_v1.fw [12.711043] powervr ffef400000.gpu: [drm] FW version v1.0 (build 6645434 OS) [12.719787] [drm] Initialized powervr 1.0.0 for ffef400000.gpu on minor 0	N/A	More Details
CVE-2026-31691	In the Linux kernel, the following vulnerability has been resolved: igb: remove napi_synchronize() in igb_down() When an AF_XDP zero-copy application terminates abruptly (e.g., kill -9), the XSK buffer pool is destroyed but NAPI polling continues. igb_clean_rx_irq_zc() repeatedly returns the full budget, preventing napi_complete_done() from clearing NAPI_STATE_SCHED. igb_down() calls napi_synchronize() before napi_disable() for each queue vector. napi_synchronize() spins waiting for NAPI_STATE_SCHED to clear, which never happens. igb_down() blocks indefinitely, the TX watchdog fires, and the TX queue remains permanently stalled. napi_disable() already handles this correctly: it sets NAPI_STATE_DISABLE. After a full-budget poll, __napi_poll() checks napi_disable_pending(). If set, it forces completion and clears NAPI_STATE_SCHED, breaking the loop that napi_synchronize() cannot. napi_synchronize() was added in commit 41f149a285da ("igb: Fix possible panic caused by Rx traffic arrival while interface is down"). napi_disable() provides stronger guarantees: it prevents further scheduling and waits for any active poll to exit. Other Intel drivers (ixgbe, ice, i40e) use napi_disable() without a preceding napi_synchronize() in their down paths. Remove redundant napi_synchronize() call	N/A	More Details

	and reorder napi_disable() before igb_set_queue_napi() so the queue-to-NAPI mapping is only cleared after polling has fully stopped.		
CVE-2026-5394	An authenticated administrative user who can import or save DataObject class definitions can inject attacker-controlled composite index metadata and trigger unintended SQL execution in the backend. This issue affects pimcore: 12.3.3.	N/A	More Details
CVE-2026-3087	If `shutil.unpack_archive()` is given a ZIP archive with an absolute Windows path containing a drive (`C:\\...`) then the archive will be extracted outside the target directory which is different than other operating systems. Only Windows is affected by this vulnerability.	N/A	More Details
CVE-2026-5362	An authenticated attacker with permission to edit document content can store crafted HTML/JavaScript in a Document embed editable and cause script execution when the published page is rendered. This issue affects pimcore: v12.3.3.	N/A	More Details
CVE-2024-54011	Penetration Testing engineers at Amazon have discovered a flaw where the camera system fails to properly handle data supplied in certain requests, causing a service disruption. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	N/A	More Details
CVE-2024-54012	Penetration Testing engineers at Amazon discovered a vulnerability where the camera system failed to properly validate input, allowing specially crafted requests containing malicious commands to be executed on the device. The manufacturer has released patch firmware for the flaw; please refer to the manufacturer's report for details and workarounds.	N/A	More Details
CVE-2024-54013	Penetration Testing engineers at Amazon have identified a security flaw related to request handling in the web server component that could, under certain conditions, lead to unintended access to protected functions. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds	N/A	More Details
CVE-2026-5779	An insecure direct object reference (IDOR) vulnerability in MphRx's Minerva V3.6.0, specifically in the '/minerva/user/updateUserProfile' endpoint. This allows an authenticated user to modify the information of other registered users. Successful exploitation of this vulnerability allows an authenticated user to modify other users' information, such as their email address, and request a new password via the '/webconnect/#/forgotPassword' endpoint. This could lead to complete account takeover.	N/A	More Details
CVE-2026-5780	An insecure direct object reference (IDOR) vulnerability in MphRx's Minerva V3.6.0, specifically in the endpoint '/minerva/moUser/show/'. If this vulnerability is successfully exploited, an authenticated user can access the data of other registered users simply by modifying the ID. This allows an attacker to obtain a list of users.	N/A	More Details
