SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 May 2026

Generated on 06 May 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-2026-42369	GV-VMS V20 is a Video Monitoring Software used to gather the feeds of many surveillance cameras and manage other security devices. It is a native application accessed locally, but it is also possible to enable remote access via the "WebCam Server" feature. Once enabled, it is possible to access to the management and monitoring feature via a regular Web interface. This webersever is another native application, compiled without ASLR, which makes exploitation much easier and more likely. Most of the features require authentication before being reachable and leverage a standard login page to grant access. However the `gvapi` endpoint uses its own authentication mechanism via an `HTTP Authorization` header. It supports both `Basic` authentication and the `Digest` modes of authentication. #### Stack-overflow via unbound copy of base64 decoded string The `b64decoder` string is sized dynamically, but it is then copied to the `Buffer` stack variable one character at the time at [0], and there's no bound-check. As such, if the decoded string is bigger than 256 characters (the size of the `Buffer` variable) then a stack overflow occurs. Because the data can be fully controlled by an attacker and lack of ASLR, this vulnerability can easily be exploited to gain full code execution as SYSTEM on the machine running the service.	10.0	More Details
CVE-2026-36767	A path traversal vulnerability in the /content/images/add endpoint of shopizer v3.2.5 allows attackers write arbitrary files to any writeable path via a crafted POST request.	10.0	More Details
CVE-2026-37541	Buffer overflow vulnerability in Open Vehicle Monitoring System 3 (OVMS3) 3.3.005. In canformat_gvret.cpp, the length field in GVRET binary data is not properly validated, allowing remote attackers to cause a denial of service or possibly execute arbitrary code via crafted GVRET frames.	10.0	More Details
CVE-2026-35051	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is an authentication bypass vulnerability in Traefik's ForwardAuth middleware when trustForwardHeader=false is configured and Traefik is deployed behind a trusted upstream proxy. This issue has been patched in versions 2.11.43, 3.6.14, and 3.7.0-rc.2.	10.0	More Details
CVE-2026-39858	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is a high severity authentication bypass vulnerability in Traefik's ForwardAuth and snippet-based authentication middleware. Traefik's forwarded-header sanitization logic targets only canonical header names (e.g., X-Forwarded-Proto) and does not strip or normalize alias variants that use underscores instead of dashes (e.g., X_Forwarded_Proto). These unsanitized alias headers are forwarded intact to the authentication backend. When the backend normalizes underscore and dash header forms equivalently, an attacker can inject spoofed trust context — such as a trusted scheme or host — through the alias headers and bypass authentication on protected routes without valid credentials. This issue has been patched in versions 2.11.43, 3.6.14, and 3.7.0-rc.2.	10.0	More Details
CVE-2026-7411	In Eclipse BaSyx Java Server SDK versions prior to 2.0.0-milestone-10, inadequate path normalization in the Submodel HTTP API allows an unauthenticated remote attacker to perform a path traversal attack. By supplying a maliciously crafted fileName parameter during a file upload operation, an attacker can bypass intended storage boundaries and write arbitrary files to any location on the host filesystem accessible by the Java process. This can lead to Remote Code Execution (RCE) and complete system compromise.	10.0	More Details
CVE-2026-42810	Apache Polaris accepts literal `*` characters in namespace and table names. When it later builds temporary S3 access policies for delegated table access, those same characters appear to be reused unescaped in S3 IAM resource patterns and `s3:prefix` conditions. In S3 IAM policy matching, `*` is treated as a wildcard rather than as ordinary text. That means temporary credentials issued for one crafted table can match the storage path of a different table. In private testing against Polaris 1.4.0 using Polaris' AWS S3 temporary- credential path on both MinIO and real AWS S3, credentials returned for crafted tables such as `f*.t1`, `f*.*`, `*.*`, and `foo.*` could reach other tables' S3 locations. The confirmed behavior includes: - reading another table's metadata control file ([Iceberg metadata JSON]); - listing another table's exact S3 table prefix ([table prefix]); - and, when write delegation was returned for the crafted table, creating and deleting an object under another table's exact S3 table prefix. A control case using ordinary different names did not allow the same cross-table	9.9	More Details

	access. A least-privilege AWS S3 variant was also confirmed in which the attacker principal had no Polaris permissions on the victim table and only the minimal permissions required to create and use a crafted wildcard table (namespace-scoped `TABLE_CREATE` and `TABLE_WRITE_DATA` on `*`). In that setup, direct Polaris access to `foo.t1` remained forbidden, but the attacker could still create and load `*.*`, receive delegated S3 credentials, and use those credentials to list, read, create, and delete objects under `foo.t1`. In Iceberg, the metadata JSON file is a control file: it tells readers which data files belong to the table, which snapshots exist, and which table version to read. So unauthorized access to it is already a meaningful confidentiality problem. The confirmed write-capable variant means the issue is not limited to disclosure.		
CVE-2026-42364	An os command injection vulnerability exists in the DdnsSetting.cgi functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted DDNS configuration can lead to arbitrary command execution. An attacker can modify a configuration value to trigger this vulnerability.	9.9	More Details
CVE-2026-42368	A privilege escalation vulnerability exists in the Web Interface functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted HTTP request can lead to execute priviledged operation. An attacker can visit a webpage to trigger this vulnerability.	9.9	More Details
CVE-2026-42812	In Apache Iceberg, the table's metadata files are control files: they tell readers which data files belong to the table and which table version to read. `write.metadata.path` is an optional table property that tells Polaris where to write those metadata files. For a table already registered in a Polaris-managed catalog, changing only that property through an `ALTER TABLE`-style settings change (not a row-level `INSERT`, `SELECT`, `UPDATE`, or `DELETE`) bypasses the commit-time branch that is supposed to revalidate storage locations. The full persisted / credential-vending variant requires the affected catalog to have `polaris.config.allow.unstructured.table.location=true`, with `allowedLocations` broad enough to include the attacker-chosen target. `allowedLocations` is the admin-configured allowlist of storage paths that the catalog is allowed to use. Public project materials suggest that this flag is a real supported compatibility / layout mode, not just a contrived lab-only prerequisite. In that configuration, a user who can change table settings can cause Apache Polaris itself to write new table metadata to an attacker-chosen reachable storage location before the intended location-validation branch runs. If the later concrete-path validation also accepts that location, Polaris persists the resulting metadata path into stored table state. Later table-load and credential APIs can then return temporary cloud-storage credentials for the same location without revalidating it. In plain terms, Polaris can later hand out temporary storage access for the same attacker-chosen area. That attacker-chosen area does not need to be limited to the poisoned table's own files. If it is a broader storage prefix, another table's prefix, or, depending on configuration or provider behavior, even a bucket/container root, the resulting disclosure or corruption scope can extend to any data and metadata Polaris can reach there. The practical consequences are therefore similar to the staged-create credential-vending issue already discussed: data and metadata reachable in that storage scope can be exposed and, if write-capable credentials are later issued, modified, corrupted, or removed. Even before that later credential step, Polaris itself performs the metadata write to the unchecked location. So the core issue is not only later credential vending. The primary defect is that Polaris skips its intended location checks before performing a security- sensitive metadata write when only `write.metadata.path` changes. When `polaris.config.allow.unstructured.table.location=false`, current code review suggests the later `updateTableLike(...)` validation usually rejects out-of-tree metadata locations before the unsafe path is persisted. That may reduce the persisted / credential-vending variant, but it does not prevent the underlying defect: Polaris still skips the intended pre-write location check when only `write.metadata.path` changes.	9.9	More Details
CVE-2026-42811	In plain terms, Apache Polaris is supposed to issue short-lived GCS credentials that only work for one table's files, but a crafted namespace or table name can cause those credentials to work across the configured bucket instead. Apache Polaris builds Google Cloud Storage downscoped credentials by creating a Credential Access Boundary (CAB) with CEL conditions that are intended to restrict access to the requested table's storage path. The relevant CEL string is built from the bucket name and the table path. That table path is derived from namespace and table identifiers. In current code, that path appears to be inserted into the CEL expression without escaping. As a result, a namespace or table identifier containing a single quote and other URI-safe CEL fragments can break out of the intended quoted string and change the meaning of the CEL condition. In private testing against Polaris 1.4.0 on real Google Cloud Storage, it was confirmed that Polaris accepted a crafted identifier and returned delegated GCS credentials whose CEL path restriction had effectively collapsed. Those delegated credentials could then: - list another table's object prefix; - read another table's metadata control file (Iceberg metadata JSON); - create and delete an object under another table's object prefix; - and also list, read, create, and delete objects under an unrelated external prefix in the same bucket that was not part of any table path. That last point is important. The issue is not limited to "another table". In the confirmed setup, once Apache Polaris returned credentials for the crafted table, the path restriction inside the configured bucket was effectively gone. The practical effect is that temporary credentials for one crafted table can be broader than the table Polaris was asked to authorize, and can become effectively bucket-wide within the configured bucket. The current GCS testing used a Polaris principal with broad catalog privileges for setup. A separate least-privilege Polaris RBAC variant has not yet been tested on GCS. However, the storage-credential broadening behavior itself has been confirmed on GCS.	9.9	More Details
CVE-2026-42809	Apache Polaris can issue broad temporary ("vended") storage credentials during staged table creation before the effective table location has been validated or durably reserved. Those temporary credentials are meant to limit the scope of accessible table data and metadata, but this scope limitation becomes attacker- directed because the attacker can choose a reachable target location. In the confirmed variant, if the caller supplies a custom `location` during stage create and requests credential vending, Apache Polaris uses that location to construct delegated storage credentials immediately. The stage-create path itself neither runs the normal location validation nor the overlap checks before those credentials are issued. Closely related to that, the staged-create flow also accepts `write.data.path` / `write.metadata.path` in the request properties and feeds those location overrides into the same effective table location set used for credential vending. Those fields are secondary to the main custom-`location` exploit, but they are still attacker-influenced location inputs that should be validated before any credentials are issued.	9.9	More Details
CVE-2026-7747	A security flaw has been discovered in Totolink N300RH 3.2.4-B20220812. Affected by this vulnerability is the function loginauth of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. Performing a manipulation of the argument Password results in buffer overflow. 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-2026-26332	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.0, SuppressedError allows attackers to escape the sandbox and run arbitrary code. This issue has been patched in version 3.11.0.	9.8	More Details
CVE-2026-24781	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.0, VM2 suffers from a sandbox breakout vulnerability through the inspect function. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This issue has been patched in version 3.11.0.	9.8	More Details
	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.10.5, the fix for CVE-2023-37466 is insufficient and can be		

CVE-2026-24120	circumvented allowing attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This issue has been patched in version 3.10.5.	9.8	More Details
CVE-2026-24118	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.0, VM2 suffers from a sandbox breakout vulnerability. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This issue has been patched in version 3.11.0.	9.8	More Details
CVE-2025-70067	Buffer Overflow vulnerability exists in Assimp versions up to 6.0.2 in the FBX Importer. The vulnerability occurs in aiMaterial::AddBinaryProperty, where a property key string from a crafted FBX file is copied into a fixed-size heap buffer using strcpy() without runtime length validation	9.8	More Details
CVE-2026-7834	A security vulnerability has been detected in EFM ipTIME NAS1dual 1.5.24. This issue affects the function get_csrf_whites of the file /cgi/advanced/misc_main.cgi. Such manipulation leads to stack-based buffer overflow. The attack can be launched 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.	9.8	More Details
CVE-2026-42027	Arbitrary Class Instantiation via Model Manifest in Apache OpenNLP ExtensionLoader Versions Affected: before 2.5.9, before 3.0.0-M3 Description: The ExtensionLoader.instantiateExtension(Class, String) method loads a class by its fully-qualified name via Class.forName() and invokes its no-arg constructor, with the class name sourced from the manifest.properties entry of a model archive. The existing isAssignableFrom check correctly rejects classes that are not subtypes of the expected extension interface (BaseToolFactory for factory=, ArtifactSerializer for serializer-class-*), but the check runs after Class.forName() has already loaded and initialized the named class. Class.forName() with default initialization semantics executes the target class's static initializer before returning, so an attacker who can supply a crafted model archive can cause the static initializer of any class on the classpath to run during model loading, regardless of whether that class passes the subsequent type check. Exploitation requires a class with attacker-useful side effects in its static initializer (for example, JNDI lookup, outbound network I/O, or filesystem access) to be present on the classpath, so this is not a drop-in remote code execution; however, the attack surface grows as third-party model distribution becomes more common (community model repositories, Hugging Face-style sharing), where users routinely load model files from origins they do not control. A secondary, narrower vector affects deployments that ship legitimate BaseToolFactory or ArtifactSerializer subclasses with side-effecting no-arg constructors: a malicious manifest can name such a class and force its constructor to run during model load. Mitigation: * 2.x users should upgrade to 2.5.9. * 3.x users should upgrade to 3.0.0-M3. Note: The fix introduces a package-prefix allowlist that is consulted before Class.forName() is invoked, so the static initializer of a disallowed class is never executed. Classes under the opennlp. prefix remain permitted by default. Deployments that load models referencing factories or serializers outside opennlp.* must opt those packages in, either programmatically via ExtensionLoader.registerAllowedPackage(String) before the first model load, or by setting the OPENNLP_EXT_ALLOWED_PACKAGES system property to a comma-separated list of allowed package prefixes. Users who cannot upgrade immediately should ensure that all model files are sourced from trusted origins and should audit their classpath for classes with side-effecting static initializers or constructors, particularly any that perform JNDI lookups, network requests, or filesystem operations during class initialization.	9.8	More Details
CVE-2025-14320	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Tegsoft Management and Information Services Trade Limited Company Online Support Application allows Reflected XSS. This issue affects Online Support Application: from V3 through 31122025.	9.8	More Details
CVE-2026-7719	A security flaw has been discovered in Totolink WA300 5.2cu.7112_B20190227. The affected element is the function loginauth of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument http_host results in buffer overflow. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-36841	TOTOLINK N200RE V5 was discovered to contain a command injection vulnerability via the macstr and bandstr parameters in the formMapDelDevice function.	9.8	More Details
CVE-2026-7458	The User Verification by PickPlugins plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.46. This is due to the use of a loose PHP comparison operator to validate OTP codes in the "user_verification_form_wrap_process_otpLogin" function. This makes it possible for unauthenticated attackers to log in as any user with a verified email address, such as an administrator, by submitting a "true" OTP value.	9.8	More Details
CVE-2026-26956	vm2 is an open source vm/sandbox for Node.js. In version 3.10.4, vm2 is vulnerable to full sandbox escape with arbitrary code execution. Attacker code inside VM.run() obtains host process object and runs host commands with zero host cooperation. This issue has been patched in version 3.10.5.	9.8	More Details
CVE-2026-42374	D-Link DIR-600L Hardware Revision B1 (End-of-Life) contains a hardcoded telnet backdoor. The device starts a telnet daemon at boot via /bin/telnetd.sh with the username "Alphanetworks" and the static password "wrgn61_dlwbr_dir600L" read from /etc/alpha_config/image_sign. The custom telnetd binary accepts a -u user:password flag, and the custom login binary uses strcmp() to validate credentials. Successful authentication grants an unauthenticated attacker on the local network a root shell with full administrative control. The device has reached End-of-Life (EOL) and will not receive patches.	9.8	More Details
CVE-2026-42076	Evolver is a GEP-powered self-evolving engine for AI agents. Prior to version 1.69.3, a command injection vulnerability in the _extractLLM() function allows attackers to execute arbitrary shell commands on the server. The function constructs a curl command using string concatenation and passes it to execSync() without proper sanitization, enabling remote code execution when the corpus parameter contains shell metacharacters. This issue has been patched in version 1.69.3.	9.8	More Details
CVE-2026-42373	D-Link DIR-605L Hardware Revision B2 (End-of-Life, EOL) contains a hardcoded telnet backdoor. The device starts a telnet daemon at boot via /bin/telnetd.sh with the username "Alphanetworks" and the static password "wrgn76_dlwbr_dir605L" read from /etc/alpha_config/image_sign. The custom telnetd binary accepts a -u user:password flag, and the custom login binary uses strcmp() to validate credentials. Successful authentication grants an unauthenticated attacker on the local network a root shell with full administrative control. The device has reached End-of-Life (EOL) and will not receive patches.	9.8	More Details
CVE-2023-54344	Eclipse Equinox OSGi 3.7.2 and earlier contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary commands by sending payloads to the console interface. Attackers can connect to the OSGi console port and send base64-encoded bash commands wrapped in fork directives to achieve code execution and establish reverse shell connections.	9.8	More Details

CVE-2026-42375	D-Link DIR-600L Hardware Revision A1 (End-of-Life) contains a hardcoded telnet backdoor. The device starts a telnet daemon at boot via /bin/telnetd.sh with the username "Alphanetworks" and the static password "wrgn35_dlwbr_dir600l" read from /etc/alpha_config/image_sign. The custom telnetd binary accepts a -u user:password flag, and the custom login binary uses strcmp() to validate credentials. Successful authentication grants an unauthenticated attacker on the local network a root shell with full administrative control. The device has reached End-of-Life (EOL) and will not receive patches.	9.8	More Details
CVE-2026-27960	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. In versions 6.6.0 through 6.9.12, there is a privilege escalation vulnerability that can be exploited by unauthenticated attackers to query the API as any existing user, including the default admin account. This issue has been fixed in version 6.9.13. As a workaround, the default admin can be disabled using the `APP__ADMIN__EXTERNALLY_MANAGED` configuration.	9.8	More Details
CVE-2026-7853	A weakness has been identified in D-Link DI-8100 16.07.26A1. Affected is the function sprintf of the file /auto_reboot.asp of the component HTTP Handler. This manipulation of the argument enable/time causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-42376	D-Link DIR-456U Hardware Revision A1 (End-of-Life, EOL) contains a hardcoded telnet backdoor. The device starts a telnet daemon at boot via /etc/init0.d/S80telnetd.sh with the username "Alphanetworks" and the static password "whdrv01_dlob_dir456U" read from /etc/config/image_sign. The custom telnetd binary accepts a -u user:password flag, and the custom login binary uses strcmp() to validate credentials. Successful authentication grants an unauthenticated attacker on the local network a root shell with full administrative control. The device has reached End-of-Life (EOL) and will not receive patches.	9.8	More Details
CVE-2026-42796	Arelle before 2.39.10 contains an unauthenticated remote code execution vulnerability in the /rest/configure REST endpoint that accepts a plugins query parameter and forwards it to the plugin manager without authentication or authorization. Attackers can supply a URL to a malicious Python file through the plugins parameter, causing the Arelle webserver to download and execute the attacker-controlled code within the Arelle process with its privileges.	9.8	More Details
CVE-2026-5722	The MoreConvert Pro plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.9.14. This is due to the guest waitlist verification flow not invalidating or regenerating verification tokens when the customer email address is changed. This makes it possible for unauthenticated attackers to authenticate as existing users, including administrators, by obtaining a valid guest verification token for an attacker-controlled email, changing the same guest customer email to the target account email through the public waitlist flow, and then using the original verification link.	9.8	More Details
CVE-2025-13618	The Mentoring plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.2.8. This is due to the plugin not properly restricting the roles that users can register with in the mentoring_process_registration() function. This makes it possible for unauthenticated attackers to register with administrator-level user accounts.	9.8	More Details
CVE-2026-5294	The Geeky Bot plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.2.2. This is due to a nopriv AJAX route allowing attacker-controlled model/function dispatch and reaching a plugin installer helper that downloads and unzips attacker-supplied ZIP files into wp-content/plugins/. This makes it possible for unauthenticated attackers to perform arbitrary plugin installation and achieve remote code execution.	9.8	More Details
CVE-2026-7823	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function setAppFilterCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument enable results in os command injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2023-54342	Eclipse Equinox OSGi versions 3.8 through 3.18 contain a remote code execution vulnerability in the console interface that allows unauthenticated attackers to execute arbitrary code by exploiting the fork command functionality. Attackers can establish a telnet connection to the OSGi console, perform a telnet handshake, and send fork commands to download and execute malicious Java code, establishing a reverse shell connection.	9.8	More Details
CVE-2026-4882	The User Registration Advanced Fields plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'URAF_AJAX::method_upload' function in all versions up to, and including, 1.6.20. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: The vulnerability can only be exploited if a "Profile Picture" field is added to the form.	9.8	More Details
CVE-2026-7854	A security vulnerability has been detected in D-Link DI-8100 16.07.26A1. Affected by this vulnerability is the function url_rule_asp of the file /url_rule.asp of the component POST Parameter Handler. Such manipulation leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-37539	Buffer overflow vulnerability in cannelloni v2.0.0 in CAN frame parsing in parser.cpp in function parseCANFrame, and decoder.cpp in function decodeFrame allowing remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via crafted CAN FD frames.	9.8	More Details
CVE-2026-42779	The fix for CVE-2026-41635 was not applied to the 2.1.X and 2.2.X branches. Here was the original issue description: 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 2.1.0 <= 2.1.11, and 2.2.0 <= 2.2.6. The problem is resolved in Apache MINA 2.1.12, and 2.2.7 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-2026-7567	The Temporary Login plugin for WordPress is vulnerable to Authentication Bypass in versions up to and including 1.0.0. This is due to improper input validation in the maybe_login_temporary_user() function, which fails to verify that the 'temp-login-token' GET parameter is a scalar string before processing it. When the parameter is supplied as an array, PHP's empty() check is bypassed and sanitize_key() returns an empty string, which is then passed as the meta_value to get_users(). WordPress ignores an empty meta_value and returns all users matching the meta_key '_temporary_login_token', allowing authentication without a valid token. This makes it possible for unauthenticated attackers to authenticate as any active temporary login user by sending a single crafted GET request.	9.8	More Details
CVE-2026-42994	Bitwarden CLI 2026.4.0 from 2026-04-22T21:57Z to 2026-04-22T23:30Z, when obtained from npm, had embedded malicious code. This is related to a Checkmarx supply chain incident.	9.8	More Details
CVE-2026-	Integer underflow vulnerability in Open-SAE-J1939 thru commit b6caf884df46435e539b1ecbf92b6c29b345bdfe (2025-11-30) in SAE_J1939_Read_Transport_Protocol_Data_Transfer,allows attackers to write to arbitrary memory via crafted	9.8	More Details

37534	sequence number from the CAN frame.		
CVE-2026-7538	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function Vulnerability of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument proto 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-2026-33447	CVE-2026-33447 is a buffer overflow in a message parsing function of the Secure Access client prior to 14.50. Attackers with control of a modified server can send a special packet that can overwrite a small portion of memory conceivably leading to memory corruption or denial of service.	9.8	More Details
CVE-2026-33446	CVE-2026-33446 is a buffer overflow in the authentication sub-system of the Secure Access client prior to 14.50. Attackers with control of a modified server can send a special packet that can overwrite a small portion of memory conceivably leading to memory corruption or a denial of service.	9.8	More Details
CVE-2025-71284	Synway SMG Gateway Management Software contains an OS command injection vulnerability in the RADIUS configuration endpoint at /en/9-2radius.php where the radius_address POST parameter is split and interpolated directly into a sed command without sanitization. An unauthenticated remote attacker can inject arbitrary shell commands by submitting a POST request with crafted radius_address, radius_address2, shared_secret2, source_ip, timeout, or retry parameters along with save=1 and enable_radius=1 to achieve remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-07-11 (UTC).	9.8	More Details
CVE-2022-50993	Weaver (Fanwei) E-office versions prior to 10.0_20221201 contain an unauthenticated arbitrary file upload vulnerability in the OfficeServer.php endpoint that allows remote attackers to upload malicious files by sending multipart POST requests with arbitrary filenames and disguised content types. Attackers can upload PHP webshells to the Document directory and execute them via HTTP GET requests to achieve remote code execution as the web server user. Exploitation evidence was first observed by the Shadowserver Foundation on 2022-10-10 (UTC).	9.8	More Details
CVE-2026-4670	Authentication bypass by primary weakness vulnerability in Progress Software MOVEit Automation allows Authentication Bypass. This issue affects MOVEit Automation: from 2025.0.0 before 2025.0.9, from 2024.0.0 before 2024.1.8, versions prior to 2024.0.0.	9.8	More Details
CVE-2018-25318	Tenda FH303/A300 firmware V5.07.68_EN contains a session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient cookie validation. Attackers can send GET requests to the /goform/AdvSetDns endpoint with a crafted admin cookie to change DNS servers and redirect user traffic to malicious sites.	9.8	More Details
CVE-2018-25317	Tenda W3002R/A302/W309R wireless routers version V5.07.64_en contain a cookie session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient session validation. Attackers can send GET requests to the /goform/AdvSetDns endpoint with a crafted admin language cookie to change primary and secondary DNS servers, redirecting user traffic to malicious DNS servers.	9.8	More Details
CVE-2018-25316	Tenda W308R v2 V5.07.48 contains a cookie session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient session validation. Attackers can send GET requests to the goform/AdvSetDns endpoint with a crafted admin language cookie to change DNS servers and redirect user traffic to malicious sites.	9.8	More Details
CVE-2026-26015	DocsGPT is a GPT-powered chat for documentation. From version 0.15.0 to before version 0.16.0, an attacker accessing both the official DocsGPT website or any local and public deployment, can craft a malicious payload bypassing the "MCP test" behavior to achieve arbitrary remote code execution (RCE). This issue has been patched in version 0.16.0.	9.8	More Details
CVE-2026-41940	cPanel and WHM versions after 11.40 contain an authentication bypass vulnerability in the login flow that allows unauthenticated remote attackers to gain unauthorized access to the control panel.	9.8	More Details
CVE-2026-38992	Cockpit v2.13.5 and earlier is vulnerable to arbitrary code execution via the filter parameter within multiple endpoints. This vulnerability allows an attacker to run system commands on the underlying infrastructure via the MongoLite $func operator.	9.8	More Details
CVE-2026-42778	The fix for CVE-2026-41409 was not applied to the 2.1.X and 2.2.X branches. Here was the original issue description: 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 2.1.0 <= 2.1.11, and 2.2.0 <= 2.2.6. The problem is resolved in Apache MINA 2.1.12, and 2.2.7 by applying the classname allowlist earlier. Affected are applications using Apache MINA that call IoBuffer.getObject(). Applications using Apache MINA are advised to upgrade 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 2.1.0 <= 2.1.110, and 2.2.0 <= 2.2.6. The problem is resolved in Apache MINA 2.1.12, and 2.2.7 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-2026-7546	A security vulnerability has been detected in Totolink NR1800X 9.1.0u.6279_B20210910. The impacted element is the function find_host_ip of the component lighttpd. Such manipulation of the argument Host leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-31705	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out-of-bounds write in smb2_get_ea() EA alignment smb2_get_ea() applies 4-byte alignment padding via memset() after writing each EA entry. The bounds check on buf_free_len is performed before the value memcpy, but the alignment memset fires unconditionally afterward with no check on remaining space. When the EA value exactly fills the remaining buffer (buf_free_len == 0 after value subtraction), the alignment memset writes 1-3 NUL bytes past the buf_free_len boundary. In compound requests where the response buffer is shared across commands, the first command (e.g., READ) can consume most of the buffer, leaving a tight remainder for the QUERY_INFO EA response. The alignment memset then overwrites past the physical kvmalloc allocation into adjacent kernel heap memory. Add a bounds check before the alignment memset to ensure buf_free_len can accommodate the padding bytes. This is the same bug pattern fixed by commit beef2634f81f ("ksmbd: fix potencial OOB in get_file_all_info() for compound requests") and commit fda9522ed6af ("ksmbd: fix OOB write in QUERY_INFO for compound requests"), both of which added bounds checks before unconditional writes in QUERY_INFO response handlers.	9.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: net/x25: Fix potential double free of skb When alloc_skb fails in x25_queue_rx_frame it calls kfree_skb(skb) at line 48 and returns 1 (error). This error propagates back through the call chain: x25_queue_rx_frame returns 1 | v x25_state3_machine receives the return value 1 and takes the else branch at		

43011	line 278, setting queued=0 and returning 0 | v x25_process_rx_frame returns queued=0 | v x25_backlog_rcv at line 452 sees queued=0 and calls kfree_skb(skb) again This would free the same skb twice. Looking at x25_backlog_rcv: net/x25/x25_in.c:x25_backlog_rcv() { ... queued = x25_process_rx_frame(sk, skb); ... if (!queued) kfree_skb(skb); }	9.8	More Details
CVE-2026-42473	Unsafe deserialization vulnerability in MixPHP Framework 2.x thru 2.2.17. The session and cache handlers use unserialize() on data from the filesystem in the FileHandler object.	9.8	More Details
CVE-2026-43039	In the Linux kernel, the following vulnerability has been resolved: net: ti: icssg-prueth: fix missing data copy and wrong recycle in ZC RX dispatch emac_dispatch_skb_zc() allocates a new skb via napi_alloc_skb() but never copies the packet data from the XDP buffer into it. The skb is passed up the stack containing uninitialized heap memory instead of the actual received packet, leaking kernel heap contents to userspace. Copy the received packet data from the XDP buffer into the skb using skb_copy_to_linear_data(). Additionally, remove the skb_mark_for_recycle() call since the skb is backed by the NAPI page frag allocator, not page_pool. Marking a non-page_pool skb for recycle causes the free path to return pages to a page_pool that does not own them, corrupting page_pool state. The non-ZC path (emac_rx_packet) does not have these issues because it uses napi_build_skb() to wrap the existing page_pool page directly, requiring no copy, and correctly marks for recycle since the page comes from page_pool_dev_alloc_pages().	9.8	More Details
CVE-2026-37531	AGL app-framework-main thru 17.1.12 contains a Zip Slip path traversal vulnerability (CWE-22) combined with a TOCTOU race condition (CWE-367) in the widget installation flow. The is_valid_filename function in wgtpkg-zip.c validates ZIP entry names but does not check for dot notation directory traversal sequences it only blocks absolute paths. The zread extraction function uses openat(workdirfd, filename, O_CREAT) which resolves dot notation values relative to the work directory, allowing files to be written anywhere on the filesystem. Critically, in function install_widget in file wgtpkg-install.c, extraction via zread occurs BEFORE signature verification via check_all_signatures. Even if signature verification fails, the error cleanup (remove_workdir) only deletes the temporary work directory files written outside via path traversal persist permanently.	9.8	More Details
CVE-2026-43038	In the Linux kernel, the following vulnerability has been resolved: ipv6: icmp: clear skb2->cb[] in ip6_err_gen_icmpv6_unreach() Sashiko AI-review observed: In ip6_err_gen_icmpv6_unreach(), the skb is an outer IPv4 ICMP error packet where its cb contains an IPv4 inet_skb_parm. When skb is cloned into skb2 and passed to icmp6_send(), it uses IP6CB(skb2). IP6CB interprets the IPv4 inet_skb_parm as an inet6_skb_parm. The cipso offset in inet_skb_parm.opt directly overlaps with dsthao in inet6_skb_parm at offset 18. If an attacker sends a forged ICMPv4 error with a CIPSO IP option, dsthao would be a non-zero offset. Inside icmp6_send(), mip6_addr_swap() is called and uses ipv6_find_tlv(skb, opt->dsthao, IPV6_TLV_HAO). This would scan the inner, attacker-controlled IPv6 packet starting at that offset, potentially returning a fake TLV without checking if the remaining packet length can hold the full 18-byte struct ipv6_destopt_hao. Could mip6_addr_swap() then perform a 16-byte swap that extends past the end of the packet data into skb_shared_info? Should the cb array also be cleared in ip6_err_gen_icmpv6_unreach() and ip6ip6_err() to prevent this? This patch implements the first suggestion. I am not sure if ip6ip6_err() needs to be changed. A separate patch would be better anyway.	9.8	More Details
CVE-2026-43037	In the Linux kernel, the following vulnerability has been resolved: ip6_tunnel: clear skb2->cb[] in ip4ip6_err() Oskar Kjos reported the following problem. ip4ip6_err() calls icmp_send() on a cloned skb whose cb[] was written by the IPv6 receive path as struct inet6_skb_parm. icmp_send() passes IPCB(skb2) to __ip_options_echo(), which interprets that cb[] region as struct inet_skb_parm (IPv4). The layouts differ: inet6_skb_parm.nhoff at offset 14 overlaps inet_skb_parm.opt.rr, producing a non-zero rr value. __ip_options_echo() then reads optlen from attacker-controlled packet data at sptr[rr+1] and copies that many bytes into dopt->__data, a fixed 40-byte stack buffer (IP_OPTIONS_DATA_FIXED_SIZE). To fix this we clear skb2->cb[], as suggested by Oskar Kjos. Also add minimal IPv4 header validation (version == 4, ihl >= 5).	9.8	More Details
CVE-2026-42472	Unsafe deserialization vulnerability in MixPHP Framework 2.x thru 2.2.17. The session and cache handlers use unserialize() on data from Redis in the RedisHandler object.	9.8	More Details
CVE-2026-42483	A heap-based buffer overflow in the Kerberos hash parser in hashcat v7.1.2 allows an attacker to cause a denial of service or possibly execute arbitrary code via a crafted Kerberos hash file. The issue affects module_hash_decode in multiple Kerberos-related modules because account_info_len is calculated from untrusted delimiter positions without upper-bound validation before memcpy copies the data into a fixed-size account_info buffer.	9.8	More Details
CVE-2026-42482	A stack-based buffer overflow in mangle_to_hex_lower() and mangle_to_hex_upper() in src/rp_cpu.c in hashcat v7.1.2 allows an attacker to cause a denial of service or possibly execute arbitrary code via a crafted rule file, or via the -j or -k rule options used with password candidates of 128 or more characters. The vulnerability is caused by a bounds check that fails to account for the 2x expansion that occurs when password bytes are converted to hexadecimal.	9.8	More Details
CVE-2026-42484	A heap-based buffer overflow in hex_to_binary in the PKZIP hash parser in hashcat v7.1.2 allows an attacker to cause a denial of service or possibly execute arbitrary code via a crafted PKZIP hash file. The issue affects modules 17200, 17210, 17220, 17225, and 17230. When data_type_enum<=1, attacker-controlled hex data from a user-supplied hash string is decoded into a fixed-size buffer without proper input-length validation.	9.8	More Details
CVE-2026-31718	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in __ksmbd_close_fd() via durable scavenger When a durable file handle survives session disconnect (TCP close without SMB2_LOGOFF), session_fd_check() sets fp->conn = NULL to preserve the handle for later reconnection. However, it did not clean up the byte-range locks on fp->lock_list. Later, when the durable scavenger thread times out and calls __ksmbd_close_fd(NULL, fp), the lock cleanup loop did: spin_lock(&fp->conn->llist_lock); This caused a slab use-after-free because fp->conn was NULL and the original connection object had already been freed by ksmbd_tcp_disconnect(). The root cause is asymmetric cleanup: lock entries (smb_lock->clist) were left dangling on the freed conn->lock_list while fp->conn was nulled out. To fix this issue properly, we need to handle the lifetime of smb_lock->clist across three paths: - Safely skip clist deletion when list is empty and fp->conn is NULL. - Remove the lock from the old connection's lock_list in session_fd_check() - Re-add the lock to the new connection's lock_list in ksmbd_reopen_durable_fd().	9.8	More Details
CVE-2026-42087	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. From version 6.7.0 to before version 7.0.0-rc3, a SQL injection vulnerability exists in the Time-Series Database (TSDB) component of COSMOS. The tsdb_lookup function in the cvt_model.rb file directly places user-supplied input into a SQL query without sanitizing the input. As a result, a user can break out of the initial SQL statement and execute arbitrary SQL commands, including deleting data. This issue has been patched in version 7.0.0-rc3.	9.6	More Details
CVE-2026-	An issue in the fileMd5 parameter in the /a/file/upload endpoint of JeeSite v5.15.1 allows authenticated attackers with file upload permissions to execute a path traversal and write arbitrary files with whitelisted suffixes to arbitrary filesystem	9.6	More Details

36760	locations while chunked upload is enabled.		
CVE-2026-5166	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Software Center allows Path Traversal. This issue affects Pardus Software Center: before 0.6.4.	9.6	More Details
CVE-2026-42088	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. Prior to version 7.0.0-rc3, the Script Runner widget allows users to execute Python and Ruby scripts directly from the openc3-COSMOS-script-runner-api container. Because all the docker containers share a network, users can execute specially crafted scripts to bypass the API permissions check and perform administrative actions, including reading and modifying data inside the Redis database, which can be used to read secrets and change COSMOS settings, as well as read and write to the buckets service, which holds configuration, log, and plugin files. These actions are normally only available from the Admin Console or with administrative privileges. Any user with permission to create and run scripts can connect to any service in the docker network. This issue has been patched in version 7.0.0-rc3.	9.6	More Details
CVE-2026-42090	Notesnook is a note-taking app focused on user privacy & ease of use. Prior to Notesnook Web/Desktop version 3.3.15 and prior to Notesnook iOS/Android version 3.3.20, a stored XSS vulnerability in the note export flow can be escalated to remote code execution in the desktop app. The root cause is that exported note fields such as title, headline, and content are inserted into the generated HTML template without HTML escaping. When the note is later exported to PDF, Notesnook renders that HTML into a same-origin, unsandboxed iframe using iframe.srcdoc = ... Injected script executes in the Notesnook origin. In the desktop app, this becomes RCE because Electron is configured with nodeIntegration: true and contextIsolation: false. This issue has been patched in Notesnook Web/Desktop version 3.3.15 and Notesnook iOS/Android version 3.3.20.	9.6	More Details
CVE-2026-25293	Buffer overflow due to incorrect authorization in PLC FW	9.6	More Details
CVE-2026-41571	Note Mark is an open-source note-taking application. In version 0.19.2, IsPasswordMatch in backend/db/models.go falls back to a hard-coded bcrypt("null") placeholder whenever a user has no stored password. OIDC-registered users are created with an empty password, so anyone who submits password: "null" to the internal login endpoint receives a valid session for that user. The bypass is unauthenticated and requires no user interaction. This issue has been patched in version 0.19.3.	9.4	More Details
CVE-2026-7161	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-2026-40797	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saleswonder LLC WebinarIgnition allows Blind SQL Injection. This issue affects WebinarIgnition: from n/a through 4.08.253.	9.3	More Details
CVE-2026-43534	OpenClaw before 2026.4.10 contains an input validation vulnerability that allows external hook metadata to be enqueued as trusted system events. Attackers can supply malicious hook names to escalate untrusted input into higher-trust agent context.	9.1	More Details
CVE-2026-36356	The GoAhead web server on MeiG Smart FORGE_SLT711 devices (firmware MDM9607.LE.1.0-00110-STD.PROD-1) allows unauthenticated OS command injection via the /action/SetRemoteAccessCfg endpoint.	9.1	More Details
CVE-2026-43566	OpenClaw versions 2026.4.7 before 2026.4.14 contain a privilege escalation vulnerability where heartbeat owner downgrade logic skips webhook wake events carrying untrusted content. Attackers can exploit this by sending untrusted webhook wake events to preserve owner-like execution context when the run should have been downgraded.	9.1	More Details
CVE-2026-7482	Ollama before 0.17.1 contains a heap out-of-bounds read vulnerability in the GGUF model loader. The /api/create endpoint accepts an attacker-supplied GGUF file in which the declared tensor offset and size exceed the file's actual length; during quantization in fs/ggml/gguf.go and server/quantization.go (WriteTo()), the server reads past the allocated heap buffer. The leaked memory contents may include environment variables, API keys, system prompts, and concurrent users' conversation data, and can be exfiltrated by uploading the resulting model artifact through the /api/push endpoint to an attacker-controlled registry. The /api/create and /api/push endpoints have no authentication in the upstream distribution. Default deployments bind to 127.0.0.1, but the documented OLLAMA_HOST=0.0.0.0 configuration is widely used in practice (large public-internet exposure observed).	9.1	More Details
CVE-2025-14543	Improper Restriction of XML External Entity Reference vulnerability in Connext Professional (Core Libraries) allows Serialized Data External Linking.This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.1.1, from 6.1.0 before 6.1.*, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*, from 4.3x before 5.2.*.	9.1	More Details
CVE-2026-40682	XML External Entity (XXE) via Unsanitized Dictionary Parsing in Apache OpenNLP DictionaryEntryPersistor Versions Affected: before 2.5.9, before 3.0.0-M3 Description: The DictionaryEntryPersistor class initializes a static SAXParserFactory at class-load time without enabling FEATURE_SECURE_PROCESSING or disabling DTD processing. When create(InputStream, EntryInserter) is invoked, the only feature set on the XMLReader is namespace support — external entity resolution and DOCTYPE declarations remain fully enabled. An attacker who can supply a crafted dictionary file (e.g., a stop-word list or domain dictionary) containing a malicious DOCTYPE declaration can trigger local file disclosure via file:// entity references or server-side request forgery via http:// entity references during SAX parsing, before the application processes a single dictionary entry. This is inconsistent with the project's own XmlUtil.createSaxParser() helper, which correctly sets FEATURE_SECURE_PROCESSING and disallow-doctype-decl and is used by all other XML parsing paths in the codebase. The public Dictionary(InputStream) constructor delegates directly to this method and is the documented API for loading user-supplied dictionaries, making untrusted input a realistic scenario. Mitigation: 2.x users should upgrade to 2.5.9. 3.x users should upgrade to 3.0.0-M3. Users who cannot upgrade immediately should ensure that all dictionary files are sourced from trusted origins and should consider wrapping the Dictionary(InputStream) constructor with input validation that rejects any XML containing a DOCTYPE declaration before it reaches the parser.	9.1	More Details

CVE-2026-7381	Plack::Middleware::XSendfile versions through 1.0053 for Perl can allow client-controlled path rewriting. Plack::Middleware::XSendfile allows the variation setting (sendfile type) to be set by the client via the X-Sendfile-Type header, if it is not considered in the middleware constructor or the Plack environment. A malicious client can set the X-Sendfile-Type header to "X-Accel-Redirect" to services running behind nginx reverse proxies, and then set the X-Accel-Mapping to map the path to an arbitrary file on the server. Since 1.0053, Plack::Middleware::XSendfile is deprecated and will be removed from future releases of Plack. This is similar to CVE-2025-61780 for Rack::Sendfile, although Plack::Middleware::XSendfile has some mitigations that disallow regular expressions to be used in the mapping, and only apply the mapping for the "X-Accel-Redirect" type.	9.1	More Details
CVE-2026-7372	A stack overflow vulnerability exists in the WebCam Server Login functionality of GeoVision GV-VMS V20 20.0.2. A specially crafted HTTP request can lead to an arbitrary code execution. An attacker can make an unauthenticated HTTP request to trigger this vulnerability. #### Stack-overflow via unconstrained sscanf The call to `sscanf` at [1] to split the `Buffer` variable into the `username` and `password` variables doesn't limit the size of the extracted content to match the destination buffers' sizes. In this case, if either the username or password decoded from the authorization string exceeds `40` characters (the size the stack variables `username` and `password`) then a stack overflow will occur. The data is controlled by an attacker, but sronger constraints (e.g. no null bytes) may make exploitation harder. A successful attack could lead to full code execution as SYSTEM on the machine running the service.	9.0	More Details
CVE-2026-30893	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.4.0 to before version 4.14.4, a path traversal vulnerability in Wazuh's cluster synchronization extraction routine allows an authenticated cluster peer to write arbitrary files outside the intended extraction directory on other cluster nodes. This can be escalated to code execution in the Wazuh service context by overwriting Python modules loaded by Wazuh components (proof of concept available as separate attachment). In deployments where the cluster daemon runs with elevated privileges, system-level compromise is possible. This issue has been patched in version 4.14.4.	9.0	More Details
CVE-2026-42370	A stack overflow vulnerability exists in the WebCam Server Login functionality of GeoVision GV-VMS V20 20.0.2. A specially crafted HTTP request can lead to an arbitrary code execution. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	9.0	More Details
CVE-2026-42523	Jenkins GitHub Plugin 1.46.0 and earlier improperly processes the current job URL as part of JavaScript implementing validation of the feature "GitHub hook trigger for GITScm polling", resulting in a stored cross-site scripting (XSS) vulnerability exploitable by non-anonymous attackers with Overall/Read permission.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-7641	The Import and export users and customers plugin for WordPress is vulnerable to Privilege Escalation in all versions up to and including 2.0.8 via the `save_extra_user_profile_fields()` function. This is due to an incomplete blocklist that correctly restricts capability meta keys for the primary site (e.g., `wp_capabilities`, `wp_user_level`) but fails to block the equivalent meta keys for any other subsite in a WordPress Multisite network (e.g., `wp_2_capabilities`, `wp_2_user_level`), allowing these keys to pass the `in_array()` check and be written directly to user meta via `update_user_meta()`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their privileges to Administrator on any subsite within the Multisite network by submitting a crafted profile update to `/wp-admin/profile.php`. Exploitation requires that an administrator has previously imported a CSV file containing multisite-prefixed capability column headers and has enabled the 'Show fields in profile?' option, which causes those keys to be stored in the `acui_columns` option and exposed as editable fields on the user profile page.	8.8	More Details
CVE-2026-7512	A flaw has been found in UTT HiPER 1200GW up to 2.5.3-1703. The affected element is the function strcpy of the file /goform/formUser. Executing a manipulation can lead to buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2023-54348	ERPGo SaaS 3.9 contains a CSV injection vulnerability that allows authenticated attackers to execute arbitrary code by injecting formula payloads into vendor name fields. Attackers can add malicious formulas like =10+20+cmd|' /C calc'!A0 in the vendor creation form, which execute when the exported CSV file is opened in spreadsheet applications.	8.8	More Details
CVE-2026-5140	Improper neutralization of CRLF sequences ('CRLF injection') vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Update allows Authentication Bypass. This issue affects Pardus Update: from 0.6.3 before 0.6.4.	8.8	More Details
CVE-2026-24072	An escalation of privilege bug in various modules in Apache HTTP 2.4.66 and earlier allows local .htaccess authors to read files with the privileges of the httpd user. Users are recommended to upgrade to version 2.4.67, which fixes this issue.	8.8	More Details
CVE-2025-58074	A privilege escalation vulnerability exists during the installation of Norton Secure VPN via the Microsoft Store. A low-privilege user can replace files during the installation process, which may result in deletion of arbitrary files that can lead to elevation of privileges.	8.8	More Details
CVE-2026-7470	A flaw has been found in Tenda 4G300 US_4G300V1.0Mt_V1.01.42_CN_TDC01. Affected is the function sub_427C3C of the file /goform/SafeMacFilter. This manipulation of the argument page causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2023-54345	Frappe Framework ERPNext 13.4.0 contains a sandbox escape vulnerability in RestrictedPython that allows authenticated users with System Manager role to execute arbitrary code by exploiting frame introspection. Attackers can create a server script via the /app/server-script endpoint and access the gi_frame attribute to traverse the call stack and invoke os.popen to execute system commands.	8.8	More Details
CVE-2026-5141	Improper Privilege Management, Improper Access Control, Incorrect privilege assignment vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Software Center allows Hijacking a privileged process. This issue affects Pardus Software Center: from 1.0.2 before 1.0.3.	8.8	More Details
CVE-2026-	Improper link resolution before file access ('link following') vulnerability in TUBITAK BILGEM Software Technologies Research Institute	8.8	More

5161	Pardus About allows Symlink Attack. This issue affects Pardus About: before 1.2.2.		Details
CVE-2026-23918	Double Free and possible RCE vulnerability in Apache HTTP Server with the HTTP/2 protocol. This issue affects Apache HTTP Server: 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	8.8	More Details
CVE-2026-3772	The WP Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.9.2. This is due to missing nonce verification in the 'add_plugins_page' and 'add_themes_page' functions. This makes it possible for unauthenticated attackers to overwrite arbitrary plugin and theme PHP files with attacker-controlled code via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	8.8	More Details
CVE-2026-7420	A security flaw has been discovered in UTT HiPER 1250GW up to 3.2.7-210907-180535. Impacted is the function strcpy of the file route/goform/ConfigAdvideo. The manipulation of the argument Profile results in buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-7419	A vulnerability was identified in UTT HiPER 1250GW up to 3.2.7-210907-180535. This issue affects the function strcpy of the file route/goform/formTaskEdit_ap. The manipulation of the argument Profile leads to buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-7418	A vulnerability was determined in UTT HiPER 1250GW up to 3.2.7-210907-180535. This vulnerability affects the function strcpy of the file route/goform/NTP. Executing a manipulation of the argument Profile can lead to buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-43048	In the Linux kernel, the following vulnerability has been resolved: HID: core: Mitigate potential OOB by removing bogus memset() The memset() in hid_report_raw_event() has the good intention of clearing out bogus data by zeroing the area from the end of the incoming data string to the assumed end of the buffer. However, as we have previously seen, doing so can easily result in OOB reads and writes in the subsequent thread of execution. The current suggestion from one of the HID maintainers is to remove the memset() and simply return if the incoming event buffer size is not large enough to fill the associated report. Suggested-by Benjamin Tissoires <bentiss@kernel.org> [bentiss: changed the return value]	8.8	More Details
CVE-2026-29514	NetBox versions 4.3.5 through 4.5.4 contain a remote code execution vulnerability in the RenderTemplateMixin.get_environment_params() method that allows authenticated users with exporttemplate or configtemplate permissions to execute arbitrary code by specifying malicious Python callables in the environment_params field. Attackers can bypass Jinja2 SandboxedEnvironment protections by setting the finalize parameter to any importable Python callable such as subprocess.getoutput, which is invoked on every rendered expression outside the sandbox's call interception mechanism, achieving remote code execution as the NetBox service user.	8.8	More Details
CVE-2026-34965	Cockpit CMS contains an authenticated remote code execution vulnerability in the /cockpit/collections/save_collection endpoint that allows authenticated attackers with collection management privileges to inject arbitrary PHP code into collection rules parameters. Attackers can inject malicious PHP code through rule parameters which is written directly to server-side PHP files and executed via include() to achieve arbitrary command execution on the underlying server.	8.8	More Details
CVE-2026-42372	D-Link DIR-605L Hardware Revision A1 (End-of-Life, EOL) contains a hardcoded telnet backdoor. The device starts a telnet daemon at boot via /bin/telnetd.sh with the username "Alphanetworks" and the static password "wrgn35_dlwbr_dir605l" read from /etc/alpha_config/image_sign. The custom telnetd binary accepts a -u user:password flag, and the custom login binary uses strcmp() to validate credentials. Successful authentication grants an unauthenticated attacker on the local network a root shell with full administrative control. The device has reached End-of-Life (EOL) and will not receive patches.	8.8	More Details
CVE-2026-38991	Cockpit 2.13.5 and earlier is affected by a misconfiguration within the Bucket component _isFileTypeAllowed function where a specially crafted filename bypasses an extension filter. This allows an authenticated attacker to rename arbitrary files with the .php file extension enabling arbitrary code to be executed on the underlying server.	8.8	More Details
CVE-2026-0073	In adbd_tls_verify_cert of auth.cpp, there is a possible bypass of wireless ADB mutual authentication due to a logic error in the code. This could lead to remote (proximal/adjacent) code execution as the shell user with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2018-25308	BuddyPress Xprofile Custom Fields Type 2.6.3 contains a remote code execution vulnerability that allows authenticated users to delete arbitrary files by manipulating unescaped POST parameters. Attackers can modify the field_hiddenfile and field_deleteimg parameters during profile editing to unlink files from the server.	8.8	More Details
CVE-2026-6389	IBM Turbonomic prometurbo agent 8.16.0 through 8.17.6 IBM Turbonomic Application Resource Management grants excessive cluster-wide permissions, including unrestricted read access to all secrets. An attacker that compromises the operator or its service account can exfiltrate sensitive credentials, escalate privileges, and potentially achieve full cluster compromise.	8.8	More Details
CVE-2026-6543	IBM Langflow Desktop 1.0.0 through 1.8.4 Langflow allows an attacker to execute arbitrary commands with the privileges of the process running Langflow. This allows reading sensitive environment variables (API keys, DB credentials), modifying files, or launching further attacks on the internal network.	8.8	More Details
CVE-2026-6849	Improper neutralization of special elements used in an OS command ('OS command injection') vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus OS My Computer allows OS Command Injection. This issue affects Pardus OS My Computer: from <=0.7.5 before 0.8.0.	8.8	More Details
CVE-2026-31773	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SMP: derive legacy responder STK authentication from MITM state The legacy responder path in smp_random() currently labels the stored STK as authenticated whenever pending_sec_level is BT_SECURITY_HIGH. That reflects what the local service requested, not what the pairing flow actually achieved. For Just Works/Confirm legacy pairing, SMP_FLAG_MITM_AUTH stays clear and the resulting STK should remain unauthenticated even if the local side requested HIGH security. Use the established MITM state when storing the responder STK so the key metadata matches the pairing result. This also keeps the legacy path aligned with the Secure Connections code, which already treats JUST_WORKS/JUST_CFM as unauthenticated.	8.8	More Details
CVE-2026-7466	AgentFlow contains an arbitrary code execution vulnerability that allows attackers to execute local Python pipeline files by supplying a user-controlled pipeline_path parameter to the POST /api/runs and POST /api/runs/validate endpoints. Attackers can induce requests to the local AgentFlow API to load and execute existing Python pipeline files on disk, resulting in code execution in the context of the user running AgentFlow.	8.8	More Details