CVE-2026-5781	An authorization vulnerability in MphRx's Minerva V3.6.0, specifically in the '/minerva/moUser/update' endpoint, could allow an authenticated user with user modification privileges to escalate their privileges by sending an HTTP request with a manipulated 'identifier' field. Successful exploitation of this vulnerability could allow an authenticated user to obtain administrator privileges. It is not possible to escalate privileges through the graphical user interface.	N/A	More Details
CVE-2026-40550	mpGabinet is vulnerable to Privilege Escalation due to excessive database privileges assigned to the user used by the application. An attacker with access to any running application instance connected to the backend server can extract database credentials from the application’s memory by inspecting the running process. While ability to retrieve credentials from memory is expected behavior, the exposed credentials grant administrative access to the database, exceeding the privileges required for normal application functionality. This allows an attacker to perform actions beyond those permitted through the application interface. This issue affects mpGabinet version 23.12.19 and below.	N/A	More Details
CVE-2026-31681	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_multiport: validate range encoding in checkentry ports_match_v1() treats any non-zero pflags entry as the start of a port range and unconditionally consumes the next ports[] element as the range end. The checkentry path currently validates protocol, flags and count, but it does not validate the range encoding itself. As a result, malformed rules can mark the last slot as a range start or place two range starts back to back, leaving ports_match_v1() to step past the last valid ports[] element while interpreting the rule. Reject malformed multiport v1 rules in checkentry by validating that each range start has a following element and that the following element is not itself marked as another range start.	N/A	More Details
CVE-2026-31677	In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - limit RX SG extraction by receive buffer budget Make af_alg_get_rsgl() limit each RX scatterlist extraction to the remaining receive buffer budget. af_alg_get_rsgl() currently uses af_alg_readable() only as a gate before extracting data into the RX scatterlist. Limit each extraction to the remaining af_alg_rcvbuf(sk) budget so that receive-side accounting matches the amount of data attached to the request. If skcipher cannot obtain enough RX space for at least one chunk while more data remains to be processed, reject the recvmsg call instead of rounding the request length down to zero.	N/A	More Details
CVE-2026-6175	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-41427	Better Auth is an authentication and authorization library for TypeScript. Prior to 1.6.5, the clientPrivileges option documents a create action, but the OAuth client creation endpoints did not invoke the hook before persisting new clients. Deployments that configured clientPrivileges to restrict client registration were not actually restricted — any authenticated user could reach the create endpoints and register an OAuth client with attacker-chosen redirect URIs and metadata. This vulnerability is fixed in 1.6.5.	N/A	More Details
CVE-2026-41240	DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Versions prior to 3.4.0 have an inconsistency between FORBID_TAGS and FORBID_ATTR handling when function-based ADD_TAGS is used. Commit c361baa added an early exit for FORBID_ATTR at line 1214. The same fix was not applied to FORBID_TAGS. At line 1118-1123, when EXTRA_ELEMENT_HANDLING.tagCheck returns true, the short-circuit evaluation skips the FORBID_TAGS check entirely. This allows forbidden elements to survive sanitization with their attributes intact. Version 3.4.0 patches the issue.	N/A	More Details

CVE-2026-5039	TP-Link TL-WR841N v13 uses DES-CBC encryption in the TDDPv2 debug protocol with a cryptographic key derived from default web management credentials, making the key predictable if device is left in default configuration. A network-adjacent attacker can exploit this weakness to gain unauthorized access to the protocol, read debug data, modify certain device configuration values, and trigger device reboot, resulting in loss of integrity and a denial-of-service condition.	N/A	More Details
CVE-2026-33694	This vulnerability allows an attacker to create a junction, enabling the deletion of arbitrary files with SYSTEM privileges. As a result, this condition potentially facilitates arbitrary code execution, whereby an attacker may exploit the vulnerability to execute malicious code with elevated SYSTEM privileges.	N/A	More Details