CVE-2026-7548	A vulnerability was detected in Totolink NR1800X 9.1.0u.6279_B20210910. This affects the function sub_41A68C of the file /cgi-bin/cstecgi.cgi. Performing a manipulation of the argument setUssd results in command injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7503	A vulnerability was detected in code-projects for Plugin 4.1.2cu.5137. The impacted element is the function setWiFiMultipleConfig in the library /lib/cste_modules/wireless.so of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument wepkey2 results in buffer overflow. The attack can be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7551	HKUDS OpenHarness contains a remote code execution vulnerability in the /bridge slash command that allows remote senders accepted by configuration to execute arbitrary operating system commands. Attackers can invoke the /bridge spawn command with attacker-controlled command text that is forwarded to the bridge session manager and executed through the shared shell subprocess helper, allowing them to spawn shell sessions as the OpenHarness process user and access local files, credentials, workspace state, and repository contents.	8.8	More Details
CVE-2026-43018	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: fix potential UAF in hci_le_remote_conn_param_req_evt hci_conn lookup and field access must be covered by hdev lock in hci_le_remote_conn_param_req_evt, otherwise it's possible it is freed concurrently. Extend the hci_dev_lock critical section to cover all conn usage.	8.8	More Details
CVE-2026-7750	A vulnerability was detected in Totolink N300RH 3.2.4-B20220812. This vulnerability affects the function setMacFilterRules of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument mac_address results in buffer overflow. The attack may be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-42434	OpenClaw versions 2026.4.5 before 2026.4.10 contain a sandbox escape vulnerability allowing sandboxed agents to override exec routing by specifying host=node. Attackers can bypass sandbox boundaries and route execution to remote nodes instead of intended sandbox paths.	8.8	More Details
CVE-2026-42435	OpenClaw versions from 2026.2.22 before 2026.4.12 contain an insufficient shell-wrapper detection vulnerability allowing attackers to inject environment variable assignments at the argv level. Attackers can bypass exec preflight handling to manipulate high-risk shell variables like SHELLOPTS and PS4, affecting execution semantics and security controls.	8.8	More Details
CVE-2026-7749	A security vulnerability has been detected in Totolink N300RH 3.2.4-B20220812. This affects the function setWanConfig of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument priDns leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-6963	The WP Mail Gateway plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wmg_save_provider_config AJAX action in all versions up to, and including, 1.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update SMTP settings and redirect mail which can be used for privilege escalation by triggering a password reset email and using that to access and administrator's account.	8.8	More Details
CVE-2026-31706	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate num_aces and harden ACE walk in smb_inherit_dacl() smb_inherit_dacl() trusts the on-disk num_aces value from the parent directory's DACL xattr and uses it to size a heap allocation: aces_base = kmalloc(sizeof(struct smb_ace) * num_aces * 2, ...); num_aces is a u16 read from le16_to_cpu(parent_pdacl->num_aces) without checking that it is consistent with the declared pdacl_size. An authenticated client whose parent directory's security.NTACL is tampered (e.g. via offline xattr corruption or a concurrent path that bypasses parse_dacl()) can present num_aces = 65535 with minimal actual ACE data. This causes a ~8 MB allocation (not kzalloc, so uninitialized) that the subsequent loop only partially populates, and may also overflow the three-way size_t multiply on 32-bit kernels. Additionally, the ACE walk loop uses the weaker offsetof(struct smb_ace, access_req) minimum size check rather than the minimum valid on-wire ACE size, and does not reject ACEs whose declared size is below the minimum. Reproduced on UML + KASAN + LOCKDEP against the real ksmbd code path. A legitimate mount.cifs client creates a parent directory over SMB (ksmbd writes a valid security.NTACL xattr), then the NTACL blob on the backing filesystem is rewritten to set num_aces = 0xFFFF while keeping the posix_acl_hash bytes intact so ksmbd_vfs_get_sd_xattr()'s hash check still passes. A subsequent SMB2 CREATE of a child under that parent drives smb2_open() into smb_inherit_dacl() (share has "vfs objects = acl_xattr" set), which fails the page allocator: WARNING: mm/page_alloc.c:5226 at __alloc_frozen_pages_noprof+0x46c/0x9c0 Workqueue: ksmbd-io handle_ksmbd_work __alloc_frozen_pages_noprof+0x46c/0x9c0 ___kmalloc_large_node+0x68/0x130 __kmalloc_large_node_noprof+0x24/0x70 __kmalloc_noprof+0x4c9/0x690 smb_inherit_dacl+0x394/0x2430 smb2_open+0x595d/0xabe0 handle_ksmbd_work+0x3d3/0x1140 With the patch applied the added guard rejects the tampered value with -EINVAL before any large allocation runs, smb2_open() falls back to smb2_create_sd_buffer(), and the child is created with a default SD. No warning, no splat. Fix by: 1. Validating num_aces against pdacl_size using the same formula applied in parse_dacl(). 2. Replacing the raw kmalloc(sizeof * num_aces * 2) with kmalloc_array(num_aces * 2, sizeof(...)) for overflow-safe allocation. 3. Tightening the per-ACE loop guard to require the minimum valid ACE size (offsetof(smb_ace, sid) + CIFS_SID_BASE_SIZE) and rejecting under-sized ACEs, matching the hardening in smb_check_perm_dacl() and parse_dacl(). v1 -> v2: - Replace the synthetic test-module splat in the changelog with a real-path UML + KASAN reproduction driven through mount.cifs and SMB2 CREATE; Namjae flagged the kcifs3_test_inherit_dacl_old name in v1 since it does not exist in ksmbd. - Drop the commit-hash citation from the code comment per Namjae's review; keep the parse_dacl() pointer.	8.8	More Details
CVE-2026-36956	A Cross-Site Request Forgery (CSRF) vulnerability exists in the web management interface of the Dbit N300 T1 Pro wireless router V1.0.0. The router fails to implement proper CSRF protection mechanisms such as anti-CSRF tokens or strict Origin/Referer validation for administrative API endpoints. An attacker can craft a malicious webpage that sends forged HTTP requests to configuration endpoints such as /api/setWlan. If an authenticated administrator visits the malicious webpage, the victim's browser automatically includes the valid session cookie in the request, allowing the router to process the request as a legitimate administrative action.	8.8	More Details
CVE-2026-2052	The Widget Options – Advanced Conditional Visibility for Gutenberg Blocks & Classic Widgets plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.2.2 via the Display Logic feature. This is due to the plugin using eval() on user-supplied Display Logic expressions with an insufficient blocklist/allowlist that can be bypassed using array_map with string concatenation, combined with a lack of authorization enforcement on the extended_widget_opts_block attribute. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server. The vulnerability was partially patched in version 4.2.0.	8.8	More Details
CVE-2026-36960	A Cross-Site Request Forgery (CSRF) vulnerability exists in the web management interface of the U-SPEED N300 Rounter V1.0.0. The device does not implement CSRF protection mechanisms such as anti-CSRF tokens or strict Origin/Referer validation for administrative API endpoints. An attacker can craft a malicious webpage that sends forged HTTP requests to configuration endpoints. If an authenticated administrator visits the malicious webpage, the victim's browser automatically includes the valid session cookie in the request, allowing the router to process the request as a legitimate administrative action.	8.8	More Details

CVE-2026-7855	A vulnerability was detected in D-Link DI-8100 16.07.26A1. Affected by this issue is the function tggl_asp of the file /tggl.asp of the component HTTP Request Handler. Performing a manipulation of the argument Name results in buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-7607	A security vulnerability has been detected in TRENDnet TEW-821DAP 1.12B01. Impacted is the function auto_update_firmware of the component Firmware Udpate. The manipulation of the argument str leads to buffer overflow. The attack may be initiated remotely. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-7489	CTMS developed by Sunnet has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2026-36762	An issue in the fileEntityId parameter in the /a/file/upload endpoint of JeeSite v5.15.1 allows authenticated attackers with file upload permissions to execute a path traversal and write arbitrary files with whitelisted suffixes to arbitrary filesystem locations.	8.8	More Details
CVE-2026-31717	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate owner of durable handle on reconnect Currently, ksmbd does not verify if the user attempting to reconnect to a durable handle is the same user who originally opened the file. This allows any authenticated user to hijack an orphaned durable handle by predicting or brute-forcing the persistent ID. According to MS-SMB2, the server MUST verify that the SecurityContext of the reconnect request matches the SecurityContext associated with the existing open. Add a durable_owner structure to ksmbd_file to store the original opener's UID, GID, and account name. and catpure the owner information when a file handle becomes orphaned. and implementing ksmbd_vfs_compare_durable_owner() to validate the identity of the requester during SMB2_CREATE (DHnC).	8.8	More Details
CVE-2026-36765	An XML external entity (XXE) vulnerability in the /designer/loadReport endpoint of SpringBlade v4.8.0 allows authenticated attackers to execute arbitrary code via injecting a crafted payload.	8.8	More Details
CVE-2026-31709	In the Linux kernel, the following vulnerability has been resolved: smb: client: validate the whole DACL before rewriting it in cifsacl build_sec_desc() and id_mode_to_cifs_acl() derive a DACL pointer from a server-supplied dacloffset and then use the incoming ACL to rebuild the chmod/chown security descriptor. The original fix only checked that the struct smb_acl header fits before reading dacl_ptr->size or dacl_ptr->num_aces. That avoids the immediate header-field OOB read, but the rewrite helpers still walk ACEs based on pdacl->num_aces with no structural validation of the incoming DACL body. A malicious server can return a truncated DACL that still contains a header, claims one or more ACEs, and then drive replace_sids_and_copy_aces() or set_chmod_dacl() past the validated extent while they compare or copy attacker-controlled ACEs. Factor the DACL structural checks into validate_dacl(), extend them to validate each ACE against the DACL bounds, and use the shared validator before the chmod/chown rebuild paths. parse_dacl() reuses the same validator so the read-side parser and write-side rewrite paths agree on what constitutes a well-formed incoming DACL.	8.8	More Details
CVE-2026-31735	In the Linux kernel, the following vulnerability has been resolved: iommupt: Fix short gather if the unmap goes into a large mapping unmap has the odd behavior that it can unmap more than requested if the ending point lands within the middle of a large or contiguous IOPTE. In this case the gather should flush everything unmapped which can be larger than what was requested to be unmapped. The gather was only flushing the range requested to be unmapped, not extending to the extra range, resulting in a short invalidation if the caller hits this special condition. This was found by the new invalidation/gather test I am adding in preparation for ARMv8. Claude deduced the root cause. As far as I remember nothing relies on unmapping a large entry, so this is likely not a triggerable bug.	8.8	More Details
CVE-2026-6261	The Betheme theme for WordPress is vulnerable to Arbitrary File Upload in versions up to, and including, 28.4. This is due to the upload_icons() function workflow moving and unzipping user-controlled ZIP files into a public uploads directory without validating extracted file types. This makes it possible for authenticated attackers, with author-level access and above, to upload arbitrary files (including PHP) and achieve remote code execution via the Icons icon-pack upload flow.	8.8	More Details
CVE-2026-42468	Buffer overflow vulnerability in Open Vehicle Monitoring System 3 (OVMS3) 3.3.005. In canformat_pcap.cpp , the parser's phdr.len field is not properly validated, allowing remote attackers to cause a denial of service or possibly execute arbitrary code via crafted PCAP input.	8.8	More Details
CVE-2026-43571	OpenClaw before 2026.4.10 contains a plugin trust bypass vulnerability that allows channel setup catalog lookups to resolve workspace plugin shadows before bundled channel plugins. Attackers can exploit this by crafting malicious workspace plugins that bypass intended trust gates during setup-time plugin loading.	8.8	More Details
CVE-2026-7748	A weakness has been identified in Totolink N300RH 3.2.4-B20220812. Affected by this issue is the function setUpgradeFW of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. Executing a manipulation of the argument FileName can lead to buffer overflow. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-5402	TLS protocol dissector heap overflow in Wireshark 4.6.0 to 4.6.4 allows denial of service and possible code execution	8.8	More Details
CVE-2026-7717	A vulnerability was determined in Totolink WA300 5.2cu.7112_B20190227. This issue affects the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. Executing a manipulation of the argument File can lead to buffer overflow. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-37536	miaofng/uds-c commit e506334e270d77b20c0bc259ac6c7d8c9b702b7a (2016-10-05) contains a stack buffer overflow in send_diagnostic_request. A 6-byte stack buffer (MAX_DIAGNOSTIC_PAYLOAD_SIZE=6) receives memcpy at offset 1+pid_length with payload_length bytes. MAX_UDS_REQUEST_PAYLOAD_LENGTH=7, so 1+2+7=10 exceeds buffer by 4 bytes. No bounds check on payload_length before memcpy.	8.8	More Details
CVE-2026-7685	A vulnerability was detected in Edimax BR-6208AC up to 1.02. Affected is an unknown function of the file /goform/setWAN. Performing a manipulation of the argument pptpDfGateway results in buffer overflow. The attack may 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.	8.8	More Details
CVE-2026-7684	A security vulnerability has been detected in Edimax BR-6428nC up to 1.16. This impacts an unknown function of the file /goform/setWAN. Such manipulation of the argument pptpDfGateway leads to buffer overflow. The attack can be launched 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.	8.8	More Details

CVE-2026-43530	OpenClaw versions 2026.2.23 before 2026.4.12 contain a weakened exec approval binding vulnerability in busybox and toybox applet execution that allows attackers to obscure which applet would actually run. Attackers can exploit opaque multi-call binaries to bypass exec approval mechanisms and weaken risk classification of unsafe applet invocations.	8.8	More Details
CVE-2026-31739	In the Linux kernel, the following vulnerability has been resolved: crypto: tegra - Add missing CRYPTO_ALG_ASYNC The tegra crypto driver failed to set the CRYPTO_ALG_ASYNC on its asynchronous algorithms, causing the crypto API to select them for users that request only synchronous algorithms. This causes crashes (at least). Fix this by adding the flag like what the other drivers do. Also remove the unnecessary CRYPTO_ALG_TYPE_* flags, since those just get ignored and overridden by the registration function anyway.	8.8	More Details
CVE-2026-7675	A vulnerability has been found in Shenzhen Libituo Technology LBT-T300-HW1 up to 1.2.8. Impacted is the function start_lan of the file /apply.cgi. The manipulation of the argument Channel/ApCliSsid leads to buffer overflow. The attack is possible to be carried out remotely. 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.	8.8	More Details
CVE-2026-7674	A flaw has been found in Shenzhen Libituo Technology LBT-T300-HW1 up to 1.2.8. This issue affects the function start_single_service of the component Web Management Interface. Executing a manipulation of the argument vpn_pptp_server/vpn_l2tp_server can lead to buffer overflow. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-43569	OpenClaw before 2026.4.9 contains an authentication bypass vulnerability allowing untrusted workspace plugins to be auto-enabled during non-interactive onboarding when provider auth choices are shadowed. Attackers can exploit this by crafting malicious workspace plugins that are automatically selected and enabled during authentication setup without explicit user consent.	8.8	More Details
CVE-2026-7513	A vulnerability has been found in UTT HiPER 1200GW up to 2.5.3-170306. The impacted element is the function strcpy of the file /goform/formRemoteControl. The manipulation leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-35228	Vulnerability in the Oracle MCP Server Helper Tool product of Oracle Open Source Projects (component: helper tool). The supported versions that is affected is 1.0.1-1.0.156. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle MCP Server Helper Tool. Successful attacks of this vulnerability can result in Oracle MCP Server Helper Tool executing malicious SQL.	8.7	More Details
CVE-2026-42365	A guessable session cookie vulnerability exists in the Web Interface functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted series of HTTP requests can lead to an authentication bypas. An attacker can bruteforce session cookies to trigger this vulnerability.	8.6	More Details
CVE-2026-42469	Buffer overflow vulnerability in Open Vehicle Monitoring System 3 (OVMS3) 3.3.005. In canformat_canswitch.cpp the parser does not properly validate a CANswitch DLC value, allowing remote attackers to cause a denial of service or possibly execute arbitrary code via crafted CANswitch frames.	8.6	More Details
CVE-2026-42079	PPTAgent is an agentic framework for reflective PowerPoint generation. Prior to commit 418491a, PPTAgent is vulnerable to arbitrary code execution via Python eval() of LLM-generated code with builtins in scope. This issue has been patched via commit 418491a.	8.6	More Details
CVE-2026-43533	OpenClaw before 2026.4.10 contains an arbitrary file read vulnerability in QQBot media tags that allows attackers to reference host-local paths outside the intended media storage boundary. Attackers can craft malicious reply text containing media tags to disclose arbitrary local files through outbound media handling.	8.6	More Details
CVE-2026-7412	In Eclipse BaSyx Java Server SDK versions prior to 2.0.0-milestone-10, the Operation Delegation feature fails to validate the destination URI of delegated requests. An unauthenticated remote attacker can exploit this design flaw to force the BaSyx server to execute blind HTTP POST requests to arbitrary internal or external targets. This allows an attacker to bypass network segmentation and pivot into isolated internal IT/OT infrastructure or target Cloud Metadata services (IMDS).	8.6	More Details
CVE-2026-42439	OpenClaw before 2026.4.10 contains a server-side request forgery policy bypass vulnerability in the browser tabs action select and close routes. Attackers can bypass configured browser SSRF policy protections by exploiting the /tabs/action endpoint to perform unauthorized tab navigation operations.	8.5	More Details
CVE-2026-37552	Unsafe deserialization vulnerability in MixPHP Framework 2.x thru 2.2.17. The sync-invoke TCP server (Server.php:87) receives data from a TCP socket, passes it directly to Opis\Closure\unserialize(), then executes the result via call_user_func(). No authentication or signature verification exists on the TCP connection. An attacker with access to the localhost TCP port (server binds 127.0.0.1) can send a crafted serialized PHP closure to achieve arbitrary code execution.	8.4	More Details
CVE-2018-25315	Alloksoft Video joiner 4.6.1217 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string in the License Name field. Attackers can craft a payload with structured exception handler (SEH) overwrite and shellcode to achieve code execution when the application processes the license registration input.	8.4	More Details
CVE-2018-25314	Allok soft WMV to AVI MPEG DVD WMV Converter 4.6.1217 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized string in the License Name field. Attackers can craft a malicious input containing shellcode with structured exception handler (SEH) overwrite to bypass protections and execute code with application privileges.	8.4	More Details
CVE-2026-7111	Text::CSV_XS versions before 1.62 for Perl have a use-after-free when registered callbacks extend the Perl argument stack, which may enable type confusion or memory corruption. The Parse, print, getline, and getline_all methods invoke registered callbacks (for example after_parse, before_print, or on_error) and cache the Perl argument stack pointer across the call. If a callback extends the argument stack enough to trigger a reallocation, the return value is written through the stale pointer into the freed buffer, and the caller reads the original $self argument as the return value instead. Calling code that expects parsed data from getline_all receives the Text::CSV_XS object in its place, leading to logic errors or crashes. Text::CSV_XS objects used without any registered callbacks are not affected.	8.4	More Details
CVE-2018-25307	SysGauge Pro 4.6.12 contains a local buffer overflow vulnerability in the Register function that allows local attackers to overwrite the structured exception handler by supplying a crafted unlock key. Attackers can inject shellcode through the Unlock Key field during registration to execute arbitrary code with application privileges.	8.4	More Details
CVE-2018-25304	Free Download Manager 2.0 Built 417 contains a local buffer overflow vulnerability in the URL import functionality that allows attackers to trigger a structured exception handler (SEH) chain exploitation. Attackers can craft a malicious URL file that, when imported through the File > Import > Import lists of downloads menu, causes a buffer overflow in the Location header response that	8.4	More Details

	overwrites the SEH chain and executes arbitrary code.		
CVE-2018-25303	Allok Video to DVD Burner 2.6.1217 contains a stack-based buffer overflow vulnerability in the License Name field that allows local attackers to execute arbitrary code by triggering a structured exception handler (SEH) overwrite. Attackers can craft a malicious input string with 780 bytes of junk data followed by SEH chain pointers and shellcode, then paste it into the License Name field during registration to achieve code execution.	8.4	More Details
CVE-2018-25301	Easy MPEG to DVD Burner 1.7.11 contains a structured exception handling (SEH) local buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious username string. Attackers can craft a payload containing junk data, SEH chain pointers, and shellcode that overwrites the SEH handler to redirect execution and run arbitrary commands like opening calc.exe.	8.4	More Details
CVE-2026-37540	OpenAMP v2025.10.0 ELF loader contains an integer overflow vulnerability in firmware image parsing. In elf_loader.c, it performs multiplication of two attacker-controlled 16-bit values from the ELF header without overflow checking. On 32-bit embedded systems (STM32MP1, Zynq, i.MX), large values can cause the product to wrap around to a small value.	8.4	More Details
CVE-2018-25299	Prime95 29.4b8 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting structured exception handling (SEH) mechanisms. Attackers can inject malicious payload through the optional proxy hostname field in the PrimeNet connection settings to trigger the overflow and execute system commands.	8.4	More Details
CVE-2026-30363	flipperzero-firmware commit ad2a80 was discovered to contain a stack overflow in the "Main" function.	8.4	More Details
CVE-2026-31712	In the Linux kernel, the following vulnerability has been resolved: ksmbd: require minimum ACE size in smb_check_perm_dacl() Both ACE-walk loops in smb_check_perm_dacl() only guard against an under-sized remaining buffer, not against an ACE whose declared `ace->size` is smaller than the struct it claims to describe: if (offsetof(struct smb_ace, access_req) > aces_size) break; ace_size = le16_to_cpu(ace->size); if (ace_size > aces_size) break; The first check only requires the 4-byte ACE header to be in bounds; it does not require access_req (4 bytes at offset 4) to be readable. An attacker who has set a crafted DACL on a file they own can declare ace->size == 4 with aces_size == 4, pass both checks, and then granted |= le32_to_cpu(ace->access_req); /* upper loop */ compare_sids(&sid, &ace->sid); /* lower loop */ reads access_req at offset 4 (OOB by up to 4 bytes) and ace->sid at offset 8 (OOB by up to CIFS_SID_BASE_SIZE + SID_MAX_SUB_AUTHORITIES * 4 bytes). Tighten both loops to require ace_size >= offsetof(struct smb_ace, sid) + CIFS_SID_BASE_SIZE which is the smallest valid on-wire ACE layout (4-byte header + 4-byte access_req + 8-byte sid base with zero sub-auths). Also reject ACEs whose sid.num_subauth exceeds SID_MAX_SUB_AUTHORITIES before letting compare_sids() dereference sub_auth[] entries. parse_sec_desc() already enforces an equivalent check (lines 441-448); smb_check_perm_dacl() simply grew weaker validation over time. Reachability: authenticated SMB client with permission to set an ACL on a file. On a subsequent CREATE against that file, the kernel walks the stored DACL via smb_check_perm_dacl() and triggers the OOB read. Not pre-auth, and the OOB read is not reflected to the attacker, but KASAN reports and kernel state corruption are possible.	8.3	More Details
CVE-2026-6266	A flaw was found in the AAP gateway. The user auto-link strategy, introduced in AAP 2.6, automatically links an external Identity Provider (IDP) identity to an existing AAP user account based on email matching without verifying email ownership. This allows a remote attacker to potentially hijack a victim's account or gain unauthorized access to other accounts, including administrative accounts, by manipulating the IDP-provided email.	8.3	More Details
CVE-2026-43526	OpenClaw before 2026.4.12 contains a server-side request forgery vulnerability in QQBot reply media URL handling that allows attackers to fetch arbitrary content. Attackers can exploit this by providing malicious media URLs that trigger SSRF requests, with fetched bytes subsequently re-uploaded through the channel.	8.2	More Details
CVE-2018-25300	XATABoost CMS 1.0.0 contains a union-based SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the id parameter. Attackers can send GET requests to news.php with malicious id values to extract sensitive database information.	8.2	More Details
CVE-2026-40912	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is a high severity authentication bypass vulnerability in Traefik's StripPrefixRegex middleware when used in combination with ForwardAuth, BasicAuth, or DigestAuth. The middleware matches the regex against the decoded URL path but uses the resulting byte length to slice the percent-encoded raw path. When a dot (or multiple dots) appears in the prefix portion of the URL, the raw path after stripping becomes a dot-segment (e.g. /./admin/secret). ForwardAuth receives this dot-segment path in X-Forwarded-Uri, which does not match the protected path patterns and therefore allows the request through. The backend then normalizes the dot-segment to the real path per RFC 3986 and serves the protected content An unauthenticated attacker can exploit this against any backend that performs dot-segment normalization. This issue has been patched in versions 2.11.43, 3.6.14, and 3.7.0-rc.2.	8.2	More Details
CVE-2026-2554	The WCFM – Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.7.25 via the 'wcfm_delete_wcfm_customer' due to missing validation on the 'customerid' user controlled key. This makes it possible for authenticated attackers, with Vendor-level access and above, to delete arbitrary users, including Administrators.	8.1	More Details
CVE-2026-42471	Unsafe deserialization vulnerability in MixPHP Framework 2.x thru 2.2.17. The sync-invoke client (Connection.php:76) calls unserialize() on data received from the server response, enabling client-side RCE if connecting to a malicious server.	8.1	More Details
CVE-2026-43051	In the Linux kernel, the following vulnerability has been resolved: HID: wacom: fix out-of-bounds read in wacom_intuos_bt_irq The wacom_intuos_bt_irq() function processes Bluetooth HID reports without sufficient bounds checking. A maliciously crafted short report can trigger an out-of-bounds read when copying data into the wacom structure. Specifically, report 0x03 requires at least 22 bytes to safely read the processed data and battery status, while report 0x04 (which falls through to 0x03) requires 32 bytes. Add explicit length checks for these report IDs and log a warning if a short report is received.	8.1	More Details
CVE-2026-36340	An issue in Krayin CRM v.2.1.5 and fixed in v.2.1.6 allows a remote attacker to execute arbitrary code via the compose email function	8.1	More Details
CVE-2026-7402	Improper Control of Interaction Frequency vulnerability in MeWare Software Development Inc. PDKS allows Flooding. This issue affects PDKS: from V16.20200313 before VMYR_3.5.2025117.	8.1	More Details

CVE-2026-22165	A web page that contains unusual WebGPU content loaded into the GPU GLES render process and can trigger a write UAF crash in the GPU GLES user-space shared library. On certain platforms, when the process executing graphics workload has system privileges this could enable further exploits on the device.	8.1	More Details
CVE-2026-22166	A web page that contains unusual WebGPU content loaded into the GPU GLES render process and can trigger write UAF crash in the GPU GLES user-space shared library. On certain platforms, when the process executing graphics workload has system privileges this could enable subsequent exploit on the system.	8.1	More Details
CVE-2026-42511	The BOOTP file field is written to the lease file without escaping embedded double-quotes, allowing injection of arbitrary dhclient.conf directives. When the lease file is subsequently re-parsed by dhclient, e.g., after a system restart, an attacker-controlled field from the lease is passed to dhclient-script(8), which evaluates it. A rogue DHCP server may be able to execute arbirary code as root on a system running dhclient.	8.1	More Details
CVE-2026-29199	phpBB before 3.3.16 is vulnerable to Host Header Injection that can lead to password rest link poisoning. When force_server_vars is disabled, the servers hostname may be extracted from the HTTP Host header which is used to generate the password reset link URL. An attacker who can manipulate the Host header (e.g. through misconfigured host setup or missing header validation by the webserver) can cause password reset emails to contain a link pointing to an attacker-controlled domain, potentially leading to account takeover.	8.1	More Details
CVE-2026-7399	Authorization bypass through User-Controlled key vulnerability in MeWare Software Development Inc. PDKS allows Privilege Abuse. This issue affects PDKS: from V16.20200313 before VMYR_3.5.2025117.	8.1	More Details
CVE-2026-40600	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew allows authenticated users with access to one project to update or delete a SharePolicy record that belongs to a different project. The affected routes authorize the caller against the project in the URL path, but they never verify that policy_id belongs to that project. This permits cross-project modification of dashboard sharing rules, including visibility, password requirements, allowed parameters, and expiration settings. This issue has been patched in version 5.0.0.	8.1	More Details
CVE-2026-44331	In ProFTPD through 1.3.9a before 7666224, a SQL injection vulnerability in sqltab_fetch_clients_cb() in contrib/mod_wrap2_sql.c allows a remote attacker to inject arbitrary SQL commands via a crafted domain name that is accessed in a reverse DNS lookup. When "UseReverseDNS on" is enabled, the attacker-supplied hostname is passed unescaped into SQL queries. The character restrictions of DNS names may affect exploitability.	8.1	More Details
CVE-2026-7491	School App developed by Zyosoft has an Insecure Direct Object Reference vulnerability, allowing authenticated remote attackers to modify a specific parameter to read and modify other users' data.	8.1	More Details
CVE-2026-42512	As dhclient is building an environment to pass to dhclient-script, it may need to resize the array of string pointers. The code which expands the array incorrectly calculates its new size when requesting memory, resulting in a heap buffer overrun. A specially crafted packet can cause dhclient to overrun its buffer of environment entries. This can result in a crash, but it may be possible to leverage this bug to achieve remote code execution.	8.1	More Details
CVE-2026-42075	Evolver is a GEP-powered self-evolving engine for AI agents. Prior to version 1.69.3, a path traversal vulnerability in the skill download (fetch) command allows attackers to write files to arbitrary locations on the filesystem. The --out= flag accepts user-provided paths without validation, enabling directory traversal attacks that can overwrite critical system files or create files in sensitive location. This issue has been patched in version 1.69.3.	8.1	More Details
CVE-2026-37537	collin80/Open-SAE-J1939 thru commit 744024d4306bc387857dfce439558336806acb06 (2023-03-08) contains an integer underflow leading to out-of-bounds write in Transport Protocol Data Transfer handling. At line 23: uint8_t index = data[0] - 1. When data[0] (sequence number from CAN frame) is 0, index underflows to 255. Subsequent write at tp_dt->data[255*7 + i-1] reaches offset 1791, exceeding the MAX_TP_DT buffer (1785 bytes) by 6 bytes.	8.1	More Details
CVE-2026-40904	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes multiple dataset and dataRequest endpoints that authorize low-privileged project members at the team level instead of binding the requested dataset_id, dataRequest id, and connection_id to the caller's allowed projects. An authenticated attacker who only has access to one project inside a team can read, execute, create, update, and delete datasets and data requests that belong to other projects in the same team. The issue is exploitable remotely with ordinary project-level credentials and leads to cross-project data disclosure and unauthorized use of victim-side database or API connections. This issue has been patched in version 5.0.0.	8.1	More Details
CVE-2026-35547	When processing the header of an incoming message, libnv failed to properly validate the message size. The lack of validation allows a malicious program to write outside the bounds of a heap allocation. This can trigger a crash or system panic, and it may be possible for an unprivileged user to exploit the bug to elevate their privileges.	8.1	More Details
CVE-2026-7426	Insufficient validation of the prefix length field in IPv6 Router Advertisement processing in FreeRTOS-Plus-TCP before V4.2.6 and V4.4.1 allows an adjacent network actor to cause memory corruption by sending a crafted Router Advertisement with a prefix length value exceeding the maximum valid length, resulting in a heap buffer overflow. Users processing IPv4 RA only are not impacted. To mitigate this issue, users should upgrade to the fixed version when available.	8.1	More Details
CVE-2026-31708	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix OOB read in smb2_ioctl_query_info QUERY_INFO path smb2_ioctl_query_info() has two response-copy branches: PASSTHRU_FSCTL and the default QUERY_INFO path. The QUERY_INFO branch clamps qi.input_buffer_length to the server-reported OutputBufferLength and then copies qi.input_buffer_length bytes from qi_rsp->Buffer to userspace, but it never verifies that the flexible-array payload actually fits within rsp_iov[1].iov_len. A malicious server can return OutputBufferLength larger than the actual QUERY_INFO response, causing copy_to_user() to walk past the response buffer and expose adjacent kernel heap to userspace. Guard the QUERY_INFO copy with a bounds check on the actual Buffer payload. Use struct_size(qi_rsp, Buffer, qi.input_buffer_length) rather than an open-coded addition so the guard cannot overflow on 32-bit builds.	8.1	More Details
CVE-2026-31779	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix potential out-of-bounds read in iwl_mvm_nd_match_info_handler() The memcpy function assumes the dynamic array notif->matches is at least as large as the number of bytes to copy. Otherwise, results->matches may contain unwanted data. To guarantee safety, extend the validation in one of the checks to ensure sufficient packet length. Found by Linux Verification Center (linuxtesting.org) with SVACE.	8.1	More Details
CVE-			

2026-42222	Nginx UI is a web user interface for the Nginx web server. In version 2.3.5, an unauthenticated bootstrap takeover exists in nginx-ui during the initial installation window exposed by POST /api/install. At time of publication no public patches are available.	8.1	More Details
CVE-2026-29004	BusyBox before commit 42202bf contains a heap buffer overflow vulnerability in the DHCPv6 client (udhcpc6) DNS_SERVERS option handler in networking/udhcp/d6_dhcpc.c that allows network-adjacent attackers to trigger memory corruption by sending a crafted DHCPv6 response with a malformed D6_OPT_DNS_SERVERS option. Attackers can exploit incorrect heap buffer allocation calculations in the option_to_env() function to cause denial of service or achieve arbitrary code execution on embedded systems without heap hardening.	8.1	More Details
CVE-2026-42221	Nginx UI is a web user interface for the Nginx web server. From version 2.0.0 to before version 2.3.8, an unauthenticated network attacker can claim the initial administrator account on a fresh nginx-ui instance during the first-run setup window. The public /api/install endpoint is reachable without authentication, and the request-encryption flow only protects payload confidentiality in transit; it does not authenticate who is allowed to perform installation. A remote attacker who reaches the service before the legitimate operator can set the admin email, username, and password, causing permanent initial-instance takeover. This issue has been patched in version 2.3.8.	8.1	More Details
CVE-2026-7647	The Profile Builder Pro plugin for WordPress is vulnerable to PHP Object Injection in all versions up to and including 3.14.5. This is due to the use of PHP's maybe_unserialize() function on the attacker-controlled 'args' POST parameter within the wppb_request_users_pins_action_callback() AJAX handler, which lacked any nonce verification, type checking, or input validation before deserialization. Because the handler was registered with both wp_ajax_ and wp_ajax_nopriv_ hooks, it was reachable by completely unauthenticated users. This makes it possible for unauthenticated attackers to inject arbitrary PHP objects into application memory.	8.1	More Details
CVE-2026-31771	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: move wake reason storage into validated event handlers hci_store_wake_reason() is called from hci_event_packet() immediately after stripping the HCI event header but before hci_event_func() enforces the per-event minimum payload length from hci_ev_table. This means a short HCI event frame can reach bacpy() before any bounds check runs. Rather than duplicating skb parsing and per-event length checks inside hci_store_wake_reason(), move wake-address storage into the individual event handlers after their existing event-length validation has succeeded. Convert hci_store_wake_reason() into a small helper that only stores an already-validated bdaddr while the caller holds hci_dev_lock(). Use the same helper after hci_event_func() with a NULL address to preserve the existing unexpected-wake fallback semantics when no validated event handler records a wake address. Annotate the helper with __must_hold(&hdev->lock) and add lockdep_assert_held(&hdev->lock) so future call paths keep the lock contract explicit. Call the helper from hci_conn_request_evt(), hci_conn_complete_evt(), hci_sync_conn_complete_evt(), le_conn_complete_evt(), hci_le_adv_report_evt(), hci_le_ext_adv_report_evt(), hci_le_direct_adv_report_evt(), hci_le_pa_sync_established_evt(), and hci_le_past_received_evt().	8.1	More Details
CVE-2026-42084	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. Prior to versions 6.10.5 and 7.0.0-rc3, the OpenC3 password change functionality allows a user to change their password without providing the old password, by accepting a valid session token instead. In assumed breach scenarios, this behaviour can be exploited by an attacker who has already obtained a valid session token, to gain persistence in hijacked account (including admin) and prevent legitimate users from accessing the account. This issue has been patched in versions 6.10.5 and 7.0.0-rc3.	8.1	More Details
CVE-2026-7424	Integer underflow in the DHCPv6 sub-option parser in FreeRTOS-Plus-TCP before V4.4.1 and V4.2.6 allows an adjacent network actor to corrupt the device's IPv6 address assignment, DNS configuration, and lease times, and to cause a denial of service (permanent IP task freeze requiring hardware reset) by sending a single crafted DHCPv6 packet. The issue is present whenever DHCPv6 is enabled. To mitigate this issue, users should upgrade to version V4.2.6 or V4.4.1 or newer.	8.1	More Details
CVE-2025-67796	IKUS Rdiffweb before 2.10.5 has an improper authorization flaw that allows an attacker with any valid or stolen access token to act as other users. The API does not enforce binding between the authenticated subject and the targeted user/tenant, so crafted requests can read or modify other users data and, in some cases, perform privileged actions. This issue may enable cross-tenant access. Fixed in version 2.10.6.	8.1	More Details
CVE-2026-5712	This vulnerability impacts all versions of IdentityIQ and allows an authenticated identity that is the requestor or assignee of a work item to edit the definition of a role without having an assigned capability that would allow role editing.	8.0	More Details
CVE-2026-0204	A vulnerability in the access control mechanism of SonicOS may allow certain management interface functions to be accessible under specific conditions.	8.0	More Details
CVE-2026-43003	An issue was discovered in OpenStack ironic-python-agent 1.0.0 through 11.5.0. Ironic Python Agent (IPA) sometimes executes grub-install from within a chroot of the deployed partition image, leading to code execution in the case of a malicious image.	8.0	More Details
CVE-2026-42524	Jenkins HTML Publisher Plugin 427 and earlier does not escape job name and URL in the legacy wrapper file, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	8.0	More Details
CVE-2026-43001	An issue was discovered in OpenStack Keystone 13 through 29. POST /v3/credentials did not validate that the caller-supplied project_id for an EC2-type credential matched the project of the authenticating application credential. This allowed an attacker holding an unrestricted application credential for project A to create an EC2 credential targeting project B; a subsequent /v3/ec2tokens exchange would then issue a Keystone token scoped to project B while still carrying the original app_cred_id, enabling cross-project lateral movement within the credential owner's role footprint.	7.9	More Details
CVE-2026-43023	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SCO: fix race conditions in sco_sock_connect() sco_sock_connect() checks sk_state and sk_type without holding the socket lock. Two concurrent connect() syscalls on the same socket can both pass the check and enter sco_connect(), leading to use-after-free. The buggy scenario involves three participants and was confirmed with additional logging instrumentation: Thread A (connect): HCI disconnect: Thread B (connect): sco_sock_connect(sk) sco_sock_connect(sk) sk_state==BT_OPEN sk_state==BT_OPEN (pass, no lock) (pass, no lock) sco_connect(sk): sco_connect(sk): hci_dev_lock hci_dev_lock hci_connect_sco <- blocked -> hcon1 sco_conn_add->conn1 lock_sock(sk) sco_chan_add: conn1->sk = sk sk->conn = conn1 sk_state=BT_CONNECT release_sock hci_dev_unlock hci_dev_lock sco_conn_del: lock_sock(sk) sco_chan_del: sk->conn=NULL conn1->sk=NULL sk_state= BT_CLOSED SOCK_ZAPPED release_sock hci_dev_unlock (unblocked) hci_connect_sco -> hcon2 sco_conn_add -> conn2 lock_sock(sk) sco_chan_add: sk->conn=conn2 sk_state= BT_CONNECT // zombie sk! release_sock hci_dev_unlock Thread B revives a BT_CLOSED + SOCK_ZAPPED socket back to BT_CONNECT. Subsequent cleanup triggers double sock_put() and use-after-free. Meanwhile conn1 is leaked as it was orphaned when sco_conn_del() cleared the association. Fix this by:	7.8	More Details

	- Moving lock_sock() before the sk_state/sk_type checks in sco_sock_connect() to serialize concurrent connect attempts - Fixing the sk_type != SOCK_SEQPACKET check to actually return the error instead of just assigning it - Adding a state re-check in sco_connect() after lock_sock() to catch state changes during the window between the locks - Adding sco_pi(sk)->conn check in sco_chan_add() to prevent double-attach of a socket to multiple connections - Adding hci_conn_drop() on sco_chan_add failure to prevent HCI connection leaks		
CVE-2026-43033	In the Linux kernel, the following vulnerability has been resolved: crypto: authencesn - Do not place hiseq at end of dst for out-of-place decryption When decrypting data that is not in-place (src != dst), there is no need to save the high-order sequence bits in dst as it could simply be re-copied from the source. However, the data to be hashed need to be rearranged accordingly. Thanks,	7.8	More Details
CVE-2026-31780	In the Linux kernel, the following vulnerability has been resolved: wifi: wilc1000: fix u8 overflow in SSID scan buffer size calculation The variable valuesize is declared as u8 but accumulates the total length of all SSIDs to scan. Each SSID contributes up to 33 bytes (IEEE80211_MAX_SSID_LEN + 1), and with WILC_MAX_NUM_PROBED_SSID (10) SSIDs the total can reach 330, which wraps around to 74 when stored in a u8. This causes kmalloc to allocate only 75 bytes while the subsequent memcpy writes up to 331 bytes into the buffer, resulting in a 256-byte heap buffer overflow. Widen valuesize from u8 to u32 to accommodate the full range.	7.8	More Details
CVE-2026-31772	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: fix stack buffer overflow in hci_le_big_create_sync hci_le_big_create_sync() uses DEFINE_FLEX to allocate a struct hci_cp_le_big_create_sync on the stack with room for 0x11 (17) BIS entries. However, conn->num_bis can hold up to HCI_MAX_ISO_BIS (31) entries — validated against ISO_MAX_NUM_BIS (0x1f) in the caller hci_conn_big_create_sync(). When conn->num_bis is between 18 and 31, the memcpy that copies conn->bis into cp->bis writes up to 14 bytes past the stack buffer, corrupting adjacent stack memory. This is trivially reproducible: binding an ISO socket with bc_num_bis = ISO_MAX_NUM_BIS (31) and calling listen() will eventually trigger hci_le_big_create_sync() from the HCI command sync worker, causing a KASAN-detectable stack-out-of-bounds write: BUG: KASAN: stack-out-of-bounds in hci_le_big_create_sync+0x256/0x3b0 Write of size 31 at addr ffffc90000487b48 by task kworker/u9:0/71 Fix this by changing the DEFINE_FLEX count from the incorrect 0x11 to HCI_MAX_ISO_BIS, which matches the maximum number of BIS entries that conn->bis can actually carry.	7.8	More Details
CVE-2018-25302	Allok AVI to DVD SVCD VCD Converter 4.0.1217 contains a structured exception handling (SEH) based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string in the License Name field. Attackers can craft a payload with junk data, NSEH bypass, SEH handler address, and shellcode that triggers the overflow when pasted into the License Name field and the Register button is clicked, resulting in code execution.	7.8	More Details
CVE-2026-33451	CVE-2026-33451 is an arbitrary read/write vulnerability in the Secure Access Windows client prior to 14.50. Attackers with local control of the Windows client can send malformed data to an API and elevate their level of privilege to system.	7.8	More Details
CVE-2026-37526	AGL app-framework-binder (afb-daemon) through v19.90.0 allows any local process to execute privileged supervision commands (Exit, Do, Sclose, Config, Trace, Debug, Token, slist) without authentication via the abstract Unix socket @urn:AGL:afs:supervision:socket. The on_supervision_call function in src/afb-supervision.c dispatches all 8 commands without any credential verification. The abstract socket has no DAC protection, as acknowledged in the official CAUTION comment in src/afs-supervision.h. This allows a low-privileged local process to kill the daemon (DoS via Exit command), execute arbitrary API calls (via Do command), close arbitrary user sessions (via Sclose command), or leak the entire global configuration (via Config command). The vulnerability was introduced in commit b8c9d5de384efcfa53ebdb3f0053d7b3723777e1 on 2017-06-29.	7.8	More Details
CVE-2026-31700	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix TOCTOU race on mmap'd vnet_hdr in tpacket_snd() In tpacket_snd(), when PACKET_VNET_HDR is enabled, vnet_hdr points directly into the mmap'd TX ring buffer shared with userspace. The kernel validates the header via __packet_snd_vnet_parse() but then re-reads all fields later in virtio_net_hdr_to_skb(). A concurrent userspace thread can modify the vnet_hdr fields between validation and use, bypassing all safety checks. The non-TPACKET path (packet_snd()) already correctly copies vnet_hdr to a stack-local variable. All other vnet_hdr consumers in the kernel (tun.c, tap.c, virtio_net.c) also use stack copies. The TPACKET TX path is the only caller of virtio_net_hdr_to_skb() that reads directly from user-controlled shared memory. Fix this by copying vnet_hdr from the mmap'd ring buffer to a stack-local variable before validation and use, consistent with the approach used in packet_snd() and all other callers.	7.8	More Details
CVE-2026-31782	In the Linux kernel, the following vulnerability has been resolved: perf/x86: Fix potential bad container_of in intel_pmu_hw_config Auto counter reload may have a group of events with software events present within it. The software event PMU isn't the x86_hybrid_pmu and a container_of operation in intel_pmu_set_acr_caused_constr (via the hybrid helper) could cause out of bound memory reads. Avoid this by guarding the call to intel_pmu_set_acr_caused_constr with an is_x86_event check.	7.8	More Details
CVE-2026-7270	An operator precedence bug in the kernel results in a scenario where a buffer overflow causes attacker-controlled data to overwrite adjacent execve(2) argument buffers. The bug may be exploitable by an unprivileged user to obtain superuser privileges.	7.8	More Details
CVE-2026-43019	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: fix potential UAF in set_cig_params_sync hci_conn lookup and field access must be covered by hdev lock in set_cig_params_sync, otherwise it's possible it is freed concurrently. Take hdev lock to prevent hci_conn from being deleted or modified concurrently. Just RCU lock is not suitable here, as we also want to avoid "tearing" in the configuration.	7.8	More Details
CVE-2026-39457	When exchanging data over a socket, libnv uses select(2) to wait for data to arrive. However, it does not verify whether the provided socket descriptor fits in select(2)'s file descriptor set size limit of FD_SETSIZE (1024). An attacker who is able to force a libnv application to allocate large file descriptors, e.g., by opening many descriptors and executing a program which is not careful to close them upon startup, can trigger stack corruption. If the target application is setuid-root, then this could be used to elevate local privileges.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: bpf: sockmap: Fix use-after-free of sk->sk_socket in sk_psock_verdict_data_ready(). syzbot reported use-after-free of AF_UNIX socket's sk->sk_socket in sk_psock_verdict_data_ready(). [0] In unix_stream_sendmsg(), the peer socket's ->sk_data_ready() is called after dropping its unix_state_lock(). Although the sender socket holds the peer's refcount, it does not prevent the peer's sock_orphan(), and the peer's sk_socket might be freed after one RCU grace period. Let's fetch the peer's sk->sk_socket and sk->sk_socket->ops under RCU in sk_psock_verdict_data_ready(). [0]: BUG: KASAN: slab-use-after-free in sk_psock_verdict_data_ready+0xec/0x590 net/core/skmsg.c:1278 Read of size 8 at addr ffff8880594da860 by task syz.4.1842/11013 CPU: 1 UID: 0 PID: 11013 Comm: syz.4.1842 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2026 Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xba/0x230 mm/kasan/report.c:482 kasan_report+0x117/0x150 mm/kasan/report.c:595 sk_psock_verdict_data_ready+0xec/0x590 net/core/skmsg.c:1278 unix_stream_sendmsg+0x8a3/0xe80 net/unix/af_unix.c:2482		

CVE-2026-43016	sock_sendmsg_nosec net/socket.c:721 [inline] __sock_sendmsg net/socket.c:736 [inline] ____sys_sendmsg+0x972/0x9f0 net/socket.c:2585 ___sys_sendmsg+0x2a5/0x360 net/socket.c:2639 __sys_sendmsg net/socket.c:2671 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x1bd/0x2a0 net/socket.c:2674 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7facf899c819 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:00007facf9827028 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007facf8c15fa0 RCX: 00007facf899c819 RDX: 0000000000000000 RSI: 0000200000000500 RDI: 0000000000000004 RBP: 00007facf8a32c91 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007facf8c16038 R14: 00007facf8c15fa0 R15: 00007ffd41b01c78 </TASK> Allocated by task 11013: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 unpoison_slab_object mm/kasan/common.c:340 [inline] __kasan_slab_alloc+0x6c/0x80 mm/kasan/common.c:366 kasan_slab_alloc include/linux/kasan.h:253 [inline] slab_post_alloc_hook mm/slub.c:4538 [inline] slab_alloc_node mm/slub.c:4866 [inline] kmem_cache_alloc_lru_noprof+0x2b8/0x640 mm/slub.c:4885 sock_alloc_inode+0x28/0xc0 net/socket.c:316 alloc_inode+0x6a/0x1b0 fs/inode.c:347 new_inode_pseudo include/linux/fs.h:3003 [inline] sock_alloc net/socket.c:631 [inline] __sock_create+0x12d/0x9d0 net/socket.c:1562 sock_create net/socket.c:1656 [inline] __sys_socketpair+0x1c4/0x560 net/socket.c:1803 __do_sys_socketpair net/socket.c:1856 [inline] __se_sys_socketpair net/socket.c:1853 [inline] __x64_sys_socketpair+0x9b/0xb0 net/socket.c:1853 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 15: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:584 poison_slab_object mm/kasan/common.c:253 [inline] __kasan_slab_free+0x5c/0x80 mm/kasan/common.c:285 kasan_slab_free include/linux/kasan.h:235 [inline] slab_free_hook mm/slub.c:2685 [inline] slab_free mm/slub.c:6165 [inline] kmem_cache_free+0x187/0x630 mm/slub.c:6295 rcu_do_batch kernel/rcu/tree.c: ---truncated---	7.8	More Details
CVE-2025-52347	An issue in the component DirectIo64.sys of PassMark BurnInTest v11.0 Build 1011, OSForensics v11.1 Build 1007, and PerformanceTest v11.1 Build 1004 allows attackers to access kernel memory and escalate privileges via a crafted IOCTL 0x8011E044 call.	7.8	More Details
CVE-2026-43009	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix incorrect pruning due to atomic fetch precision tracking When backtrack_insn encounters a BPF_STX instruction with BPF_ATOMIC and BPF_FETCH, the src register (or r0 for BPF_CMPXCHG) also acts as a destination, thus receiving the old value from the memory location. The current backtracking logic does not account for this. It treats atomic fetch operations the same as regular stores where the src register is only an input. This leads the backtrack_insn to fail to propagate precision to the stack location, which is then not marked as precise! Later, the verifier's path pruning can incorrectly consider two states equivalent when they differ in terms of stack state. Meaning, two branches can be treated as equivalent and thus get pruned when they should not be seen as such. Fix it as follows: Extend the BPF_LDX handling in backtrack_insn to also cover atomic fetch operations via is_atomic_fetch_insn() helper. When the fetch dst register is being tracked for precision, clear it, and propagate precision over to the stack slot. For non-stack memory, the precision walk stops at the atomic instruction, same as regular BPF_LDX. This covers all fetch variants. Before: 0: (b7) r1 = 8 ; R1=8 1: (7b) *(u64 *)(r10 -8) = r1 ; R1=8 R10=fp0 fp-8=8 2: (b7) r2 = 0 ; R2=0 3: (db) r2 = atomic64_fetch_add((u64 *)(r10 -8), r2) ; R2=8 R10=fp0 fp-8=mmmmmmmm 4: (bf) r3 = r10 ; R3=fp0 R10=fp0 5: (0f) r3 += r2 mark_precise: frame0: last_idx 5 first_idx 0 subseq_idx -1 mark_precise: frame0: regs=r2 stack= before 4: (bf) r3 = r10 mark_precise: frame0: regs=r2 stack= before 3: (db) r2 = atomic64_fetch_add((u64 *)(r10 -8), r2) mark_precise: frame0: regs=r2 stack= before 2: (b7) r2 = 0 6: R2=8 R3=fp8 6: (b7) r0 = 0 ; R0=0 7: (95) exit After: 0: (b7) r1 = 8 ; R1=8 1: (7b) *(u64 *)(r10 -8) = r1 ; R1=8 R10=fp0 fp-8=8 2: (b7) r2 = 0 ; R2=0 3: (db) r2 = atomic64_fetch_add((u64 *)(r10 -8), r2) ; R2=8 R10=fp0 fp-8=mmmmmmmm 4: (bf) r3 = r10 ; R3=fp0 R10=fp0 5: (0f) r3 += r2 mark_precise: frame0: last_idx 5 first_idx 0 subseq_idx -1 mark_precise: frame0: regs=r2 stack= before 4: (bf) r3 = r10 mark_precise: frame0: regs=r2 stack= before 3: (db) r2 = atomic64_fetch_add((u64 *)(r10 -8), r2) mark_precise: frame0: regs= stack=-8 before 2: (b7) r2 = 0 mark_precise: frame0: regs= stack=-8 before 1: (7b) *(u64 *)(r10 -8) = r1 mark_precise: frame0: regs=r1 stack= before 0: (b7) r1 = 8 6: R2=8 R3=fp8 6: (b7) r0 = 0 ; R0=0 7: (95) exit	7.8	More Details
CVE-2026-31786	In the Linux kernel, the following vulnerability has been resolved: Buffer overflow in drivers/xen/sys-hypervisor.c The build id returned by HYPERVISOR_xen_version(XENVER_build_id) is neither NUL terminated nor a string. The first causes a buffer overflow as sprintf in buildid_show will read and copy till it finds a NUL. 00000000 f4 91 51 f4 dd 38 9e 9d 65 47 52 eb 10 71 db 50 |..Q..8..eGR..q.P| 00000010 b9 a8 01 42 6f 2e 32 |...Bo.2| 00000017 So use a memcpy instead of sprintf to have the correct value: 00000000 f4 91 51 f4 dd 00 9e 9d 65 47 52 eb 10 71 db 50 |..Q.....eGR..q.P| 00000010 b9 a8 01 42 |...B| 00000014 (the above have a hack to embed a zero inside and check it's returned correctly). This is XSA-485 / CVE-2026-31786	7.8	More Details
CVE-2026-31716	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: validate rec->used in journal-replay file record check check_file_record() validates rec->total against the record size but never validates rec->used. The do_action() journal-replay handlers read rec->used from disk and use it to compute memmove lengths: DeleteAttribute: memmove(attr, ..., used - asize - roff) CreateAttribute: memmove(..., attr, used - roff) change_attr_size: memmove(..., used - PtrOffset(rec, next)) When rec->used is smaller than the offset of a validated attribute, or larger than the record size, these subtractions can underflow allowing us to copy huge amounts of memory in to a 4kb buffer, generally considered a bad idea overall. This requires a corrupted filesystem, which isn't a threat model the kernel really needs to worry about, but checking for such an obvious out-of-bounds value is good to keep things robust, especially on journal replay Fix this up by bounding rec->used correctly. This is much like commit b2bc7c44ed17 ("fs/ntfs3: Fix slab-out-of-bounds read in DeleteIndexEntryRoot") which checked different values in this same switch statement.	7.8	More Details
CVE-2026-31693	In the Linux kernel, the following vulnerability has been resolved: cifs: some missing initializations on replay In several places in the code, we have a label to signify the start of the code where a request can be replayed if necessary. However, some of these places were missing the necessary reinitializations of certain local variables before replay. This change makes sure that these variables get initialized after the label.	7.8	More Details
CVE-2025-14576	Insufficient validation of node IDs in Qt SVG module allows arbitrary QML/JavaScript code injection when loading malicious SVG files through the VectorImage component in Qt Quick. While QML execution is typically more restricted than native code execution, this could still lead to denial of service, information disclosure, or other impacts depending on the application's privilege level and data access.	7.8	More Details
CVE-2026-5403	SBC codec crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service and possible code execution	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: writeback: Fix use after free in inode_switch_wbs_work_fn() inode_switch_wbs_work_fn() has a loop like: wb_get(new_wb); while (1) { list = llist_del_all(&new_wb->switch_wbs_ctxs); /* Nothing to do? */ if (!list) break; ... process the items ... } Now adding of items to the list looks like: wb_queue_isw() if (llist_add(&isw->list, &wb-		