CVE-2026-6074	A path traversal condition in Intrado 911 Emergency Gateway could allow an attacker with existing network access the ability to access the EGW management interface without authentication. Successful exploitation of this vulnerability could allow a user to read, modify, or delete files.	N/A	More Details
CVE-2026-6375	A vulnerability in SpiceJet's booking API allows unauthenticated users to query passenger name records (PNRs) without any access controls. Because PNR identifiers follow a predictable pattern, an attacker could systematically enumerate valid records and obtain associated passenger names. This flaw stems from missing authorization checks on an endpoint intended for authenticated profile access.	N/A	More Details
CVE-2026-6376	A weakness in SpiceJet's public booking retrieval page permits full passenger booking details to be accessed using only a PNR and last name, with no authentication or verification mechanisms. This results in exposure of extensive personal, travel, and booking metadata to any unauthenticated user who can obtain or guess those basic inputs. The issue arises from improper access control on a sensitive data retrieval function.	N/A	More Details
CVE-2026-41274	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the GraphCypherQAChain node forwards user-provided input directly into the Cypher query execution pipeline without proper sanitization. An attacker can inject arbitrary Cypher commands that are executed on the underlying Neo4j database, enabling data exfiltration, modification, or deletion. This vulnerability is fixed in 3.1.0.	N/A	More Details
CVE-2026-41317	Press, a Frappe custom app that runs Frappe Cloud, manages infrastructure, subscription, marketplace, and software-as-a-service (SaaS).`press.api.account.create_api_secret` is prone to CSRF-like exploits. This endpoint writes to database and it is also accessible via GET method. The patch in commit 52ea2f2d1b587be0807557e96f025f47897d00fd restricts method to POST.	N/A	More Details
CVE-2026-41430	Press, a Frappe custom app that runs Frappe Cloud, manages infrastructure, subscription, marketplace, and software-as-a-service (SaaS). Redirect parameter on login page is vulnerable to reflected XSS. The patch in commit 16d1b6ca2559f858a1de77bcb03fd7f1b81671c6 fixes the issue by restricting redirects to internal URLs only.	N/A	More Details
CVE-2026-6272	A client holding only a read JWT scope can still register itself as a signal provider through the production kuksa.val.v2 OpenProviderStream API by sending ProvideSignalRequest. 1. Obtain any valid token with only read scope. 2. Connect to the normal production gRPC API (kuksa.val.v2). 3. Open OpenProviderStream. 4. Send ProvideSignalRequest for a target signal ID. 5. Wait for the broker to forward GetProviderValueRequest. 6. Reply with attacker-controlled GetProviderValueResponse. 7. Other clients performing GetValue / GetValues for that signal receive forged data.	N/A	More Details
CVE-2026-4313	AdaptiveGRC is vulnerable to Stored XSS via text type fields across the forms. Authenticated attacker can replace the value of the text field in the HTTP POST request. Improper parameter validation by the server results in arbitrary JavaScript execution in the victim's browser. Critically, this may allow the attacker to obtain the administrator authentication token and perform arbitrary actions with administrative privileges, which could lead to further compromise. This issue occurs in versions released before December 2025.	N/A	More Details
CVE-2026-6043	P4 Server versions prior to 2026.1 are configured with insecure default settings that, when exposed to untrusted networks, allow unauthenticated attackers to create arbitrary user accounts, enumerate existing users, authenticate to accounts with no password set, and access depot contents via the built-in 'remote' user. These default settings, taken together, can lead to unauthorized access to source code repositories and other managed assets. The 2026.1 release, expected in May 2026, enforces secure-by-default configurations on upgrade and new installations	N/A	More Details