CVE-2026-31703	>switch_wbs_ctxs)) queue_work(isw_wq, &wb->switch_work); Because inode_switch_wbs_work_fn() loops when processing isw items, it can happen that wb->switch_work is pending while wb->switch_wbs_ctxs is empty. This is a problem because in that case wb can get freed (no isw items -> no wb reference) while the work is still pending causing use-after-free issues. We cannot just fix this by cancelling work when freeing wb because that could still trigger problematic 0 -> 1 transitions on wb refcount due to wb_get() in inode_switch_wbs_work_fn(). It could be all handled with more careful code but that seems unnecessarily complex so let's avoid that until it is proven that the looping actually brings practical benefit. Just remove the loop from inode_switch_wbs_work_fn() instead. That way when wb_queue_isw() queues work, we are guaranteed we have added the first item to wb->switch_wbs_ctxs and nobody is going to remove it (and drop the wb reference it holds) until the queued work runs.	7.8	More Details
CVE-2026-37525	AGL app-framework-binder (afb-daemon) through v19.90.0 contains a privilege escalation vulnerability in the supervision Do command. The on_supervision_call function in src/afb-supervision.c explicitly nullifies the request credentials by calling afb_context_change_cred(&xreq->context, NULL) before dispatching an attacker-controlled API call via xapi->itf->call(xapi->closure, xreq). The NULL propagation chain through afb-context.c:110 (context->credentials = afb_cred_addref(NULL)) and afb-cred.c:163 (returns NULL when cred is NULL) confirms that credentials are zeroed before the target API executes. The attacker controls both api and verb parameters via JSON input, allowing execution of any registered API with a NULL credential context. APIs that rely on context->credentials for authorization decisions may fail open when receiving NULL credentials, enabling privilege escalation. This vulnerability was introduced in commit abbb4599f0b921c6f434b6bd02bcfb277eecf745 on 2018-02-14.	7.8	More Details
CVE-2026-7791	Improper privilege management in the log rotation mechanism of the Skylight Workspace Config Service in Amazon WorkSpaces for Windows before 2.6.2034.0 allows a local non-admin authenticated user to place arbitrary files into arbitrary locations bypassing file system permission protections, leading to local privilege escalation to SYSTEM.	7.8	More Details
CVE-2026-31742	In the Linux kernel, the following vulnerability has been resolved: vt: discard stale unicode buffer on alt screen exit after resize When enter_alt_screen() saves vc_uni_lines into vc_saved_uni_lines and sets vc_uni_lines to NULL, a subsequent console resize via vc_do_resize() skips reallocating the unicode buffer because vc_uni_lines is NULL. However, vc_saved_uni_lines still points to the old buffer allocated for the original dimensions. When leave_alt_screen() later restores vc_saved_uni_lines, the buffer dimensions no longer match vc_rows/vc_cols. Any operation that iterates over the unicode buffer using the current dimensions (e.g. csi_J clearing the screen) will access memory out of bounds, causing a kernel oops: BUG: unable to handle page fault for address: 0x0000002000000020 RIP: 0010:csi_J+0x133/0x2d0 The faulting address 0x0000002000000020 is two adjacent u32 space characters (0x20) interpreted as a pointer, read from the row data area past the end of the 25-entry pointer array in a buffer allocated for 80x25 but accessed with 240x67 dimensions. Fix this by checking whether the console dimensions changed while in the alternate screen. If they did, free the stale saved buffer instead of restoring it. The unicode screen will be lazily rebuilt via vc_uniscr_check() when next needed.	7.8	More Details
CVE-2026-31769	In the Linux kernel, the following vulnerability has been resolved: gpib: fix use-after-free in IO ioctl handlers The IBRD, IBWRT, IBCMD, and IBWAIT ioctl handlers use a gpib_descriptor pointer after board->big_gpib_mutex has been released. A concurrent IBCLOSEDEV ioctl can free the descriptor via close_dev_ioctl() during this window, causing a use-after-free. The IO handlers (read_ioctl, write_ioctl, command_ioctl) explicitly release big_gpib_mutex before calling their handler. wait_ioctl() is called with big_gpib_mutex held, but ibwait() releases it internally when wait_mask is non-zero. In all four cases, the descriptor pointer obtained from handle_to_descriptor() becomes unprotected. Fix this by introducing a kernel-only descriptor_busy reference count in struct gpib_descriptor. Each handler atomically increments descriptor_busy under file_priv->descriptors_mutex before releasing the lock, and decrements it when done. close_dev_ioctl() checks descriptor_busy under the same lock and rejects the close with -EBUSY if the count is non-zero. A reference count rather than a simple flag is necessary because multiple handlers can operate on the same descriptor concurrently (e.g. IBRD and IBWAIT on the same handle from different threads). A separate counter is needed because io_in_progress can be cleared from unprivileged userspace via the IBWAIT ioctl (through general_ibstatus() with set_mask containing CMPL), which would allow an attacker to bypass a check based solely on io_in_progress. The new descriptor_busy counter is only modified by the kernel IO paths. The lock ordering is consistent (big_gpib_mutex -> descriptors_mutex) and the handlers only hold descriptors_mutex briefly during the lookup, so there is no deadlock risk and no impact on IO throughput.	7.8	More Details
CVE-2026-7584	The LabOne Q serialization framework uses a class-loading mechanism (import_cls) to dynamically import and instantiate Python classes during deserialization. Prior to the fix, this mechanism accepted arbitrary fully-qualified class names from the serialized data without any validation of the target class or restriction on which modules could be imported. An attacker can craft a serialized experiment file that causes the deserialization engine to import and instantiate arbitrary Python classes with attacker-controlled constructor arguments, resulting in arbitrary code execution in the context of the user running the Python process. Exploitation requires the victim to load a malicious file using LabOne Q's deserialization functions, for example a compromised experiment file shared for collaboration or support purposes.	7.8	More Details
CVE-2026-43030	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix regsafe() for pointers to packet In case rold->reg->range == BEYOND_PKT_END && rcur->reg->range == N regsafe() may return true which may lead to current state with valid packet range not being explored. Fix the bug.	7.8	More Details
CVE-2026-43056	In the Linux kernel, the following vulnerability has been resolved: net: mana: fix use-after-free in add_adev() error path If auxiliary_device_add() fails, add_adev() jumps to add_fail and calls auxiliary_device_uninit(adev). The auxiliary device has its release callback set to adev_release(), which frees the containing struct mana_adev. Since adev is embedded in struct mana_adev, the subsequent fall-through to init_fail and access to adev->id may result in a use-after-free. Fix this by saving the allocated auxiliary device id in a local variable before calling auxiliary_device_add(), and use that saved id in the cleanup path after auxiliary_device_uninit().	7.8	More Details
CVE-2026-31743	In the Linux kernel, the following vulnerability has been resolved: nvmem: zynqmp_nvmem: Fix buffer size in DMA and memcpy Buffer size used in dma allocation and memcpy is wrong. It can lead to undersized DMA buffer access and possible memory corruption. use correct buffer size in dma_alloc_coherent and memcpy.	7.8	More Details
CVE-2026-31761	In the Linux kernel, the following vulnerability has been resolved: iio: gyro: mpu3050: Move iio_device_register() to correct location iio_device_register() should be at the end of the probe function to prevent race conditions. Place iio_device_register() at the end of the probe function and place iio_device_unregister() accordingly.	7.8	More Details
CVE-2026-22167	Software installed and run as a non-privileged user may conduct improper GPU system calls to force GPU to write to arbitrary physical memory pages. Under certain circumstances this exploit could be used to corrupt data pages not allocated by the GPU driver but memory pages in use by the kernel and drivers running on the platform altering their behaviour. This attack can lead the GPU to perform write operations on restricted internal GPU buffers that can lead to a second order affect of corrupted arbitrary physical memory.	7.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ti-adc161s626: use DMA-safe memory for spi_read() Add a DMA-safe buffer and use it for spi_read() instead of a stack memory. All SPI buffers must be DMA-safe. Since we only need up to 3	7.8	More

31768	bytes, we just use a u8[] instead of __be16 and __be32 and change the conversion functions appropriately.		Details
CVE-2026-36365	An issue in Lymphatus caesium-image-compressor All versions up to and including commit 02da2c6 allows a local attacker to execute arbitrary code via the shutdownMachine and putMachineToSleep functions in PostCompressionActions.cpp	7.8	More Details
CVE-2026-31694	In the Linux kernel, the following vulnerability has been resolved: fuse: reject oversized dirents in page cache fuse_add_dirent_to_cache() computes a serialized dirent size from the server-controlled namelen field and copies the dirent into a single page-cache page. The existing logic only checks whether the dirent fits in the remaining space of the current page and advances to a fresh page if not. It never checks whether the dirent itself exceeds PAGE_SIZE. As a result, a malicious FUSE server can return a dirent with namelen=4095, producing a serialized record size of 4120 bytes. On 4 KiB page systems this causes memcpy() to overflow the cache page by 24 bytes into the following kernel page. Reject dirents that cannot fit in a single page before copying them into the readdir cache.	7.8	More Details
CVE-2026-5405	RDP protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service and possible code execution	7.8	More Details
CVE-2026-30769	An issue in the TVicPort64.sys component of EnTech Taiwan TVicPort Product v4.0, File v5.2.1.0 allows attackers to escalate privileges via sending crafted IOCTL 0x80002008 requests.	7.8	More Details
CVE-2025-47405	Memory corruption when processing camera sensor input/output control codes with invalid output buffers.	7.8	More Details
CVE-2026-31695	In the Linux kernel, the following vulnerability has been resolved: wifi: virt_wifi: remove SET_NETDEV_DEV to avoid use-after-free Currently we execute `SET_NETDEV_DEV(dev, &priv->lowerdev->dev)` for the virt_wifi net devices. However, unregistering a virt_wifi device in netdev_run_todo() can happen together with the device referenced by SET_NETDEV_DEV(). It can result in use-after-free during the ethtool operations performed on a virt_wifi device that is currently being unregistered. Such a net device can have the `dev.parent` field pointing to the freed memory, but ethnl_ops_begin() calls `pm_runtime_get_sync(dev->dev.parent)`. Let's remove SET_NETDEV_DEV for virt_wifi to avoid bugs like this: == BUG: KASAN: slab-use-after-free in __pm_runtime_resume+0xe2/0xf0 Read of size 2 at addr ffff88810cfc46f8 by task pm/606 Call Trace: <TASK> dump_stack_lvl+0x4d/0x70 print_report+0x170/0x4f3 ? __pfx__raw_spin_lock_irqsave+0x10/0x10 kasan_report+0xda/0x110 ? __pm_runtime_resume+0xe2/0xf0 ? __pm_runtime_resume+0xe2/0xf0 __pm_runtime_resume+0xe2/0xf0 ethnl_ops_begin+0x49/0x270 ethnl_set_features+0x23c/0xab0 ? __pfx_ethnl_set_features+0x10/0x10 ? kvm_sched_clock_read+0x11/0x20 ? local_clock_noinstr+0xf/0xf0 ? local_clock+0x10/0x30 ? kasan_save_track+0x25/0x60 ? __kasan_kmalloc+0x7f/0x90 ? genl_family_rcv_msg_attrs_parse.isra.0+0x150/0x2c0 genl_family_rcv_msg_doit+0x1e7/0x2c0 ? __pfx_genl_family_rcv_msg_doit+0x10/0x10 ? __pfx_cred_has_capability.isra.0+0x10/0x10 ? stack_trace_save+0x8e/0xc0 genl_rcv_msg+0x411/0x660 ? __pfx_genl_rcv_msg+0x10/0x10 ? __pfx_ethnl_set_features+0x10/0x10 netlink_rcv_skb+0x121/0x380 ? __pfx_genl_rcv_msg+0x10/0x10 ? __pfx_netlink_rcv_skb+0x10/0x10 ? __pfx_down_read+0x10/0x10 genl_rcv+0x23/0x30 netlink_unicast+0x60f/0x830 ? __pfx_netlink_unicast+0x10/0x10 ? __pfx___alloc_skb+0x10/0x10 netlink_sendmsg+0x6ea/0xbc0 ? __pfx_netlink_sendmsg+0x10/0x10 ? __futex_queue+0x10b/0x1f0 ___sys_sendmsg+0x7a2/0x950 ? copy_msghdr_from_user+0x26b/0x430 ? __pfx_____sys_sendmsg+0x10/0x10 ? __pfx_copy_msghdr_from_user+0x10/0x10 ___sys_sendmsg+0xf8/0x180 ? __pfx____sys_sendmsg+0x10/0x10 ? __pfx_futex_wait+0x10/0x10 ? fdget+0x2e4/0x4a0 __sys_sendmsg+0x11f/0x1c0 ? __pfx___sys_sendmsg+0x10/0x10 do_syscall_64+0xe2/0x570 ? exc_page_fault+0x66/0xb0 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> This fix may be combined with another one in the ethtool subsystem: https://lore.kernel.org/all/20260322075917.254874-1-alex.popov@linux.com/T/#u	7.8	More Details
CVE-2025-47407	Memory corruption while creating a process on the digital signal processor due to allocation failure at the kernel level.	7.8	More Details
CVE-2025-47408	Memory corruption when another driver calls an IOCTL with invalid input/output buffer.	7.8	More Details
CVE-2026-43047	In the Linux kernel, the following vulnerability has been resolved: HID: multitouch: Check to ensure report responses match the request It is possible for a malicious (or clumsy) device to respond to a specific report's feature request using a completely different report ID. This can cause confusion in the HID core resulting in nasty side-effects such as OOB writes. Add a check to ensure that the report ID in the response, matches the one that was requested. If it doesn't, omit reporting the raw event and return early.	7.8	More Details
CVE-2026-24082	Memory Corruption when copying data from a freed source while executing performance counter deselect operation.	7.8	More Details
CVE-2026-43044	In the Linux kernel, the following vulnerability has been resolved: crypto: caam - fix DMA corruption on long hmac keys When a key longer than block size is supplied, it is copied and then hashed into the real key. The memory allocated for the copy needs to be rounded to DMA cache alignment, as otherwise the hashed key may corrupt neighbouring memory. The rounding was performed, but never actually used for the allocation. Fix this by replacing kmemdup with kmalloc for a larger buffer, followed by memcpy.	7.8	More Details
CVE-2026-31758	In the Linux kernel, the following vulnerability has been resolved: usb: usbtmc: Flush anchored URBs in usbtmc_release When calling usbtmc_release, pending anchored URBs must be flushed or killed to prevent use-after-free errors (e.g. in the HCD giveback path). Call usbtmc_draw_down() to allow anchored URBs to be completed.	7.8	More Details
CVE-2026-5174	Improper input validation vulnerability in Progress Software MOVEit Automation allows Privilege Escalation. This issue affects MOVEit Automation: from 2025.1.0 before 2025.1.5, from 2025.0.0 before 2025.0.9, from 2024.0.0 before 2024.1.8, versions prior to 2024.0.0.	7.7	More Details
CVE-2026-42997	An issue was discovered in idrac in OpenStack Ironic before 35.0.1. During import, a user invoking molds can request authorization to be sent to a remote endpoint. The credential forwarded is a time-limited Keystone token (which provides access to all OpenStack services Ironic is authorized for); or basic credentials configured for molds storage. The fixed versions are 26.1.6, 29.0.5, 32.0.1, and 35.0.1.	7.7	More Details

CVE-2026-43824	In Argo CD 3.2.0 before 3.2.11 and 3.3.0 before 3.3.9, ServerSideDiff allows reading cleartext Kubernetes Secret data.	7.7	More Details
CVE-2026-36355	The rtl8192cd Wi-Fi kernel driver in the Realtek rtl819x Jungle SDK (all known versions through v3.4.14B) does not perform any access control checks on the write_mem (ioctl 0x89F5) and read_mem (ioctl 0x89F6) debug handlers, which are compiled into production builds via the unconditionally defined _IOCTL_DEBUG_CMD_ macro in 8192cd_cfg.h	7.7	More Details
CVE-2026-43573	OpenClaw before 2026.4.10 contains a server-side request forgery policy bypass vulnerability in existing-session browser interaction routes. Attackers can bypass SSRF navigation guards to interact with or navigate to unauthorized targets without policy enforcement.	7.7	More Details
CVE-2026-43527	OpenClaw before 2026.4.14 contains a server-side request forgery vulnerability in browser SSRF policy that allows private-network navigation by default. Attackers can exploit this misconfiguration to access internal services or metadata endpoints through browser-driven requests.	7.7	More Details
CVE-2026-42436	OpenClaw before 2026.4.14 contains an improper access control vulnerability in browser snapshot, screenshot, and tab routes that fail to consistently validate the final browser target after navigation. Authenticated callers can bypass SSRF restrictions to expose internal or disallowed page content by exploiting route-driven navigation without proper policy re-validation.	7.7	More Details
CVE-2026-42438	OpenClaw versions 2026.4.9 before 2026.4.10 contain a sender policy bypass vulnerability in the outbound host-media attachment read helper that allows unauthorized local file disclosure. Attackers with denied read access via toolsBySender or group policy can trigger host-media attachment loading to bypass sender and group-scoped authorization boundaries and retrieve readable local files through the outbound media path.	7.7	More Details
CVE-2026-43532	OpenClaw versions 2026.4.7 before 2026.4.10 fail to normalize Discord event cover image parameters in sandbox media processing. Attackers can bypass media normalization to inject host-local media references into channel action paths expecting normalized media.	7.7	More Details
CVE-2026-42646	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Steve Burge TaxoPress simple-tags allows Blind SQL Injection.This issue affects TaxoPress: from n/a through <= 3.44.0.	7.6	More Details
CVE-2026-31719	In the Linux kernel, the following vulnerability has been resolved: crypto: krb5enc - fix async decrypt skipping hash verification krb5enc_dispatch_decrypt() sets req->base.complete as the skcipher callback, which is the caller's own completion handler. When the skcipher completes asynchronously, this signals "done" to the caller without executing krb5enc_dispatch_decrypt_hash(), completely bypassing the integrity verification (hash check). Compare with the encrypt path which correctly uses krb5enc_encrypt_done as an intermediate callback to chain into the hash computation on async completion. Fix by adding krb5enc_decrypt_done as an intermediate callback that chains into krb5enc_dispatch_decrypt_hash() upon async skcipher completion, matching the encrypt path's callback pattern. Also fix EBUSY/EINPROGRESS handling throughout: remove krb5enc_request_complete() which incorrectly swallowed EINPROGRESS notifications that must be passed up to callers waiting on backlogged requests, and add missing EBUSY checks in krb5enc_encrypt_ahash_done for the dispatch_encrypt return value. Unset MAY_BACKLOG on the async completion path so the user won't see back-to-back EINPROGRESS notifications.	7.5	More Details
CVE-2026-43031	In the Linux kernel, the following vulnerability has been resolved: net: xilinx: axienet: Fix BQL accounting for multi-BD TX packets When a TX packet spans multiple buffer descriptors (scatter-gather), axienet_free_tx_chain sums the per-BD actual length from descriptor status into a caller-provided accumulator. That sum is reset on each NAPI poll. If the BDs for a single packet complete across different polls, the earlier bytes are lost and never credited to BQL. This causes BQL to think bytes are permanently in-flight, eventually stalling the TX queue. The SKB pointer is stored only on the last BD of a packet. When that BD completes, use skb->len for the byte count instead of summing per-BD status lengths. This matches netdev_sent_queue(), which debits skb->len, and naturally survives across polls because no partial packet contributes to the accumulator.	7.5	More Details
CVE-2026-37538	Buffer overflow vulnerability in socketcand 0.4.2 in file socketcand.c in function main allows attackers to cause a denial of service or other unspecified impacts via crafted bus_name.	7.5	More Details
CVE-2026-43029	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix soft lockup in mptcp_recvmsg() syzbot reported a soft lockup in mptcp_recvmsg() [0]. When receiving data with MSG_PEEK | MSG_WAITALL flags, the skb is not removed from the sk_receive_queue. This causes sk_wait_data() to always find available data and never perform actual waiting, leading to a soft lockup. Fix this by adding a 'last' parameter to track the last peeked skb. This allows sk_wait_data() to make informed waiting decisions and prevent infinite loops when MSG_PEEK is used. [0]: watchdog: BUG: soft lockup - CPU#2 stuck for 156s! [server:1963] Modules linked in: CPU: 2 UID: 0 PID: 1963 Comm: server Not tainted 6.19.0-rc8 #61 PREEMPT(none) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:sk_wait_data+0x15/0x190 Code: 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 41 56 41 55 41 54 49 89 f4 55 48 89 d5 53 48 89 fb <48> 83 ec 30 65 48 8b 05 17 a4 6b 01 48 89 44 24 28 31 c0 65 48 8b RSP: 0018:ffffc90000603ca0 EFLAGS: 00000246 RAX: 0000000000000000 RBX: ffff888102bf0800 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ffffc90000603d18 RDI: ffff888102bf0800 RBP: 0000000000000000 R08: 0000000000000002 R09: 0000000000000101 R10: 0000000000000000 R11: 0000000000000075 R12: ffffc90000603d18 R13: ffff888102bf0800 R14: ffff888102bf0800 R15: 0000000000000000 FS: 00007f6e38b8c4c0(0000) GS:ffff8881b877e000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055aa7bff1680 CR3: 0000000105cbe000 CR4: 00000000000006f0 Call Trace: <TASK> mptcp_recvmsg+0x547/0x8c0 net/mptcp/protocol.c:2329 inet_recvmsg+0x11f/0x130 net/ipv4/af_inet.c:891 sock_recvmsg+0x94/0xc0 net/socket.c:1100 __sys_recvfrom+0xb2/0x130 net/socket.c:2256 __x64_sys_recvfrom+0x1f/0x30 net/socket.c:2267 do_syscall_64+0x59/0x2d0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e arch/x86/entry/entry_64.S:131 RIP: 0033:0x7f6e386a4a1d Code: 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 8d 05 f1 de 2c 00 41 89 ca 8b 00 85 c0 75 20 45 31 c9 45 31 c0 b8 2d 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 6b f3 c3 66 0f 1f 84 00 00 00 00 00 41 56 41 RSP: 002b:00007ffc3c4bb078 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 000000000000861e RCX: 00007f6e386a4a1d RDX: 00000000000003ff RSI: 00007ffc3c4bb150 RDI: 0000000000000004 RBP: 00007ffc3c4bb570 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000103 R11: 0000000000000246 R12: 00005605dbc00be0 R13: 00007ffc3c4bb650 R14: 0000000000000000 R15: 0000000000000000 </TASK>	7.5	More Details
CVE-2026-33449	CVE-2026-33449 is a buffer overflow in a message handling function of the Secure Access client prior to 14.50. Attackers with control of a modified server can send a cryptographically valid message to the client, overwriting a small portion of memory conceivably leading to a denial of service.	7.5	More Details
CVE-	An issue was discovered in VrmlData_IndexedFaceSet::TShape in the VRML V2.0 parser in Open CASCADE Technology (OCCT)		

2026-42478	V8_0_0_rc5 allows attackers to cause a denial of service via a crafted VRML file. The issue occurs because malformed VRML input can trigger dereference of a corrupt or unvalidated pointer during shape construction in libTKDEVRML.so.	7.5	More Details
CVE-2025-46115	An issue in open5gs v.2.7.3 allows a remote attacker to cause a denial of service via a crafted PDU Session Modification Request	7.5	More Details
CVE-2026-42403	Apache Neethi does not properly detect circular references in policy definitions. When a WS-Policy document contains circular policy references (where Policy A references Policy B which references Policy A), the policy normalization process can enter an infinite loop or cause excessive recursion, leading to a stack overflow or application hang. An attacker can craft malicious policy documents with circular references to cause a Denial of Service condition Users are recommended to upgrade to version 3.2.2, which fixes this issue.	7.5	More Details
CVE-2026-37530	AGL agl-service-can-low-level thru 17.1.12 contains a stack buffer overflow in the uds-c library. The send_diagnostic_request function in uds.c allocates a 6-byte stack buffer (MAX_DIAGNOSTIC_PAYLOAD_SIZE=6) but copies up to 7 bytes (MAX_UDS_REQUEST_PAYLOAD_LENGTH=7) via memcpy at an offset of 1+pid_length (2-3 bytes), resulting in 1-4 bytes of controlled stack overflow. The payload_length field (uint8_t) has no bounds check against the destination buffer. On 32-bit ARM automotive ECUs without stack canaries, this can lead to return address overwrite and RCE.	7.5	More Details
CVE-2026-31711	In the Linux kernel, the following vulnerability has been resolved: smb: server: fix active_num_conn leak on transport allocation failure Commit 77ffbcac4e56 ("smb: server: fix leak of active_num_conn in ksmbd_tcp_new_connection()") addressed the kthread_run() failure path. The earlier alloc_transport() == NULL path in the same function has the same leak, is reachable pre-authentication via any TCP connect to port 445, and was empirically reproduced on UML (ARCH=um, v7.0-rc7): a small number of forced allocation failures were sufficient to put ksmbd into a state where every subsequent connection attempt was rejected for the remainder of the boot. ksmbd_kthread_fn() increments active_num_conn before calling ksmbd_tcp_new_connection() and discards the return value, so when alloc_transport() returns NULL the socket is released and -ENOMEM returned without decrementing the counter. Each such failure permanently consumes one slot from the max_connections pool; once cumulative failures reach the cap, atomic_inc_return() hits the threshold on every subsequent accept and every new connection is rejected. The counter is only reset by module reload. An unauthenticated remote attacker can drive the server toward the memory pressure that makes alloc_transport() fail by holding open connections with large RFC1002 lengths up to MAX_STREAM_PROT_LEN (0x00FFFFFF); natural transient allocation failures on a loaded host produce the same drift more slowly. Mirror the existing rollback pattern in ksmbd_kthread_fn(): on the alloc_transport() failure path, decrement active_num_conn gated on server_conf.max_connections. Repro details: with the patch reverted, forced alloc_transport() NULL returns leaked counter slots and subsequent connection attempts -- including legitimate connects issued after the forced-fail window had closed -- were all rejected with "Limit the maximum number of connections". With this patch applied, the same connect sequence produces no rejections and the counter cycles cleanly between zero and one on every accept.	7.5	More Details
CVE-2022-50992	Weaver (Fanwei) E-cology 9.5 versions prior to 10.52 contain an arbitrary file read vulnerability in the XmlRpcServlet interface at the XML-RPC endpoint that allows unauthenticated remote attackers to read arbitrary files by supplying file paths to the WorkflowService.getAttachment and WorkflowService.LoadTemplateProp methods. Attackers can exploit these methods without authentication to retrieve sensitive files including system configuration files and database credentials from the server. Exploitation evidence was first observed by the Shadowserver Foundation on 2022-12-14 (UTC).	7.5	More Details
CVE-2026-37554	An issue was discovered in Vanetza V2X v26.02 allowing remote unauthorized attackers to cause a denial of service. The vulnerability exists in the GeoNetworking packet processing pipeline where OpenSSL exceptions from ECC point validation (invalid compressed point, point not on curve) are not properly caught by the Router::indicate() call chain. The openssl_wrapper.cpp check() function (line 19) throws openssl::Exception when OpenSSL operations fail. The parser's catch block in parse_secured() should catch these, but the exception escapes through subsequent processing stages (indicate_common, indicate_extended). This causes std::terminate, crashing the V2X receiver.	7.5	More Details
CVE-2025-51846	CryptPad 2025.3.1 allows unbounded WebSocket frame flood. A remote, unauthenticated attacker can significantly degrade or deny service for all users of a CryptPad instance. Fixed in 2026.2.2.	7.5	More Details
CVE-2026-42485	AGL agl-service-can-low-level contains a stack buffer overflow in the uds-c library. The send_diagnostic_request function in uds.c allocates a 6-byte stack buffer (MAX_DIAGNOSTIC_PAYLOAD_SIZE=6) but copies up to 7 bytes (MAX_UDS_REQUEST_PAYLOAD_LENGTH=7) via memcpy at an offset of 1+pid_length (2-3 bytes), resulting in 1-4 bytes of controlled stack overflow. The payload_length field (uint8_t) has no bounds check against the destination buffer. On 32-bit ARM automotive ECUs without stack canaries, this can lead to return address overwrite and RCE.	7.5	More Details
CVE-2026-43055	In the Linux kernel, the following vulnerability has been resolved: scsi: target: file: Use kzalloc_flex for aio_cmd The target_core_file doesn't initialize the aio_cmd->iocb for the ki_write_stream. When a write command fd_execute_rw_aio() is executed, we may get a bogus ki_write_stream value, causing unintended write failure status when checking iocb->ki_write_stream > max_write_streams in the block device. Let's just use kzalloc_flex when allocating the aio_cmd and let ki_write_stream=0 to fix this issue.	7.5	More Details
CVE-2026-40601	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes POST /api/chart/:chart_id/query without authentication. The endpoint only checks team.allowReportRefresh and does not verify that the target chart belongs to a public report, that the project is public, or that sharing policy allows the operation. An unauthenticated attacker who knows a chart identifier can trigger a data refresh and retrieve the current data of private charts. This issue has been patched in version 5.0.0.	7.5	More Details
CVE-2026-33845	A flaw in GnuTLS DTLS handshake parsing allows malformed fragments with zero length and non-zero offset, leading to an integer underflow during reassembly and resulting in an out-of-bounds read. This issue is remotely exploitable and may cause information disclosure or denial of service.	7.5	More Details
CVE-2026-37457	An off-by-one out-of-bounds write vulnerability in the bgp_flowspec_op_decode() function (bgpd/bgp_flowspec_util.c) of FRRouting (FRR) stable/10.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted FlowSpec component.	7.5	More Details
CVE-2026-40595	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes public chart retrieval and export routes that only verify project-level public access and, for exports, a team-level export toggle. The routes do not verify whether the target chart is actually allowed on the public report or whether the governing SharePolicy permits public access. An unauthenticated attacker who knows a chart identifier in a public project can read or export chart data for charts that were intentionally hidden from the report. This issue has been patched in version 5.0.0.	7.5	More Details

CVE-2026-43057	In the Linux kernel, the following vulnerability has been resolved: net: correctly handle tunneled traffic on IPV6_CSUM GSO fallback NETIF_F_IPV6_CSUM only advertises support for checksum offload of packets without IPv6 extension headers. Packets with extension headers must fall back onto software checksumming. Since TSO depends on checksum offload, those must revert to GSO. The below commit introduces that fallback. It always checks network header length. For tunneled packets, the inner header length must be checked instead. Extend the check accordingly. A special case is tunneled packets without inner IP protocol. Such as RFC 6951 SCTP in UDP. Those are not standard IPv6 followed by transport header either, so also must revert to the software GSO path.	7.5	More Details
CVE-2026-4503	IBM Langflow Desktop 1.0.0 through 1.8.4 Langflow could allow an unauthenticated user to view other users' images due to an indirect object reference through a user-controlled key.	7.5	More Details
CVE-2026-42402	Apache Neethi is vulnerable to a Denial of Service attack through algorithmic complexity in policy normalization. Specially crafted WS-Policy documents can trigger an exponential Cartesian cross-product expansion during the normalization process, causing unbounded memory allocation that exhausts the JVM heap. This occurs when the normalization process generates an excessive number of policy alternatives without bounds, leading to runtime memory exhaustion. Users should upgrade to 3.2.2 which limits the maximum number of normalized policy alternatives.	7.5	More Details
CVE-2025-63548	An issue in Eprosima Micro-XREC-DDS Agent v.3.0.1 allows a remote attacker to cause a denial of service via a packet specially crafted to bear a non-valid value in any Boolean field.	7.5	More Details
CVE-2026-42467	An issue was discovered in Open-SAE-J1939 thru commit b6caf884df46435e539b1ecbf92b6c29b345bdfe (2025-11-30) in SAE_J1939_Read_Binary_Data_Transfer_DM16 causing a denial of service via crafted CAN frame on the J1939 bus.	7.5	More Details
CVE-2025-63547	An issue in Eprosima Micro-XREC-DDS Agent v.3.0.1 allows a remote attacker to cause a denial of service via a crafted packet to the MTU length field	7.5	More Details
CVE-2025-56568	Assertion failure vulnerability in the PCO (Protocol Configuration Options) parser in the SMF (Session Management Function) component of Open5GS before v2.7.5 allows remote attackers to cause denial of service via specially crafted NGAP messages containing malformed length fields in protocol configuration data.	7.5	More Details
CVE-2026-40560	Starman versions before 0.4018 for Perl allows HTTP Request Smuggling via Improper Header Precedence. Starman incorrectly prioritizes "Content-Length" over "Transfer-Encoding: chunked" when both headers are present in an HTTP request. Per RFC 7230 3.3.3, Transfer-Encoding must take precedence. An attacker could exploit this to smuggle malicious HTTP requests via a front-end reverse proxy.	7.5	More Details
CVE-2026-36959	U-SPEED N300 router V1.0.0 does not implement rate limiting or account lockout protections on the /api/login endpoint. This allows an attacker on the local network to perform unlimited authentication attempts, enabling brute-force attacks against the administrator account and potential unauthorized access to the router management interface.	7.5	More Details
CVE-2024-39847	Unauthenticated attackers can exploit a weakness in the XML parser functionality of the SOAP endpoints in 4D server. This allows them to obtain read access to files on the application server and adjacent network shares, and perform HTTP GET requests to arbitrary services.	7.5	More Details
CVE-2026-5192	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Path Traversal in versions up to, and including, 1.52.1 via the 'upload-1[file][file_path]' parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Successful exploitation requires a publicly accessible form with a File Upload field where Save and Continue is enabled in that form's Behavior settings and the Save and Continue email notification is configured to attach uploaded files in Email Notifications.	7.5	More Details
CVE-2026-6320	The Salon Booking System – Free Version plugin for WordPress is vulnerable to Arbitrary File Read in versions up to, and including, 10.30.25. This is due to the public booking flow accepting attacker-controlled file-field values and later using those stored values as trusted paths for email attachments. This makes it possible for unauthenticated attackers to read arbitrary local files and exfiltrate them via booking confirmation email attachments.	7.5	More Details
CVE-2026-37555	An issue was discovered in libsndfile 1.2.2 IMA ADPCM codec. The AIFF code path (line 241) was fixed with (sf_count_t) cast, but the WAV code path (line 235) and close path (line 167) were not. When samplesperblock (int) * blocks (int) exceeds INT_MAX, the 32-bit multiplication overflows before being assigned to sf.frames (sf_count_t/int64). With samplesperblock=50000 and blocks=50000, the product 2500000000 overflows to -1794967296. This causes incorrect frame count leading to heap buffer overflow or denial of service. Both values come from the WAV file header and are attacker-controlled. This issue was discovered after an incomplete fix for CVE-2022-33065.	7.5	More Details
CVE-2026-3456	The GeekyBot — Generate AI Content Without Prompt, Chatbot and Lead Generation plugin for WordPress is vulnerable to SQL Injection via the 'attributekey' parameter in versions up to, and including, 1.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-42440	OOM Denial of Service via Unbounded Array Allocation in Apache OpenNLP AbstractModelReader Versions Affected: before 2.5.9 before 3.0.0-M3 Description: The AbstractModelReader methods getOutcomes(), getOutcomePatterns(), and getPredicates() each read a 32-bit signed integer count field from a binary model stream and pass that value directly to an array allocation (new String[numOutcomes], new int[numOCTypes][], new String[NUM_PREDS]) without validating that the value is non-negative or within a reasonable bound. The count is therefore fully attacker-controlled when the model file originates from an untrusted source. A crafted .bin model file in which any of these count fields is set to Integer.MAX_VALUE (or any value large enough to exhaust the available heap) triggers an OutOfMemoryError at the array allocation itself, before the corresponding label or pattern data is consumed from the stream. The error occurs very early in deserialization: for a GIS model, getOutcomes() is reached after only the model-type string, the correction constant, and the correction parameter have been read; so the attacker pays no meaningful size cost to weaponize a payload, and a single small file can crash a JVM that loads it. Any code path that deserializes a .bin model is affected, including direct use of GenericModelReader and any higher-level component that delegates to it during model load. The practical impact is denial of service against processes that load model files from untrusted or semi-trusted origins. Mitigation: * 2.x users should upgrade to 2.5.9. * 3.x users should upgrade to 3.0.0-M3. Note: The fix introduces an upper bound on each of the three count fields, checked before array allocation; counts that are negative or exceed the bound cause an IllegalArgumentException to be thrown and the read to fail fast with no large allocation. The default bound is 10,000,000, which is well above the entry counts of legitimate OpenNLP	7.5	More Details

	models but far below any value that would threaten heap exhaustion. Deployments that legitimately need to load models with more entries than the default can raise the limit at JVM startup by setting the OPENNLP_MAX_ENTRIES system property to the desired positive integer (e.g. -DOPENNLP_MAX_ENTRIES=50000000); invalid or non-positive values fall back to the default. Users who cannot upgrade immediately should treat all .bin model files as untrusted input unless their provenance is verified, and should avoid loading models supplied by end users or fetched from third-party repositories without integrity checks.		
CVE-2026-42198	pgjdbc is an open source postgresql JDBC Driver. From version 42.2.0 to before version 42.7.11, pgjdbc is vulnerable to a client-side denial of service during SCRAM-SHA-256 authentication. A malicious server can instruct the driver to perform SCRAM authentication with a very large iteration count. With a large enough value, the client spends an unbounded amount of CPU time inside PBKDF2 before authentication can fail. A single attempt ties up a CPU core. Repeated or concurrent attempts exhaust client CPU and can wedge connection pools. In affected versions, loginTimeout did not fully mitigate this problem. When loginTimeout expired, the caller could stop waiting, but the worker thread performing the connection attempt could continue running and burning CPU inside the SCRAM PBKDF2 computation. This issue has been patched in version 42.7.11.	7.5	More Details
CVE-2026-5100	The AWP Classifieds plugin for WordPress is vulnerable to SQL Injection via the 'regions' parameter array keys in versions up to, and including, 4.4.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-44028	An issue was discovered in Nix before 2.34.7 and Lix before 2.95.2. Unbounded recursion in the NAR (Nix Archive) parser could lead to a stack-to-heap overflow when the parser is run on a coroutine stack. The stack is allocated without a guard page, which means that a stack overflow could overwrite memory on the heap and could allow arbitrary code execution as the Nix daemon (run as root in multi-user installations) if ASLR hardening is bypassed. This can be exploited by all users able to connect to the daemon (e.g., in Nix, this is configurable via the allowed-users setting, defaulting to all users). The fixed versions are 2.34.7, 2.33.6, 2.32.8, 2.31.5, 2.30.5, 2.29.4, and 2.28.7 for Nix (introduced in 2.24.4); and 2.95.2, 2.94.2, and 2.93.4 for Lix (introduced in 2.93.0).	7.5	More Details
CVE-2026-7776	Boundary Community Edition and Boundary Enterprise (“Boundary”) workers are vulnerable to a denial-of-service condition during node enrollment TLS handshakes. An attacker with network access to the worker authentication listener may open a connection and delay or withhold the client certificate during the TLS handshake, causing worker connection handling to block. This may prevent legitimate worker connections from being accepted or routed. This vulnerability, CVE-2026-7776, is fixed in Boundary 0.21.3, 0.20.3, 0.19.5.	7.5	More Details
CVE-2026-33846	A heap buffer overflow vulnerability exists in the DTLS handshake fragment reassembly logic of GnuTLS. The issue arises in merge_handshake_packet() where incoming handshake fragments are matched and merged based solely on handshake type, without validating that the message_length field remains consistent across all fragments of the same logical message. An attacker can exploit this by sending crafted DTLS fragments with conflicting message_length values, causing the implementation to allocate a buffer based on a smaller initial fragment and subsequently write beyond its bounds using larger, inconsistent fragments. Because the merge operation does not enforce proper bounds checking against the allocated buffer size, this results in an out-of-bounds write on the heap. The vulnerability is remotely exploitable without authentication via the DTLS handshake path and can lead to application crashes or potential memory corruption.	7.5	More Details
CVE-2026-7768	@fastify/accepts-serializer cached serializer-selection results keyed by the request Accept header without a size limit or eviction policy. A remote unauthenticated client could send many distinct but matching Accept header variants to make the cache grow unbounded, eventually exhausting the Node.js heap and crashing the process. Versions <= 6.0.3 are affected. Update to 6.0.4 or later, which bounds the cache via an LRU with a default size of 100 entries, configurable through the new cacheSize plugin option.	7.5	More Details
CVE-2026-7164	Incorrect packet validation allowed unbounded recursion parsing SCTP chunk parameters. This can eventually result in a stack overflow and panic. Remote attackers can craft packets which cause affected systems to panic. This affects any system where pf is configured to process traffic, independent of the configured ruleset.	7.5	More Details
CVE-2026-34059	Buffer Over-read vulnerability in Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	7.5	More Details
CVE-2025-70069	An issue in Assimp v.6.0.2 allows a remote attacker to cause a denial of service via the FBXConverter.cpp and ConvertMeshMultiMaterial() method	7.5	More Details
CVE-2026-6321	fast-uri decoded percent-encoded path separators and dot segments before applying dot-segment removal in its normalize() and equal() functions. Encoded path data was treated like real slashes and parent-directory references, so distinct URIs could collapse onto the same normalized path. Applications that normalize or compare attacker-controlled URLs to enforce path-based policy can be bypassed, with a path that appears confined under an allowed prefix normalizing to a different location. Versions <= 3.1.0 are affected. Update to 3.1.1 or later.	7.5	More Details
CVE-2026-42154	Prometheus is an open-source monitoring system and time series database. Prior to versions 3.5.3 and 3.11.3, the remote read endpoint (/api/v1/read) does not validate the declared decoded length in a snappy-compressed request body before allocating memory. An unauthenticated attacker can send a small payload that causes a huge heap allocation per request. Under concurrent load this can exhaust available memory and crash the Prometheus process. This issue has been patched in versions 3.5.3 and 3.11.3.	7.5	More Details
CVE-2026-29169	A NULL pointer dereference in mod_dav_lock in Apache HTTP Server 2.4.66 and earlier may allow an attacker to crash the server with a malicious request.mod_dav_lock is not used internally by mod_dav or mod_dav_fs. The only known use-case for mod_dav_lock was mod_dav_svn from Apache Subversion earlier than version 1.2.0. Users are recommended to upgrade to version 2.4.66, which fixes this issue, or remove mod_dav_lock.	7.5	More Details
CVE-2026-42151	Prometheus is an open-source monitoring system and time series database. Prior to versions 3.5.3 and 3.11.3, the client_secret field in the Azure AD remote write OAuth configuration (storage/remote/azuread) was typed as string instead of Secret. Prometheus redacts fields of type Secret when serving the configuration via the /-/config HTTP API endpoint. Because the field was a plain string, the Azure OAuth client secret was exposed in plaintext to any user or process with access to that endpoint. This issue has been patched in versions 3.5.3 and 3.11.3.	7.5	More Details
CVE-2026-25863	Conditional Fields for Contact Form 7 WordPress plugin through version 2.6.7 contains an uncontrolled resource consumption vulnerability in the Wpcf7cfMailParser class where the hide_hidden_mail_fields_regex_callback() method reads an iteration count directly from user-supplied POST parameters without validation or upper bound enforcement. Unauthenticated attackers can supply an arbitrarily large integer value through the REST API endpoint to cause unbounded loop execution with multiple preg_replace() operations, exhausting server memory and crashing the PHP process.	7.5	More Details

CVE-2026-41471	Easy PayPal Events & Tickets plugin for WordPress versions 1.3 and earlier contain an information disclosure vulnerability in the QR code scanning endpoint that allows unauthenticated attackers to enumerate and retrieve all customer order records. Attackers can iterate over sequential WordPress post IDs through the scan_qr.php endpoint to harvest the complete set of orders stored in the database without requiring authentication or prior knowledge of specific order identifiers. This plugin was officially closed as of 2026-03-18.	7.5	More Details
CVE-2026-37459	An integer underflow in FRRouting (FRR) stable/10.0 to stable/10.6 allows attackers to cause a Denial of Service (DoS) via supplying a crafted BGP UPDATE message.	7.5	More Details
CVE-2026-37461	An out-of-bounds read in the ParseIP6Extended function (/bgp/bgp.go) of gobgp v4.3.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted BGP UPDATE message.	7.5	More Details
CVE-2026-4062	The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'object_ids' and 'exclude_object_ids' parameters in all versions up to, and including, 1.13.18. This is due to insufficient escaping on the user supplied parameters and lack of sufficient preparation on the existing SQL query. The `esc_sql()` function is applied but is ineffective because the values are placed in an unquoted `IN(...)` / `NOT IN(...)` SQL context — `esc_sql()` only escapes quote characters and provides no protection against parenthesis or SQL keyword injection. Additionally, while a numeric-only sanitizer exists in `sanitize_query_args()`, it is only applied in the AJAX code path and not in the `render-map.php` or template tag code paths. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database via a time-based blind approach.	7.5	More Details
CVE-2026-32834	Easy PayPal Events & Tickets plugin for WordPress version 1.3 and earlier contain a hardcoded authentication bypass vulnerability in the QR code scanning functionality that allows unauthenticated remote attackers to bypass hash verification by supplying 'test' as the hash parameter. Attackers can access the vulnerable endpoint via the add_wpeevent_button_qr action to retrieve sensitive order details including PayPal transaction IDs, customer email addresses, purchase amounts, and ticket information for any order with a known or guessed post ID. This plugin was officially closed as of 2026-03-18.	7.5	More Details
CVE-2026-4061	The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'map_post_type' parameter in all versions up to, and including, 1.13.18. This is due to the `SearchResults` hook explicitly calling `stripslashes_deep($_POST)` which removes WordPress magic quotes protection, followed by the unsanitized `map_post_type` value being concatenated into an `IN(...)` clause without `esc_sql()` or `$wpdb->prepare()`. The 'any' branch of the same code correctly applies `array_map('esc_sql', ...)`, but the else branch does not. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database via a time-based blind approach. Exploitation requires the Geo Search feature to be enabled in plugin settings.	7.5	More Details
CVE-2026-6918	In Eclipse Open9J versions 0.21 to 0.58, a pre-authentication remote attacker can crash JITServer by sending a 32-byte crafted TCP message.	7.5	More Details
CVE-2026-36837	TOTOLINK A3002RU V3 <= V3.0.0-B20220304.1804 was discovered to contain a stack-based buffer overflow via the hostname parameter in the formMapDelDevice function.	7.5	More Details
CVE-2023-54346	WordPress Plugin Backup Migration 1.2.8 contains an information disclosure vulnerability that allows unauthenticated attackers to download complete database backups by accessing predictable file paths. Attackers can enumerate backup directories through configuration files and complete logs, then construct direct download URLs to retrieve sensitive backup archives containing full database dumps.	7.5	More Details
CVE-2026-2892	The Otter Blocks plugin for WordPress is vulnerable to Purchase Verification Bypass in all versions up to, and including, 3.1.4. This is due to the 'get_customer_data' method relying on an unsigned 'o_stripe_data' cookie to determine Stripe product ownership for unauthenticated users. The 'check_purchase' method trusts this cookie data without performing server-side verification against the Stripe API for one-time 'payment' mode purchases. This makes it possible for unauthenticated attackers to bypass Stripe purchase-gated content visibility conditions by forging the 'o_stripe_data' cookie with a target product ID, which is publicly exposed in the checkout block's HTML source.	7.5	More Details
CVE-2026-42437	OpenClaw versions 2026.4.9 before 2026.4.10 contain a denial of service vulnerability in the voice-call realtime WebSocket path that accepts oversized frames without proper validation. Remote attackers can send oversized WebSocket frames to cause service unavailability for deployments exposing the webhook path.	7.5	More Details
CVE-2026-36957	Dbit N300 T1 Pro Easy Setup Wireless Wi-Fi Router V1.0.0 is vulnerable to Denial of Service via the boa web server URI handler. By initiating a high-volume flood of HTTP GET requests to non-existent URIs, an attacker can exhaust critical system resources, including file descriptors and memory buffers. This results in a kernel deadlock or system hang that disables the web management portal and all routing capabilities.	7.5	More Details
CVE-2026-36958	A denial-of-service vulnerability exists in the U-SPEED N300 V1.0.0 wireless router. By sending a large number of concurrent HTTP requests to random or non-existent endpoints on the web management interface, an attacker can exhaust system resources in the embedded Boa HTTP server. This causes the router web interface to become unresponsive and may require manual reboot to restore normal operation.	7.5	More Details
CVE-2026-7649	The ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'orderby' parameter in all versions up to, and including, 4.0.60 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-42520	Jenkins Credentials Binding Plugin 719.v80e905ef14eb_ and earlier does not sanitize file names for file and zip file credentials, allowing attackers able to provide credentials to a job to write files to arbitrary locations on the node filesystem, which can lead to remote code execution if Jenkins is configured to allow a low-privileged user to configure file or zip file credentials used for a job running on the built-in node.	7.5	More Details
CVE-	OpenEMR 7.0.1 contains an authentication brute force vulnerability that allows attackers to bypass rate limiting protections by		

2023-54347	sending repeated login attempts to the main login endpoint. Attackers can submit POST requests with authUser and clearPass parameters to systematically test username and password combinations without account lockout restrictions.	7.5	More Details
CVE-2026-6322	fast-uri normalize() decoded percent-encoded authority delimiters inside the host component and then re-emitted them as raw delimiters during serialization. A host that combined an allowed domain, an encoded at-sign, and a different domain was re-emitted with the at-sign as a raw userinfo separator, changing the URI's authority to the second domain. Applications that normalize untrusted URLs before host allowlist checks, redirect validation, or outbound request routing can be steered to a different authority than the input appeared to specify. Versions <= 3.1.1 are affected. Update to 3.1.2 or later.	7.5	More Details
CVE-2026-3359	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to SQL Injection via the 'inputs' parameter in versions up to, and including, 1.15.42 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-4304	The WeePie Cookie Allow plugin for WordPress is vulnerable to SQL Injection via the 'consent' parameter in all versions up to, and including, 3.4.11 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-4060	The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'sort' parameter in all versions up to, and including, 1.13.18. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The `esc_sql()` function is applied but is ineffective in the `ORDER BY` context because the value is not enclosed in quotes. Additionally, while a `sanitize_sort_arg()` allowlist-based sanitizer was added in version 1.13.18, it is only applied in the AJAX code path (`sanitize_query_args()`) and not in the `render-map.php` or template tag code paths. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database via a time-based blind approach.	7.5	More Details
CVE-2026-41882	In JetBrains IntelliJ IDEA before 2024.3.7.1, 2025.1.7.1, 2025.2.6.2, 2025.3.4.1, 2026.1.1 reading arbitrary local files was possible via built-in web server	7.4	More Details
CVE-2026-42366	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the Web Interface / ssi.cgi functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted malicious url can lead to an arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	7.4	More Details
CVE-2026-7371	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the Web Interface / ssi.cgi functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted malicious url can lead to an arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability. Reflected XXS via the error message for requesting non-existing page.	7.4	More Details
CVE-2026-42799	Out-of-bounds read vulnerability in ASR Kestrel (nr_fw modules) allows Overflow Buffers. This vulnerability is associated with program files Code/Nr/nr_fw/RA/src/NrPwrCtrl.C. This issue affects Kestrel: before 2026/02/10.	7.4	More Details
CVE-2026-42800	NULL pointer dereference vulnerability in ASR1903 in ASR Lapwing_Linux on Linux (ims_client modules) allows Pointer Manipulation. This vulnerability is associated with program files sip/utils/src/sipuri.c.	7.4	More Details
CVE-2026-7398	A weakness has been identified in florensiawidjaja BioinfoMCP up to 7ada7918b9e515604d3c0ae264d3a9af10bf6e54. This vulnerability affects the function Upload of the file bioinfo_mcp_platform/app.py of the component Upload Endpoint. This manipulation of the argument Name causes path traversal. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. Continious delivery with rolling releases is used by this product. Therefore, no version details of 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-2026-29168	Allocation of Resources Without Limits or Throttling vulnerability in Apache HTTP Server's mod_md via OCSP response data. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	7.3	More Details
CVE-2026-7506	A vulnerability has been found in SourceCodester Hotel Management System 1.0. This impacts an unknown function of the file /index.php/reservation/check. Such manipulation of the argument room_type leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-43531	OpenClaw before 2026.4.9 contains an environment variable injection vulnerability allowing malicious workspace .env files to set runtime-control variables. Attackers can inject variables affecting update sources, gateway URLs, ClawHub resolution, and browser executable paths to compromise application behavior.	7.3	More Details
CVE-2026-43025	In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: ignore explicit helper on new expectations Use the existing master conntrack helper, anything else is not really supported and it just makes validation more complicated, so just ignore what helper userspace suggests for this expectation. This was uncovered when validating CTA_EXPECT_CLASS via different helper provided by userspace than the existing master conntrack helper: BUG: KASAN: slab-out-of-bounds in nf_ct_expect_related_report+0x2479/0x27c0 Read of size 4 at addr ffff8880043fe408 by task poc/102 Call Trace: nf_ct_expect_related_report+0x2479/0x27c0 ctnetlink_create_expect+0x22b/0x3b0 ctnetlink_new_expect+0x4bd/0x5c0 nfnetlink_rcv_msg+0x67a/0x950 netlink_rcv_skb+0x120/0x350 Allowing to read kernel memory bytes off the expectation boundary. CTA_EXPECT_HELP_NAME is still used to offer the helper name to userspace via netlink dump.	7.3	More Details
CVE-2026-42377	Missing Authorization vulnerability in Brainstorm Force SureForms Pro allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SureForms Pro: from n/a through 2.8.0.	7.3	More Details
CVE-2026-7505	A flaw has been found in nextlevelbuilder GoClaw and GoClaw Lite up to 3.8.5. This affects an unknown function of the component RPC Handler. This manipulation causes improper authorization. The attack may be initiated remotely. The exploit has been published and may be used. Upgrading to version 3.9.0 mitigates this issue. Patch name: 406022e79f4a18b3070a446712080571eff11e30. You should upgrade the affected component.	7.3	More Details