CVE-2026-31534	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-31593	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Reject attempts to sync VMSA of an already-launched/encrypted vCPU Reject synchronizing vCPU state to its associated VMSA if the vCPU has already been launched, i.e. if the VMSA has already been encrypted. On a host with SNP enabled, accessing guest-private memory generates an RMP #PF and panics the host. BUG: unable to handle page fault for address: ff1276cbfdf36000 #PF: supervisor write access in kernel mode #PF: error_code(0x80000003) - RMP violation PGD 5a31801067 P4D 5a31802067 PUD 40ccfb5063 PMD 40e5954063 PTE 80000040fdf36163 SEV-SNP: PFN 0x40fdf36, RMP entry: [0x6010ffffffffff001 - 0x000000000000001f] Oops: Oops: 0003 [#1] SMP NOPTI CPU: 33 UID: 0 PID: 996180 Comm: qemu-system-x86 Tainted: G OE Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: Dell Inc. PowerEdge R7625/0H1TJT, BIOS 1.5.8 07/21/2023 RIP: 0010:sev_es_sync_vmsa+0x54/0x4c0 [kvm_amd] Call Trace: <TASK> snp_launch_update_vmsa+0x19d/0x290 [kvm_amd] snp_launch_finish+0xb6/0x380 [kvm_amd] sev_mem_enc_ioctl+0x14e/0x720 [kvm_amd] kvm_arch_vm_ioctl+0x837/0xcf0 [kvm] kvm_vm_ioctl+0x3fd/0xcc0 [kvm] __x64_sys_ioctl+0xa3/0x100 x64_sys_call+0xfe0/0x2350 do_syscall_64+0x81/0x10f0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7ffff673287d </TASK> Note, the KVM flaw has been present since commit ad73109ae7ec ("KVM: SVM: Provide support to launch and run an SEV-ES guest"), but has only been actively dangerous for the host since SNP support was added. With SEV-ES, KVM would "just" clobber guest state, which is totally fine from a host kernel perspective since userspace can clobber guest state any time before sev_launch_update_vmsa().	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: pci-epf-vntb: Remove duplicate resource teardown epf_ntb_epc_destroy() duplicates the teardown that the caller is supposed to perform later. This leads to an oops when .allow_link fails or when .drop_link is performed. The following is an example oops of the former case: Unable to		

CVE-2026-31594	handle kernel paging request at virtual address dead000000000108 [...] [dead000000000108] address between user and kernel address ranges Internal error: Oops: 0000000096000044 [#1] SMP [...] Call trace: pci_epc_remove_epf+0x78/0xe0 (P) pci_primary_epc_epf_link+0x88/0xa8 configfs_symlink+0x1f4/0x5a0 vfs_symlink+0x134/0x1d8 do_symlinkat+0x88/0x138 __arm64_sys_symlinkat+0x74/0xe0 [...] Remove the helper, and drop pci_epc_put(). EPC device refcounting is tied to the configfs EPC group lifetime, and pci_epc_put() in the .drop_link path is sufficient.	N/A	More Details
CVE-2026-31595	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: pci-epf-vntb: Stop cmd_handler work in epf_ntb_epc_cleanup Disable the delayed work before clearing BAR mappings and doorbells to avoid running the handler after resources have been torn down. Unable to handle kernel paging request at virtual address ffff800083f46004 [...] Internal error: Oops: 0000000096000007 [#1] SMP [...] Call trace: epf_ntb_cmd_handler+0x54/0x200 [pci_epf_vntb] (P) process_one_work+0x154/0x3b0 worker_thread+0x2c8/0x400 kthread+0x148/0x210 ret_from_fork+0x10/0x20	N/A	More Details
CVE-2026-31596	In the Linux kernel, the following vulnerability has been resolved: ocfs2: handle invalid dinode in ocfs2_group_extend [BUG] kernel BUG at fs/ocfs2/resize.c:308! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI RIP: 0010:ocfs2_group_extend+0x10aa/0x1ae0 fs/ocfs2/resize.c:308 Code: 8b8520ff ffff83f8 860f8580 030000e8 5cc3c1fe Call Trace: ... ocfs2_ioctl+0x175/0x6e0 fs/ocfs2/ioctl.c:869 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x197/0x1e0 fs/ioctl.c:583 x64_sys_call+0x1144/0x26a0 arch/x86/include/generated/asm/syscalls_64.h:17 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x93/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e ... [CAUSE] ocfs2_group_extend() assumes that the global bitmap inode block returned from ocfs2_inode_lock() has already been validated and BUG_ONs when the signature is not a dinode. That assumption is too strong for crafted filesystems because the JBD2-managed buffer path can bypass structural validation and return an invalid dinode to the resize ioctl. [FIX] Validate the dinode explicitly in ocfs2_group_extend(). If the global bitmap buffer does not contain a valid dinode, report filesystem corruption with ocfs2_error() and fail the resize operation instead of crashing the kernel.	N/A	More Details