CVE-2026-7785	A security flaw has been discovered in A-G-U-P-T-A wireshark-mcp edaf604416fbc94a201b4043092d4a1b09a12275/400c3da70074f22f3cce7ccb65304cafc7089c89. This affects the function quick_capture of the file pyshark_mcp.py. The manipulation results in os command injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. 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-2026-7579	A security vulnerability has been detected in AstrBotDevs AstrBot up to 4.16.0. This issue affects some unknown processing of the file astrbot/dashboard/routes/auth.py of the component Dashboard. The manipulation leads to hard-coded credentials. 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-2026-7784	A vulnerability has been found in RTGS2017 NagaAgent up to 5.1.0. This issue affects some unknown processing of the file apiserver/routes/extensions.py of the component Skills Endpoint. Such manipulation of the argument Name leads to path traversal. 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-2026-7519	A vulnerability has been found in Fujian Apex LiveBOS up to 2.0. Impacted is an unknown function of the file /feed/UploadImage.do of the component Endpoint. Such manipulation of the argument filename leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.1 is recommended to address this issue. Upgrading the affected component is advised.	7.3	More Details
CVE-2026-7788	A security flaw has been discovered in Axle-Bucamp MCP-Docusaurus up to 404bc028e15ec304c9a045528560f4b5f27a17e0. The affected element is the function update_document/continue_document/delete_document/get_content of the file app/routes/document.py. Performing a manipulation of the argument DOCS_DIR/path results in path traversal. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. 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-2026-7384	A vulnerability was detected in ezequiroga mcp-bases 357ca19c7a49a9b9cb2ef639b366f03aba8bea39/c630b8ab0f970614d42da8e566e9c0d15a16414c. This impacts the function search_papers of the file research_server.py. Performing a manipulation of the argument topic 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 project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7545	A weakness has been identified in SourceCodester Advanced School Management System 1.0. The affected element is an unknown function of the file commonController.php of the component checkEmail Endpoint. This manipulation 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-2026-7549	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. This impacts an unknown function of the file /ajax.php?action=delete_customer. 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-2026-7550	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected is an unknown function of the file /ajax.php?action=save_customer. The manipulation of the argument ID 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-2026-7389	A security vulnerability has been detected in EyouCMS up to 1.7.9. The affected element is the function GetSortData of the file application/common.php. The manipulation of the argument sort_asc leads to sql injection. The attack may be initiated 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-2026-7386	A flaw has been found in fatbobman mail-mcp-bridge up to 1.3.3. Affected is an unknown function of the file src/mail_mcp_server.py. Executing a manipulation of the argument message_ids can lead to path traversal. The attack can be executed remotely. The exploit has been published and may be used. Upgrading to version 1.3.4 is able to address this issue. This patch is called 638b162b26532e32fa8d8047f638537dbdfe197a. Upgrading the affected component is recommended.	7.3	More Details
CVE-2026-7810	A flaw has been found in UsamaK98 python-notebook-mcp up to a05a232815809a7e425b5fa7be26e0d4369894c2. Impacted is the function create_notebook/read_notebook/edit_cell/add_cell of the file server.py. This manipulation causes path traversal. It is possible to initiate the attack remotely. The exploit has been published 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-2026-7811	A vulnerability has been found in 54yyyu code-mcp up to 4cfc4643541a110c906d93635b391bf7e357f4a8. The affected element is the function is_safe_path of the file src/code_mcp/server.py of the component MCP File Handler. Such manipulation leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may 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-2026-7812	A vulnerability was found in 54yyyu code-mcp up to 4cfc4643541a110c906d93635b391bf7e357f4a8. The impacted element is the function git_operation of the file src/code_mcp/server.py of the component MCP Tool. Performing a manipulation of the argument operation results in command injection. The attack can be initiated remotely. The exploit has been made public and could be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of 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-2026-7555	A vulnerability was identified in itsourcecode Electronic Judging System 1.0. This affects an unknown part of the file /intrams/login.php. Such manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-7632	A vulnerability was determined in code-projects Online Hospital Management System 1.0. This affects an unknown function of the file /viewappointment.php. This manipulation of the argument delid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
	A vulnerability has been found in Acrel Electrical EEMS Enterprise Power Operation and Maintenance Cloud Platform 1.3.0. This affects		

CVE-2026-7695	an unknown function of the file /SubstationWEBV2/main/elecMaxMinAvgValue. The manipulation of the argument fCircuitids leads to sql injection. The attack may be initiated remotely. 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.	7.3	More Details
CVE-2026-7594	A vulnerability was detected in Flux159 mcp-game-asset-gen 0.1.0. Affected is the function image_to_3d_async of the file src/index.ts of the component MCP Interface. The manipulation of the argument statusFile results in path traversal. The attack can be executed 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-2026-7727	A vulnerability was determined in Shandong Hoteam Software PDM Product Data Management System up to 8.3.9. This affects the function GetQueryMachineGridOnePageData of the file /Base/BaseService.asmx/DataService. This manipulation of the argument SortOrder causes sql injection. The attack can be initiated remotely. Upgrading to version 8.3.10 is able to mitigate this issue. You should upgrade the affected component.	7.3	More Details
CVE-2026-7723	A flaw has been found in PrefectHQ prefect up to 3.6.13. Affected is an unknown function of the file /api/events/in of the component WebSocket Endpoint. Executing a manipulation can lead to missing authentication. The attack may be performed from remote. The exploit has been published and may be used. Upgrading to version 3.6.14 is able to address this issue. This patch is called f8afecadf88ea5f73694dafa3a365b9d8fae1ad6. It is recommended to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	7.3	More Details
CVE-2026-7711	A weakness has been identified in MindsDB up to 26.01. This impacts the function exec of the file mindsdb/integrations/handlers/byom_handler/proc_wrapper.py of the component Engine Handler. Executing a manipulation can lead to unrestricted upload. The attack can be executed 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.	7.3	More Details
CVE-2026-7710	A security flaw has been discovered in YunaiV yudao-cloud up to 3.8.0. This affects the function doFilterInternal of the file JwtAuthenticationTokenFilter.java of the component Ruoyi-Vue-Pro. Performing a manipulation of the argument mock-token results in improper authentication. Remote exploitation of the attack is possible. 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.	7.3	More Details
CVE-2026-7703	A flaw has been found in AV Stumpfl Pixera Two Media Server up to 25.2 R2. Impacted is an unknown function of the component Websocket API. This manipulation causes code injection. The attack can be initiated remotely. The exploit has been published and may be used. Upgrading to version 25.2 R3 is recommended to address this issue. Upgrading the affected component is advised.	7.3	More Details
CVE-2026-7698	A vulnerability was identified in Tiandy Easy7 Integrated Management Platform 7.17.0. Affected by this vulnerability is an unknown functionality of the file /Easy7/rest/systemInfo/updateDbBackupInfo. Such manipulation of the argument week leads to os command injection. The attack can be executed 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.	7.3	More Details
CVE-2026-7598	A security vulnerability has been detected in libssh2 up to 1.11.1. The impacted element is the function userauth_password of the file src/userauth.c. Such manipulation of the argument username_len/password_len leads to integer overflow. The attack may be launched remotely. The name of the patch is 256d04b60d80bf1190e96b0ad1e91b2174d744b1. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2026-7694	A flaw has been found in Acrel Electrical ECEMS Enterprise Microgrid Energy Efficiency Management System 1.3.0. The impacted element is an unknown function of the file /SubstationWEBV2/main/elecMaxMinAvgValue. Executing a manipulation of the argument fCircuitids can lead to sql injection. The attack can be launched 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.	7.3	More Details
CVE-2026-7735	A vulnerability was found in osrg GoBGP up to 4.3.0. Affected is the function PathAttributeAigp.DecodeFromBytes of the file pkg/packet/bgp/bgp.go of the component AIGP Attribute Parser. Performing a manipulation results in buffer overflow. It is possible to initiate the attack remotely. Upgrading to version 4.4.0 is able to address this issue. The patch is named 51ad1ada06cb41ce47b7066799981816f50b7ced. The affected component should be upgraded.	7.3	More Details
CVE-2026-7593	A security vulnerability has been detected in Sunwood-ai-labs command-executor-mcp-server up to 0.1.0. This impacts the function execute_command of the file src/index.ts of the component MCP Interface. The manipulation leads to os command injection. Remote exploitation of the attack is possible. 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-2026-7679	A security flaw has been discovered in YunaiV yudao-cloud up to 2026.01. This impacts the function getAccessToken of the file yudao-module-system-biz/src/main/java/io/github/ruoyi/common/oauth2/service/impl/OAuth2TokenServiceImpl.java. Performing a manipulation results in improper authentication. The attack can 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.	7.3	More Details
CVE-2026-7670	A flaw has been found in Jinher OA 1.0. The affected element is an unknown function of the file /C6/JHSoft.Web.PlanSummarize/UserSel.aspx. This manipulation of the argument DeptIDList causes sql injection. 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.	7.3	More Details
CVE-2026-7668	A vulnerability was identified in MikroTik RouterOS 6.49.8. This vulnerability affects the function ASN1_STRING_data in the library nova/lib/www/scep.p of the component SCEP Endpoint. The manipulation of the argument transactionID/messageType leads to out-of-bounds read. 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.	7.3	More Details
CVE-2026-7644	A vulnerability has been found in ChatGPTNextWeb NextChat up to 2.16.1. Affected is the function addMcpServer of the file app/mcp/actions.ts. The manipulation leads to improper authorization. Remote exploitation of the attack is possible. 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-2026-7630	A vulnerability has been found in innocommerce InnoShop up to 0.7.8. The affected element is the function InstallServiceProvider::boot of the file innopacks/install/src/InstallServiceProvider.php of the component Installation Endpoint. The manipulation leads to improper authentication. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The identifier of the patch is 45758e4ec22451ab944ae2ae826b1e70f6450dc9. It is recommended to apply a patch to fix this issue.	7.3	More Details

CVE-2026-7592	A weakness has been identified in itsourcecode Courier Management System 1.0. This affects an unknown function of the file /edit_staff.php. 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-2026-7733	A flaw has been found in funadmin up to 7.1.0-rc6. This affects the function UploadService::chunkUpload of the file app/common/service/UploadService.php of the component Frontend Chunked Upload Endpoint. This manipulation of the argument File causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been published and may be used. Patch name: 59. To fix this issue, it is recommended to deploy a patch.	7.3	More Details
CVE-2026-7590	A vulnerability was identified in eyal-gor p_69_branch_monkey_mcp up to 69bc71874ce40050ef45fde5a435855f18af3373. The affected element is an unknown function of the file branch_monkey_mcp/bridge_and_local_actions/routes/advanced.py of the component Preview Endpoint. Such manipulation of the argument dev_script leads to os command injection. The attack can be launched remotely. The exploit is publicly available and might be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-7417	A vulnerability was found in Algovate xhs-mcp 0.8.11. This affects the function xhs_publish_content of the file src/server/mcp.server.ts of the component MCP Interface. Performing a manipulation of the argument media_paths results in server-side request forgery. The attack may 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.	7.3	More Details
CVE-2026-7416	A vulnerability was found in PolarVista xcode-mcp-server 1.0.0. This issue affects the function build_project/run_tests of the file src/index.ts of the component MCP Interface. The manipulation of the argument Request results in os command injection. The attack may be launched 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.	7.3	More Details
CVE-2026-7736	A vulnerability was determined in osrg GoBGP up to 4.3.0. Affected by this vulnerability is the function parseRibEntry of the file pkg/packet/mrt/mrt.go. Executing a manipulation can lead to integer underflow. It is possible to launch the attack remotely. Upgrading to version 4.4.0 addresses this issue. This patch is called 76d911046344a3923cbe573364197aa081944592. It is suggested to upgrade the affected component.	7.3	More Details
CVE-2026-7400	A security vulnerability has been detected in geekgod382 filesystem-mcp-server 1.0.0. This issue affects the function is_path_allowed of the file server.py of the component read_file_tool/write_file_tool. Such manipulation leads to path traversal. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 1.1.0 is capable of addressing this issue. The name of the patch is 45364545fc60dc80aadcd4379f08042d3d3d292e. Upgrading the affected component is advised.	7.3	More Details
CVE-2026-7468	A security vulnerability has been detected in 1024-lab smart-admin up to 3.30.0. This affects an unknown function of the file /smart-admin-api/druid/index.html of the component Demo Site. The manipulation leads to improper access controls. The attack may be initiated 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-2025-50328	A vulnerability in B1 Free Archiver v1.5.86 allows files extracted from downloaded archives to bypass Windows Mark of the Web (MotW) protections. When an archive is downloaded from the internet and extracted using B1 Free Archiver, the software fails to propagate the 'Zone.Identifier' alternate data stream to the extracted files. As a result, these files can be executed without triggering Windows Defender SmartScreen warnings or security prompts, enabling untrusted code execution without standard security restrictions.	7.3	More Details
CVE-2026-7446	A vulnerability was detected in VetCoders mcp-server-semgrep 1.0.0. This affects the function analyze_results/filter_results/export_results/compare_results/scan_directory/create_rule of the file src/index.ts of the component MCP Interface. The manipulation of the argument ID results in os command injection. The attack can be executed remotely. The exploit is now public and may be used. Upgrading to version 1.0.1 is able to mitigate this issue. The patch is identified as 141335da044e53c3f5b315e0386e01238405b771. It is advisable to upgrade the affected component.	7.3	More Details
CVE-2026-7404	A weakness has been identified in getsimpletool mcpo-simple-server up to 0.2.0. Affected is the function delete_shared_prompt of the file src/mcpo_simple_server/services/prompt_manager/base_manager.py. This manipulation of the argument detail causes relative path traversal. 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-2026-7443	A weakness has been identified in BurtTheCoder mcp-dnstwist up to 1.0.4. Affected by this vulnerability is the function fuzz_domain of the file src/index.ts of the component MCP Interface. Executing a manipulation of the argument Request 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. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-42615	GCHQ CyberChef before 11.0.0 allows XSS via Show Base64 offsets, as demonstrated by the /#recipe=Show_Base64_offsets('%3Cscript substring.	7.2	More Details
CVE-2026-7857	A vulnerability has been found in D-Link DI-8100 16.07.26A1. This vulnerability affects the function sprintf of the file /user_group.asp of the component CGI Handler. The manipulation leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.2	More Details
CVE-2026-6229	The Royal Elementor Addons plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 1.7.1057. This is due to insufficient validation of user-supplied URLs in the render_csv_data() function, which can be bypassed by including 'docs.google.com/spreadsheets' in a query parameter, and the subsequent use of these URLs in fopen() calls without blocking internal or private network addresses. This makes it possible for authenticated attackers, with Contributor-level access and above, to make requests to arbitrary URLs and retrieve sensitive information from internal services.	7.2	More Details
CVE-2026-7856	A flaw has been found in D-Link DI-8100 16.07.26A1. This affects an unknown part of the file /url_member.asp of the component Web Management Interface. Executing a manipulation of the argument Name can lead to buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	7.2	More Details
CVE-2026-7833	A weakness has been identified in EFM ipTIME C200 up to 1.092. This vulnerability affects the function sub_408F90 of the file /cgi/iux_set.cgi of the component ApplyRestore Endpoint. This manipulation of the argument RestoreFile causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor	7.2	More Details

	was contacted early about this disclosure but did not respond in any way.		
CVE-2026-5113	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Consent field hidden inputs in versions up to and including 2.10.0. This is due to a flawed state validation mechanism that fails open when input is sanitized by wp_kses(), combined with insufficient output escaping. The state validation logic creates two hashes (raw input and wp_kses-sanitized input) and only fails validation if BOTH hashes don't match the original state. When an attacker injects XSS payloads using tags stripped by wp_kses() (like <svg>), the sanitized hash matches while the malicious raw value is preserved and saved to the database. When administrators view the Entries List page, the stored malicious consent label is retrieved and output without escaping, causing the XSS payload to execute. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in entries that will execute whenever an authenticated administrator accesses the entries list page.	7.2	More Details
CVE-2026-5324	The Brizy – Page Builder plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting in all versions up to, and including, 2.8.11 This is due to a combination of missing nonce verification for unauthenticated form submissions, insufficient handling of FileUpload fields when no file is uploaded, and the reversal of security encoding via html_entity_decode() followed by unescaped output in the admin view. The submit_form() function skips nonce verification for non-logged-in users (api.php:198). The handleFileTypeFields() function fails to overwrite user-supplied values when no file is attached. While htmlentities() is applied during storage, html_entity_decode() reverses this on display (form-entries.php:79). The form-data.php template outputs FileUpload values directly in href attributes without esc_url(). This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the form Leads page.	7.2	More Details
CVE-2026-7246	Pallets Click, versions 8.3.2 and below, contain a command injection vulnerability in the click.edit() function, allowing attackers to pass arbitrary OS commands from an unprivileged account.	7.2	More Details
CVE-2026-7851	A vulnerability was identified in D-Link DI-8100 16.07.26A1. This affects the function sprintf of the file yyxz.asp. The manipulation of the argument ID leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.2	More Details
CVE-2026-5112	The Gravity Forms plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting in versions up to and including 2.10.0. This is due to insufficient input validation and output escaping of Calculation Product field product names when rendered inside Repeater fields. The validate() method in the GF_Field_Calculation class only validates the quantity field (.3) and completely ignores the product name field (.1), allowing malicious HTML to pass through validation. When the value is saved, the sanitize_entry_value() method returns the raw value without sanitization for fields where HTML is not expected. Subsequently, when an entry is viewed in wp-admin, the get_value_entry_detail() method concatenates the unescaped product name directly into the output string, which is then rendered by the repeater's get_value_entry_detail() method without further escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts via form submissions that will execute whenever an authenticated administrator with the gravityforms_view_entries capability accesses the entry detail page.	7.2	More Details
CVE-2026-5109	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 2.10.0. This is due to insufficient validation and output escaping of Product Option field values. The vulnerability exists because the state validation function accepts submitted values where the wp_kses()-sanitized version matches a legitimate option value, but then stores the raw unsanitized value in the database. When administrators view entry details via the Order Summary section, the option_label is output directly without escaping (view-order-summary.php line 32), executing the injected JavaScript. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in entry data that will execute whenever an administrator accesses the entry details page.	7.2	More Details
CVE-2026-5111	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 2.10.0. This is due to insufficient input validation and output escaping on Hidden Product field values when used inside Repeater fields, where repeater subfields bypass state validation checks and the Hidden Product validate() method only validates the quantity field while ignoring the product name field that is later output without proper escaping in the get_value_entry_detail() method. This makes it possible for unauthenticated attackers to inject arbitrary web scripts through form submissions that will execute whenever an administrator views the entry details.	7.2	More Details
CVE-2026-5110	The Gravity Forms plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting in versions up to and including 2.10.0. This is due to insufficient input validation and output escaping in the SingleProduct field when used inside a Repeater field. When SingleProduct fields are nested within Repeater fields, the validation flow bypasses the state validation mechanism (failed_state_validation()) that would normally prevent tampering with field values. The validate_subfield() method only calls the field's validate() method, which for SingleProduct fields only validates the quantity field and does not check the product name field for tampering. As a result, an attacker can inject arbitrary HTML and JavaScript into the product name field (input .1). This malicious input is then saved to the database without sanitization because sanitize_entry_value() returns raw values when HTML is not expected for the field type. When an administrator views the entry in wp-admin/admin.php?page=gf_entries, the get_value_entry_detail() method outputs the product name without escaping, causing the stored XSS payload to execute in the administrator's browser. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses an entry containing the malicious payload.	7.2	More Details
CVE-2018-25309	MyBB Recent threads 17.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts by creating threads with crafted subject lines. Attackers can create threads with script tags in the subject parameter to execute arbitrary JavaScript in the browsers of all users viewing the index page.	7.2	More Details
CVE-2026-7049	The PixelYourSite Pro – Your smart PIXEL (TAG) Manager plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 12.5.0.1 via the scan_video. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. The SSRF is blind because fetched response bodies are only parsed internally for YouTube/Vimeo patterns and are never returned to the attacker.	7.2	More Details
CVE-2026-4803	The Royal Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'status' parameter in the wpr_update_form_action_meta AJAX action in all versions up to, and including, 1.7.1056. This is due to insufficient input sanitization and output escaping, combined with a publicly leaked nonce that allows unauthenticated access to the AJAX handler. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via POST parameter key names in the submit_nex_form() function in versions up to, and including, 9.1.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute	7.2	More Details

5063	whenever a user accesses an injected page.		
CVE-2026-7461	Improper neutralization of inputs used in an OS command in the FSx Windows File Server volume mounting component in Amazon ECS Agent on Windows before version 1.103.0 might allow a remote authenticated threat actor to execute shell commands with SYSTEM privileges on the underlying host via a specially crafted username field in an ECS task definition. This issue requires permissions to register ECS task definitions or write to the Secrets Manager or SSM Parameter Store credentials used by the FSx volume configuration. To remediate this issue, users should upgrade to version 1.103.0.	7.2	More Details
CVE-2026-38751	OpenSTAManager version 2.10 and earlier contains an arbitrary file upload vulnerability in the module update functionality (modules/aggiornamenti/upload_modules.php)	7.2	More Details
CVE-2026-7490	CTMS and CPAS developed by Sunnet has an Arbitrary File Upload vulnerability, allowing privileged remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2026-7435	SSCMS v7.4.0 contains a SQL injection vulnerability in the stl:sqlContent tag where the queryString attribute is passed directly to database execution without parameterization or sanitization. Attackers can craft encrypted payloads submitted to the /api/stl/actions/dynamic endpoint to execute arbitrary SQL statements, leading to unauthorized database access, data disclosure, authentication bypass, data modification, or complete database compromise.	7.2	More Details
CVE-2026-3120	Improper Control of Generation of Code ('Code Injection') vulnerability in Profelis Information and Consulting Trade and Industry Limited Company SambaBox allows OS Command Injection. This issue affects SambaBox: from 5.1 before 5.3.	7.2	More Details
CVE-2026-31766	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate doorbell_offset in user queue creation amdgpu_userq_get_doorbell_index() passes the user-provided doorbell_offset to amdgpu_doorbell_index_on_bar() without bounds checking. An arbitrarily large doorbell_offset can cause the calculated doorbell index to fall outside the allocated doorbell BO, potentially corrupting kernel doorbell space. Validate that doorbell_offset falls within the doorbell BO before computing the BAR index, using u64 arithmetic to prevent overflow. (cherry picked from commit de1ef4ffd70e1d15f0bf584fd22b1f28cbd5e2ec)	7.1	More Details
CVE-2026-43006	In the Linux kernel, the following vulnerability has been resolved: io_uring/rsrc: reject zero-length fixed buffer import validate_fixed_range() admits buf_addr at the exact end of the registered region when len is zero, because the check uses strict greater-than (buf_end > imu->ubuf + imu->len). io_import_fixed() then computes offset == imu->len, which causes the bvec skip logic to advance past the last bio_vec entry and read bv_offset from out-of-bounds slab memory. Return early from io_import_fixed() when len is zero. A zero-length import has no data to transfer and should not walk the bvec array at all. BUG: KASAN: slab-out-of-bounds in io_import_reg_buf+0x697/0x7f0 Read of size 4 at addr ffff888002bcc254 by task poc/103 Call Trace: io_import_reg_buf+0x697/0x7f0 io_write_fixed+0xd9/0x250 __io_issue_sqe+0xad/0x710 io_issue_sqe+0x7d/0x1100 io_submit_sqes+0x86a/0x23c0 __do_sys_io_uring_enter+0xa98/0x1590 Allocated by task 103: The buggy address is located 12 bytes to the right of allocated 584-byte region [ffff888002bcc000, ffff888002bcc248)	7.1	More Details
CVE-2026-43616	Detect-It-Easy prior to 3.21 contains a path traversal vulnerability that allows attackers to write arbitrary files to the filesystem by crafting malicious archive entries with relative traversal sequences or absolute paths. Attackers can exploit insufficient path normalization during archive extraction to write files outside the intended extraction directory and achieve persistent code execution by overwriting user startup scripts.	7.1	More Details
CVE-2026-40563	Description: Improper Control of Generation of Code ('Code Injection') vulnerability in Apache Atlas Apache Atlas exposes a DSL search endpoint that accepts user-supplied query strings. Attacker can alter Gremlin traversal logic within grammar-allowed characters to access unintended data Affect Version: This issue affects Apache Atlas: from 0.8 through 2.4.0. For the affect version >= 2.0, vulnerability is only when Atlas is deployed with below non-default configuration. atlas.dsl.executor.traversal=false Mitigation: Users are recommended to upgrade to version 2.5.0, which fixes the issue.	7.1	More Details
CVE-2026-42476	Two heap-based out-of-bounds read vulnerabilities in the STL ASCII file parser in Open CASCADE Technology (OCCT) V8_0_0_rc5 exist in RWStl_Reader::ReadAscii because buffers returned by Standard_ReadLineBuffer::ReadLine() are not properly length-validated before strncasecmp or direct byte access. User-assisted attackers can trigger these issues by persuading a victim to open a crafted STL file with extremely short lines, resulting in a denial of service or possible information disclosure.	7.1	More Details
CVE-2026-42477	A heap-based out-of-bounds read vulnerability in RWObj_Reader::read in the OBJ file parser in Open CASCADE Technology (OCCT) V8_0_0_rc5 allows user-assisted attackers to cause a denial of service or obtain sensitive information by persuading a victim to open a crafted OBJ file. The issue occurs because Standard_ReadLineBuffer::ReadLine() can return a 1-byte buffer for a minimal OBJ line, and RWObj_Reader::read() calls pushIndices(aLine + 2) without validating the buffer length.	7.1	More Details
CVE-2026-37535	openxc/isotp-c thru commit 5a5d19245f65189202719321facd49ce6f5d46ac (2021-08-09) contains an out-of-bounds read in the ISO-TP Single Frame receive handler, where the 4-bit payload length nibble is used directly as the memcpy size without validating it against the actual CAN data length. A malicious CAN frame with an oversized length nibble can cause memory reads beyond the buffer, allowing attackers to cause a denial of service, or gain sensitive information.	7.1	More Details
CVE-2026-31774	In the Linux kernel, the following vulnerability has been resolved: io_uring/net: fix slab-out-of-bounds read in io_bundle_nbufs() sqe->len is __u32 but gets stored into sr->len which is int. When userspace passes sqe->len values exceeding INT_MAX (e.g. 0xFFFFFFFF), sr->len overflows to a negative value. This negative value propagates through the bundle recv/send path: 1. io_recv(): sel.val = sr->len (ssize_t gets -1) 2. io_recv_buf_select(): arg.max_len = sel->val (size_t gets 0xFFFFFFFFFFFFFFFF) 3. io_ring_buffers_peek(): buf->len is not clamped because max_len is astronomically large 4. iov[].iov_len = 0xFFFFFFFF flows into io_bundle_nbufs() 5. io_bundle_nbufs(): min_t(int, 0xFFFFFFFF, ret) yields -1, causing ret to increase instead of decrease, creating an infinite loop that reads past the allocated iov[] array This results in a slab-out-of-bounds read in io_bundle_nbufs() from the kmalloc-64 slab, as nbufs increments past the allocated iovec entries. BUG: KASAN: slab-out-of-bounds in io_bundle_nbufs+0x128/0x160 Read of size 8 at addr ffff888100ae05c8 by task exp/145 Call Trace: io_bundle_nbufs+0x128/0x160 io_recv_finish+0x117/0xe20 io_recv+0x2db/0x1160 Fix this by rejecting negative sr->len values early in both io_sendmsg_prep() and io_recvmsg_prep(). Since sqe->len is __u32, any value > INT_MAX indicates overflow and is not a valid length.	7.1	More Details
CVE-2026-43028	In the Linux kernel, the following vulnerability has been resolved: netfilter: x_tables: ensure names are nul-terminated Reject names that lack a \0 character before feeding them to functions that expect c-strings. Fixes tag is the most recent commit that needs this change.	7.1	More Details
	The Paid Memberships Pro plugin for WordPress is vulnerable to unauthorized modification and disruption of Stripe webhook		