CVE-2026-31601	In the Linux kernel, the following vulnerability has been resolved: vfio/xe: Reorganize the init to decouple migration from reset Attempting to issue reset on VF devices that don't support migration leads to the following: BUG: unable to handle page fault for address: 00000000000011f8 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 2 UID: 0 PID: 7443 Comm: xe_sriov_flr Tainted: G S U 7.0.0-rc1-lgci-xe-xe-4588-cec43d5c2696af219-nodebug+ #1 PREEMPT(lazy) Tainted: [S]=CPU_OUT_OF_SPEC, [U]=USER Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-P DDR4 RVP, BIOS RPLPFWI1.R00.4035.A00.2301200723 01/20/2023 RIP: 0010:xe_sriov_vfio_wait_flr_done+0xc/0x80 [xe] Code: ff c3 cc cc cc cc 0f 1f 84 00 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 0f 1f 44 00 00 55 48 89 e5 41 54 53 <83> bf f8 11 00 00 02 75 61 41 89 f4 85 f6 74 52 48 8b 47 08 48 89 RSP: 0018:ffffc9000f7c39b8 EFLAGS: 00010202 RAX: ffffffffa04d8660 RBX: ffff88813e3e4000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000f7c39c8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff888101a48800 R13: ffff88813e3e4150 R14: ffff888130d0d008 R15: ffff88813e3e40d0 FS: 00007877d3d0d940(0000) GS:ffff88890b6d3000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000000011f8 CR3: 000000015a762000 CR4: 0000000000f52ef0 PKRU: 55555554 Call Trace: <TASK> xe_vfio_pci_reset_done+0x49/0x120 [xe_vfio_pci] pci_dev_restore+0x3b/0x80 pci_reset_function+0x109/0x140 reset_store+0x5c/0xb0 dev_attr_store+0x17/0x40 sysfs_kf_write+0x72/0x90 kernfs_fop_write_iter+0x161/0x1f0 vfs_write+0x261/0x440 ksys_write+0x69/0xf0 __x64_sys_write+0x19/0x30 x64_sys_call+0x259/0x26e0 do_syscall_64+0xcb/0x1500 ? __fput+0x1a2/0x2d0 ? fput_close_sync+0x3d/0xa0 ? __x64_sys_close+0x3e/0x90 ? x64_sys_call+0x1b7c/0x26e0 ? do_syscall_64+0x109/0x1500 ? __task_pid_nr_ns+0x68/0x100 ? __do_sys_getpid+0x1d/0x30 ? x64_sys_call+0x10b5/0x26e0 ? do_syscall_64+0x109/0x1500 ? putname+0x41/0x90 ? do_faccessat+0x1e8/0x300 ? __x64_sys_access+0x1c/0x30 ? x64_sys_call+0x1822/0x26e0 ? do_syscall_64+0x109/0x1500 ? tick_program_event+0x43/0xa0 ? hrtimer_interrupt+0x126/0x260 ? irqentry_exit+0xb2/0x710 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7877d5f1c5a4 Code: c7 00 16 00 00 00 b8 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 80 3d a5 ea 0e 00 00 74 13 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 55 48 89 e5 48 83 ec 20 48 89 RSP: 002b:00007fff48e5f908 EFLAGS: 00000202 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007877d5f1c5a4 RDX: 0000000000000001 RSI: 00007877d621b0c9 RDI: 0000000000000009 RBP: 0000000000000001 R08: 00005fb49113b010 R09: 0000000000000007 R10: 0000000000000000 R11: 0000000000000202 R12: 00007877d621b0c9 R13: 0000000000000009 R14: 00007fff48e5fac0 R15: 00007fff48e5fac0 </TASK> This is caused by the fact that some of the xe_vfio_pci_core_device members needed for handling reset are only initialized as part of migration init. Fix the problem by reorganizing the code to decouple VF init from migration init.	N/A	More Details
CVE-2026-31603	In the Linux kernel, the following vulnerability has been resolved: staging: sm750fb: fix division by zero in ps_to_hz() ps_to_hz() is called from hw_sm750_crtc_set_mode() without validating that pixclock is non-zero. A zero pixclock passed via FBIOPUT_VSCREENINFO causes a division by zero. Fix by rejecting zero pixclock in lynxfb_ops_check_var(), consistent with other framebuffer drivers.	N/A	More Details
CVE-2026-31604	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: fix device leak on probe failure Driver core holds a reference to the USB interface and its parent USB device while the interface is bound to a driver and there is no need to take additional references unless the structures are needed after disconnect. This driver takes a reference to the USB device during probe but does not to release it on all probe errors (e.g. when descriptor parsing fails). Drop the redundant device reference to fix the leak, reduce cargo culting, make it easier to spot drivers where an extra reference is needed, and reduce the risk of further memory leaks.	N/A	More Details
CVE-2026-31605	In the Linux kernel, the following vulnerability has been resolved: fbdev: udlfb: avoid divide-by-zero on FBIOPUT_VSCREENINFO Much like commit 19f953e74356 ("fbdev: fb_pm2fb: Avoid potential divide by zero error"), we also need to prevent that same crash from happening in the udlfb driver as it uses pixclock directly when dividing, which will crash.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_hid: don't call cdev_init while cdev in use When calling unbind, then bind again, cdev_init reinitialized the cdev, even though there may still be references to it. That's the case when the /dev/hidg* device is still opened. This obviously unsafe behavior like oopes. This fixes this by using	N/A	More Details

31606	cdev_alloc to put the cdev on the heap. That way, we can simply allocate a new one in hidg_bind.		
CVE-2026-31610	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix mechToken leak when SPNEGO decode fails after token alloc The kernel ASN.1 BER decoder calls action callbacks incrementally as it walks the input. When ksmbd_decode_negTokenInit() reaches the mechToken [2] OCTET STRING element, ksmbd_neg_token_alloc() allocates conn->mechToken immediately via kmemdup_nul(). If a later element in the same blob is malformed, then the decoder will return nonzero after the allocation is already live. This could happen if mechListMIC [3] overrunse the enclosing SEQUENCE. decode_negotiation_token() then sets conn->use_spnego = false because both the negTokenInit and negTokenTarg grammars failed. The cleanup at the bottom of smb2_sess_setup() is gated on use_spnego: if (conn->use_spnego && conn->mechToken) { kfree(conn->mechToken); conn->mechToken = NULL; } so the kfree is skipped, causing the mechToken to never be freed. This codepath is reachable pre-authentication, so untrusted clients can cause slow memory leaks on a server without even being properly authenticated. Fix this up by not checking check for use_spnego, as it's not required, so the memory will always be properly freed. At the same time, always free the memory in ksmbd_conn_free() incase some other failure path forgot to free it.	N/A	More Details
CVE-2026-31614	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix off-by-8 bounds check in check_wsl_eas() The bounds check uses (u8 *)ea + nlen + 1 + vlen as the end of the EA name and value, but ea_data sits at offset sizeof(struct smb2_file_full_ea_info) = 8 from ea, not at offset 0. The strncmp() later reads ea->ea_data[0..nlen-1] and the value bytes follow at ea_data[nlen+1..nlen+vlen], so the actual end is ea->ea_data + nlen + 1 + vlen. Isn't pointer math fun? The earlier check (u8 *)ea > end - sizeof(*ea) only guarantees the 8-byte header is in bounds, but since the last EA is placed within 8 bytes of the end of the response, the name and value bytes are read past the end of iov. Fix this mess all up by using ea->ea_data as the base for the bounds check. An "untrusted" server can use this to leak up to 8 bytes of kernel heap into the EA name comparison and influence which WSL xattr the data is interpreted as.	N/A	More Details
CVE-2026-40609	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-41140	Poetry is a dependency manager for Python. Prior to 2.3.4, the extractall() function in src/poetry/utils/helpers.py:410-426 extracts sdist tarballs without path traversal protection on Python versions where tarfile.data_filter is unavailable. Considering only Python versions which are still supported by Poetry, these are 3.10.0 - 3.10.12 and 3.11.0 - 3.11.4. This vulnerability is fixed in 2.3.4.	N/A	More Details
CVE-2026-41326	Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. From v3.4.0 to v3.28.0, an oversight in the CopyFile policy (and perhaps the CopyFile handler) allows untrusted hosts to write to arbitrary locations inside the guest workload image. This can be used to overwrite binaries inside the guest and exfiltrate data from containers; even those running inside CVMs. This vulnerability is fixed in v3.29.0.	N/A	More Details
CVE-2026-41894	SiYuan is an open-source personal knowledge management system. Prior to 3.6.5, the fix for CVE-2026-30869 only added a denylist check (IsSensitivePath) but did not address the root cause — a redundant url.PathUnescape() call in serveExport(). An authenticated attacker can use double URL encoding (%252e%252e) to traverse directories and read arbitrary workspace files including the full SQLite database (siyuan.db), kernel log, and all user documents. This vulnerability is fixed in 3.6.5.	N/A	More Details
CVE-2026-41907	uuid is for the creation of RFC9562 (formerly RFC4122) UUIDs. Prior to 14.0.0, v3, v5, and v6 accept external output buffers but do not reject out-of-range writes (small buf or large offset). This allows silent partial writes into caller-provided buffers. This vulnerability is fixed in 14.0.0.	N/A	More Details
CVE-2026-7363	Use after free in Canvas in Google Chrome on Linux, ChromeOS prior to 147.0.7727.138 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	N/A	More Details