CVE-2026-4100	configuration in all versions up to, and including, 3.6.5. This is due to missing capability checks on the `wp_ajax_pmpro_stripe_create_webhook`, `wp_ajax_pmpro_stripe_delete_webhook`, and `wp_ajax_pmpro_stripe_rebuild_webhook` AJAX handlers. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete, create, or rebuild the site's Stripe webhook, disrupting all payment processing, subscription renewal synchronization, cancellation handling, and failed payment management.	7.1	More Details
CVE-2026-43042	In the Linux kernel, the following vulnerability has been resolved: mpls: add seqcount to protect the platform_label{,s} pair The RCU-protected codepaths (mpls_forward, mpls_dump_routes) can have an inconsistent view of platform_labels vs platform_label in case of a concurrent resize (resize_platform_label_table, under platform_mutex). This can lead to OOB accesses. This patch adds a seqcount, so that we get a consistent snapshot. Note that mpls_label_ok is also susceptible to this, so the check against RTA_DST in rtm_to_route_config, done outside platform_mutex, is not sufficient. This value gets passed to mpls_label_ok once more in both mpls_route_add and mpls_route_del, so there is no issue, but that additional check must not be removed.	7.1	More Details
CVE-2026-37532	AGL agl-service-can-low-level thru 17.1.12 contains a heap buffer over-read in the isotp-c library. In isotp_continue_receive (receive.c:87-89), the payload_length for a Single Frame is extracted from a 4-bit nibble in the CAN frame data, yielding values 0-15. However, a standard CAN frame is only 8 bytes, with payload starting at data[1] (7 bytes available). When payload_length exceeds the available data (e.g., nibble=15 but only 7 payload bytes exist), memcpy(message.payload, &data[1], payload_length) reads up to 8 bytes past the end of the data buffer.	7.1	More Details
CVE-2026-31707	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate response sizes in ipc_validate_msg() ipc_validate_msg() computes the expected message size for each response type by adding (or multiplying) attacker-controlled fields from the daemon response to a fixed struct size in unsigned int arithmetic. Three cases can overflow: KSMBD_EVENT_RPC_REQUEST: msg_sz = sizeof(struct ksmbd_rpc_command) + resp->payload_sz; KSMBD_EVENT_SHARE_CONFIG_REQUEST: msg_sz = sizeof(struct ksmbd_share_config_response) + resp->payload_sz; KSMBD_EVENT_LOGIN_REQUEST_EXT: msg_sz = sizeof(struct ksmbd_login_response_ext) + resp->ngroups * sizeof(gid_t); resp->payload_sz is __u32 and resp->ngroups is __s32. Each addition can wrap in unsigned int; the multiplication by sizeof(gid_t) mixes signed and size_t, so a negative ngroups is converted to SIZE_MAX before the multiply. A wrapped value of msg_sz that happens to equal entry->msg_sz bypasses the size check on the next line, and downstream consumers (smb2pdu.c:6742 memcpy using rpc_resp->payload_sz, kmemdup in ksmbd_alloc_user using resp_ext->ngroups) then trust the unverified length. Use check_add_overflow() on the RPC_REQUEST and SHARE_CONFIG_REQUEST paths to detect integer overflow without constraining functional payload size; userspace ksmbd-tools grows NDR responses in 4096-byte chunks for calls like NetShareEnumAll, so a hard transport cap is unworkable on the response side. For LOGIN_REQUEST_EXT, reject resp->ngroups outside the signed [0, NGROUPS_MAX] range up front and report the error from ipc_validate_msg() so it fires at the IPC boundary; with that bound the subsequent multiplication and addition stay well below UINT_MAX. The now-redundant ngroups check and pr_err in ksmbd_alloc_user() are removed. This is the response-side analogue of aab98e2dbd64 ("ksmbd: fix integer overflows on 32 bit systems"), which hardened the request side.	7.1	More Details
CVE-2025-13030	All versions of the package django-mdeditor are vulnerable to Missing Authentication for Critical Function in the image upload endpoint. An attacker can upload malicious files and achieve arbitrary code execution since this endpoint lacks authentication protection and proper sanitisation of file names.	7.1	More Details
CVE-2026-22070	ColorOS Assistant has an unauthenticated start-download channel, leading to file path traversal.	7.1	More Details
CVE-2026-31697	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp: Don't attempt to copy ID to userspace if PSP command failed When retrieving the ID for the CPU, don't attempt to copy the ID blob to userspace if the firmware command failed. If the failure was due to an invalid length, i.e. the userspace buffer+length was too small, copying the number of bytes _firmware_ requires will overflow the kernel-allocated buffer and leak data to userspace. BUG: KASAN: slab-out-of-bounds in instrument_copy_to_user ../include/linux/instrumented.h:129 [inline] BUG: KASAN: slab-out-of-bounds in _inline_copy_to_user ../include/linux/uaccess.h:205 [inline] BUG: KASAN: slab-out-of-bounds in _copy_to_user+0x66/0xa0 ../lib/usercopy.c:26 Read of size 64 at addr ffff8881867f5960 by task syz.0.906/24388 CPU: 130 UID: 0 PID: 24388 Comm: syz.0.906 Tainted: G U O 7.0.0-smp-DEV #28 PREEMPTLAZY Tainted: [U]=USER, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 12.62.0-0 11/19/2025 Call Trace: <TASK> dump_stack_lvl+0xc5/0x110 ../lib/dump_stack.c:120 print_address_description ../mm/kasan/report.c:378 [inline] print_report+0xbc/0x260 ../mm/kasan/report.c:482 kasan_report+0xa2/0xe0 ../mm/kasan/report.c:595 check_region_inline ../mm/kasan/generic.c:-1 [inline] kasan_check_range+0x264/0x2c0 ../mm/kasan/generic.c:200 instrument_copy_to_user ../include/linux/instrumented.h:129 [inline] _inline_copy_to_user ../include/linux/uaccess.h:205 [inline] _copy_to_user+0x66/0xa0 ../lib/usercopy.c:26 copy_to_user ../include/linux/uaccess.h:236 [inline] sev_ioctl_do_get_id2+0x361/0x490 ../drivers/crypto/ccp/sev-dev.c:2222 sev_ioctl+0x25f/0x490 ../drivers/crypto/ccp/sev-dev.c:2575 vfs_ioctl ../fs/ioctl.c:51 [inline] __do_sys_ioctl ../fs/ioctl.c:597 [inline] __se_sys_ioctl+0x11d/0x1b0 ../fs/ioctl.c:583 do_syscall_x64 ../arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe0/0x800 ../arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> WARN if the driver says the command succeeded, but the firmware error code says otherwise, as __sev_do_cmd_locked() is expected to return -EIO on any firwmware error.	7.1	More Details
CVE-2026-31699	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp: Don't attempt to copy CSR to userspace if PSP command failed When retrieving the PEK CSR, don't attempt to copy the blob to userspace if the firmware command failed. If the failure was due to an invalid length, i.e. the userspace buffer+length was too small, copying the number of bytes _firmware_ requires will overflow the kernel-allocated buffer and leak data to userspace. BUG: KASAN: slab-out-of-bounds in instrument_copy_to_user ../include/linux/instrumented.h:129 [inline] BUG: KASAN: slab-out-of-bounds in _inline_copy_to_user ../include/linux/uaccess.h:205 [inline] BUG: KASAN: slab-out-of-bounds in _copy_to_user+0x66/0xa0 ../lib/usercopy.c:26 Read of size 2084 at addr ffff898144612e20 by task syz.9.219/21405 CPU: 14 UID: 0 PID: 21405 Comm: syz.9.219 Tainted: G U O 7.0.0-smp-DEV #28 PREEMPTLAZY Tainted: [U]=USER, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 12.62.0-0 11/19/2025 Call Trace: <TASK> dump_stack_lvl+0xc5/0x110 ../lib/dump_stack.c:120 print_address_description ../mm/kasan/report.c:378 [inline] print_report+0xbc/0x260 ../mm/kasan/report.c:482 kasan_report+0xa2/0xe0 ../mm/kasan/report.c:595 check_region_inline ../mm/kasan/generic.c:-1 [inline] kasan_check_range+0x264/0x2c0 ../mm/kasan/generic.c:200 instrument_copy_to_user ../include/linux/instrumented.h:129 [inline] _inline_copy_to_user ../include/linux/uaccess.h:205 [inline] _copy_to_user+0x66/0xa0 ../lib/usercopy.c:26 copy_to_user ../include/linux/uaccess.h:236 [inline] sev_ioctl_do_pek_csr+0x31f/0x590 ../drivers/crypto/ccp/sev-dev.c:1872 sev_ioctl+0x3a4/0x490 ../drivers/crypto/ccp/sev-dev.c:2562 vfs_ioctl ../fs/ioctl.c:51 [inline] __do_sys_ioctl ../fs/ioctl.c:597 [inline] __se_sys_ioctl+0x11d/0x1b0 ../fs/ioctl.c:583 do_syscall_x64 ../arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe0/0x800 ../arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> WARN if the driver says the command succeeded, but the firmware error code says otherwise, as __sev_do_cmd_locked() is expected to return -EIO on any firwmware error.	7.1	More Details
	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp: Don't attempt to copy PDH cert to userspace if PSP		

CVE-2026-31698	command failed When retrieving the PDH cert, don't attempt to copy the blobs to userspace if the firmware command failed. If the failure was due to an invalid length, i.e. the userspace buffer+length was too small, copying the number of bytes _firmware_ requires will overflow the kernel-allocated buffer and leak data to userspace. BUG: KASAN: slab-out-of-bounds in instrument_copy_to_user ../include/linux/instrumented.h:129 [inline] BUG: KASAN: slab-out-of-bounds in _inline_copy_to_user ../include/linux/uaccess.h:205 [inline] BUG: KASAN: slab-out-of-bounds in _copy_to_user+0x66/0xa0 ../lib/usercopy.c:26 Read of size 2084 at addr ffff8885c4ab8aa0 by task syz.0.186/21033 CPU: 51 UID: 0 PID: 21033 Comm: syz.0.186 Tainted: G U O 7.0.0-smp-DEV #28 PREEMPTLAZY Tainted: [U]=USER, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 34.84.12-0 11/17/2025 Call Trace: <TASK> dump_stack_lvl+0xc5/0x110 ../lib/dump_stack.c:120 print_address_description ../mm/kasan/report.c:378 [inline] print_report+0xbc/0x260 ../mm/kasan/report.c:482 kasan_report+0xa2/0xe0 ../mm/kasan/report.c:595 check_region_inline ../mm/kasan/generic.c:-1 [inline] kasan_check_range+0x264/0x2c0 ../mm/kasan/generic.c:200 instrument_copy_to_user ../include/linux/instrumented.h:129 [inline] _inline_copy_to_user ../include/linux/uaccess.h:205 [inline] _copy_to_user+0x66/0xa0 ../lib/usercopy.c:26 copy_to_user ../include/linux/uaccess.h:236 [inline] sev_ioctl_do_pdh_export+0x3d3/0x7c0 ../drivers/crypto/ccp/sev-dev.c:2347 sev_ioctl+0x2a2/0x490 ../drivers/crypto/ccp/sev-dev.c:2568 vfs_ioctl ../fs/ioctl.c:51 [inline] __do_sys_ioctl ../fs/ioctl.c:597 [inline] __se_sys_ioctl+0x11d/0x1b0 ../fs/ioctl.c:583 do_syscall_x64 ../arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe0/0x800 ../arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> WARN if the driver says the command succeeded, but the firmware error code says otherwise, as __sev_do_cmd_locked() is expected to return -EIO on any firwmware error.	7.1	More Details
CVE-2026-42652	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpeverest User Registration user-registration allows Reflected XSS.This issue affects User Registration: from n/a through <= 5.1.5.	7.1	More Details
CVE-2026-35155	Dell iDRAC10, versions 1.20.70.50 and 1.30.05.10, contains an Insufficiently Protected Credentials vulnerability. A race condition vulnerability exists that could allow an authenticated low-privileged attacker to gain elevated access.	7.1	More Details
CVE-2026-7832	A security flaw has been discovered in IObit Advanced SystemCare 19. This affects an unknown part of the file ASC.exe of the component Service. The manipulation results in symlink following. Attacking locally is a requirement. This attack is characterized by high complexity. It is indicated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks.	7.0	More Details
CVE-2026-5656	Profile import path traversal in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service and possible code execution	7.0	More Details
CVE-2026-37503	Cross-Site Scripting (XSS) in V2Board thru 1.7.4. The custom_html field in theme configuration is rendered using Blade unescaped output in public/theme/v2board/dashboard.blade.php. An admin can inject arbitrary JavaScript via the saveThemeConfig API. All site visitors execute the payload, enabling cookie theft, session hijacking, or phishing.	6.9	More Details
CVE-2026-0205	A post-authentication Path Traversal vulnerability in SonicOS allows an attacker to interact with usually restricted services.	6.8	More Details
CVE-2026-43535	OpenClaw before 2026.4.14 contains an authorization context reuse vulnerability in collect-mode queue batches that allows messages from different senders to inherit the final sender's authorization context. Attackers can exploit this by sending multiple queued messages to drain batches using a more privileged sender's context, causing earlier messages to execute with elevated permissions.	6.8	More Details
CVE-2026-20451	In slbc, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10828685; Issue ID: MSV-6504.	6.7	More Details
CVE-2026-20448	In geniezone, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10708513; Issue ID: MSV-6281.	6.7	More Details
CVE-2026-20447	In geniezone, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10724073; Issue ID: MSV-6296.	6.7	More Details
CVE-2026-3340	IBM Langflow Desktop 1.0.0 through 1.8.4 IBM Langflow is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	6.5	More Details
CVE-2026-7681	A security vulnerability has been detected in jsbroks COCO Annotator up to 0.11.1. Affected by this vulnerability is an unknown functionality of the file backend/webserver/api/datasets.py of the component Dataset API. The manipulation of the argument DatasetId leads to authorization bypass. The attack may be initiated 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.	6.5	More Details
CVE-2026-6457	The Geo Mashup plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'geo_mashup_null_fields' parameter in all versions up to, and including, 1.13.19 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-43570	OpenClaw versions 2026.3.22 before 2026.4.5 contain a symlink traversal vulnerability in remote marketplace repository path handling that allows attackers to escape the expected repository root. Attackers can exploit this by providing crafted symlink paths to access files outside the intended repository directory.	6.5	More Details
CVE-2026-43504	An issue was discovered in Prosody before 0.12.6 and 1.0.0 through 13.0.0 before 13.0.5, when mod_proxy65 is enabled. Because mod_proxy65 mishandles access control in a paused scenario, relaying of unauthenticated traffic can occur.	6.5	More Details
CVE-2026-7633	A vulnerability was identified in Totolink N300RH 6.1c.1353_B20190305. This impacts the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument FileName leads to file inclusion. The attack may be performed from remote. The exploit is publicly available and might be used.	6.5	More Details

CVE-2026-42404	Apache Neethi does not impose any restrictions on URIs when manually fetching remote policy references through the PolicyReference API. When an application explicitly calls the API to retrieve a policy from a remote URI, an outbound request is made for arbitrary protocols and internal IP adddresses. From 3.2.2, only http or https URIs are allowed, and link-local/multicast/any-local addresses are forbidden. Users are recommended to upgrade to version 3.2.2, which fixes this issue.	6.5	More Details
CVE-2026-7645	A vulnerability was found in ruvnet sublinear-time-solver 1.5.0. Affected by this vulnerability is the function export_state of the file src/consciousness-explorer/mcp/server.js of the component MCP Interface. The manipulation results in path traversal. The attack can be executed 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.	6.5	More Details
CVE-2025-36122	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow an authenticated user to cause a denial of service using a specially crafted SQL query due to improper allocation of system resources.	6.5	More Details
CVE-2026-43574	OpenClaw before 2026.4.12 contains an improper authorization vulnerability in helper-backed channels where empty resolved approver lists are interpreted as explicit approval authorization. Attackers can resolve pending approvals without proper authorization by exploiting this logic flaw if they know an approval id.	6.5	More Details
CVE-2026-28909	Users who connect to malicious registries with hostnames matching the bypass patterns will have their registry credentials exposed in plaintext. This issue is fixed in container version 0.12.3.	6.5	More Details
CVE-2026-5337	During the analysis, it was identified that authenticated attackers with Subscriber-level access or higher are able to perform an Insecure Direct Object Reference (IDOR) attack. This vulnerability exists because the Frontend File Manager Plugin WordPress plugin through 23.6 does not properly validate user authorization for the requested uploaded file when processing download requests. By modifying the value of the 'file_id' parameter in the download endpoint (e.g., http://localhost/?do=wpfm_download&file_id=40&nm_file_nonce=a36fb893f1), an attacker can access files belonging to other users, including privileged users such as administrators. This allows unauthorized access/read to sensitive data stored within the application.	6.5	More Details
CVE-2026-42367	A privilege escalation vulnerability exists in the Web Interface / ssi.cgi functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted HTTP request can lead to credentials leak. An attacker can visit a webpage to trigger this vulnerability.	6.5	More Details
CVE-2026-1577	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-2026-7714	A flaw has been found in crocodilestick Calibre-Web-Automated up to 4.0.6. Affected by this issue is some unknown functionality of the file cps/cwa_functions.py of the component Admin Endpoint. This manipulation causes missing authentication. It is possible to initiate the attack remotely. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	6.5	More Details
CVE-2026-3345	IBM Langflow Desktop <=1.8.4 Langflow could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	6.5	More Details
CVE-2026-7382	Exposure of Sensitive Information to an Unauthorized Actor, Exposure of private personal information to an unauthorized actor vulnerability in MeWare Software Development Inc. PDKS allows Excavation. This issue affects PDKS: from V16.20200313 before VMYR_3.5.2025117.	6.5	More Details
CVE-2026-22740	A WebFlux server application that processes multipart requests creates temp files for parts larger than 10 K. Under some circumstances, temp files may remain not deleted after the request is fully processed. This allows an attacker to consume available disk space. Older, unsupported versions are also affected.	6.5	More Details
CVE-2026-42475	SQL injection vulnerability in MixPHP Framework 2.x thru 2.2.17 via crafted `on` array to the joinOn function in BuildHelper.php.	6.5	More Details
CVE-2026-40950	CVE-2026-40950 is a buffer overflow vulnerability in the Secure Access server prior to 14.50. Attackers with control of a modified client can send a specially crafted message to the server and cause a denial of service	6.5	More Details
CVE-2026-28532	FRRouting before 10.5.3 contains an integer overflow vulnerability in seven OSPF Traffic Engineering and Segment Routing TLV parser functions where a uint16_t accumulator variable truncates uint32_t values returned by the TLV_SIZE() macro, causing the loop termination condition to fail while pointer advancement continues unchecked. Attackers with an established OSPF adjacency can send a crafted LS Update packet with a malicious Type 10 or Type 11 Opaque LSA to trigger out-of-bounds memory reads and crash all affected routers in the OSPF area or autonomous system.	6.5	More Details
CVE-2026-40603	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes a legacy dashboard route that returns a project's report data to any authenticated member of the same team, even when that user does not have access to the specific project. The route bypasses project-level authorization and returns the raw project object. As a result, a low-privileged same-team user can read another project's dashboard data and recover the project's stored report password from the response. This issue has been patched in version 5.0.0.	6.5	More Details
CVE-2026-35514	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, the endpoint POST /user/invited does not validate any invite token, authentication header, or session. Any unauthenticated attacker can call this endpoint directly to create a fully active account and receive a valid JWT — even when the instance has existing users and signupRestricted is enabled. This bypass is distinct from the normal registration endpoint (POST /user) which enforces signupRestricted and sets active: false pending verification. This issue has been patched in version 5.0.0.	6.5	More Details
CVE-2026-3833	A flaw was found in gnutls. This vulnerability occurs because gnutls performs case-sensitive comparisons of `nameConstraints` labels, specifically for `dNSName` (DNS) or `rfc822Name` (email) constraints within `excludedSubtrees` or `permittedSubtrees`. A remote attacker can exploit this by crafting a leaf certificate with casing differences in the Subject Alternative Name (SAN), leading to a policy bypass where a certificate that should be rejected is instead accepted. This could result in unauthorized access or information disclosure.	6.5	More Details

CVE-2026-42474	SQL injection vulnerability in MixPHP Framework 2.x thru 2.2.17 via crafted `data` array to the data function in BuildHelper.php.	6.5	More Details
CVE-2026-26461	A Command Injection vulnerability in the web management interface in Aver PTC320UV2 0.1.0000.65 allows an unauthenticated attacker to execute arbitrary commands via a crafted web request.	6.5	More Details
CVE-2026-23863	An attachment spoofing issue in WhatsApp for Windows prior to v2.3000.1032164386.258709 could have allowed maliciously formatted documents with embedded NUL bytes in the filename to be shown in the application as one type of file but run as an executable when opened. We have not seen evidence of exploitation in the wild.	6.5	More Details
CVE-2026-6262	The Betheme theme for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 28.4. This is due to the upload_icons() function workflow using a user-controlled upload path (`mfn-icon-upload`) in a filesystem move operation without constraining it to the uploads directory. This makes it possible for authenticated attackers, with contributor-level access and above, to move/delete arbitrary local files via path traversal.	6.5	More Details
CVE-2026-4502	IBM Langflow Desktop 1.2.0 through 1.8.4 Langflow could allow an authenticated attacker 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.	6.5	More Details
CVE-2026-36759	A Server-Side Request Forgery (SSRF) in the /themes/{name}/upgrade-from-uri endpoint of halo v2.22.14 allows authenticated attackers to scan internal resources via a crafted GET request.	6.5	More Details
CVE-2025-14726	The Widgets for Social Photo Feed plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the '/trustindex_feed_hook_instagram/troubleshooting' and '/trustindex_feed_hook_instagram/submit-data' REST API endpoints in all versions up to, and including, 1.8. This makes it possible for unauthenticated attackers to access and update plugin settings.	6.5	More Details
CVE-2026-30246	Fiber is a web framework for Go. In github.com/gofiber/fiber/v3 versions through 3.1.0, the default key generator in the cache middleware uses only the request path and does not include the query string. As a result, requests for the same path with different query parameters can share a cache key and receive the wrong cached response. This can cause response mix-up for query-dependent endpoints and may expose data intended for a different request. This issue is fixed after version 3.1.0.	6.5	More Details
CVE-2026-43505	An issue was discovered in Prosody before 0.12.6 and 1.0.0 through 13.0.0 before 13.0.5, when mod_proxy65 is enabled. Because mod_proxy65 mishandles access control in the activation scenario, relaying of unauthenticated traffic can occur.	6.5	More Details
CVE-2026-27644	Traccar is an open source GPS tracking system. In versions between 6.11.1 and 6.13.0, the CSV export functionality writes position data, including user-controlled device and computed attributes, to CSV output without proper escaping. An attacker can inject spreadsheet formulas through exported fields. When a manager or administrator opens the exported CSV file in spreadsheet software, this can cause formula execution and lead to command execution or data exfiltration. This has been patched in version 6.13.0.	6.5	More Details
CVE-2026-3454	The GenerateBlocks plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.2.0. This is due to missing object-level authorization checks in the /wp-json/generateblocks/v1/dynamic-tag-replacements REST endpoint. The endpoint only verifies that the user has the edit_posts capability but does not verify the user has permission to access the specific post or its associated data referenced by attacker-controlled id parameters in dynamic tag content. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive information from arbitrary posts including author email addresses and non-protected post meta values by crafting dynamic tag payloads such as {{post_meta id:<target>|key:<meta_key>}} and {{post_title id:<target>|link:author_email}}.	6.5	More Details
CVE-2026-42412	Missing Authorization vulnerability in weDevs WP User Frontend allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP User Frontend: from n/a through 4.3.1.	6.5	More Details
CVE-2026-6542	IBM Langflow OSS 1.0.0 through 1.8.4 could allow any user to supply a flow_id to read transaction logs and vertex build data belonging to other users, and to delete persisted vertex build data for another user's flow.	6.5	More Details
CVE-2026-42220	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.8, an authenticated user can call GET /api/settings and retrieve sensitive configuration values, including node.secret. The same node.secret is accepted by AuthRequired() through the X-Node-Secret header (or node_secret query parameter), causing the request to be treated as authenticated via the trusted-node path and associated with the init user. This issue has been patched in version 2.3.8.	6.5	More Details
CVE-2026-41499	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.0.0 to before version 4.14.4, multiple heap-based out-of-bounds WRITE vulnerabilities exist in parse_uname_string() (remoted_op.c). This function processes OS identification data from agents and contains a dangerous code pattern that appears in 4 locations within the same function: writing to strlen(ptr) - 1 without checking for empty strings. When the string is empty, strlen() returns 0, and 0 - 1 wraps to SIZE_MAX due to unsigned integer underflow. Due to pointer arithmetic wrapping, SIZE_MAX effectively becomes -1, causing a write exactly 1 byte before the allocated buffer. This corrupts heap metadata (e.g., the chunk size field in glibc malloc), leading to heap corruption. This issue has been patched in version 4.14.4.	6.5	More Details
CVE-2026-20449	In Modem, there is a possible system crash due to a heap buffer overflow. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01760138; Issue ID: MSV-6148.	6.5	More Details
CVE-2026-42521	Jenkins Matrix Authorization Strategy Plugin 2.0-beta-1 through 3.2.9 (both inclusive) invokes parameterless constructors of classes specified in configuration when deserializing inheritance strategies, without restricting the classes that can be instantiated, allowing attackers with Item/Configure permission to instantiate arbitrary types, which may lead to information disclosure or other impacts depending on the classes available on the classpath.	6.5	More Details
CVE-2026-	OpenClaw before 2026.4.10 contains an authorization bypass vulnerability allowing operator.write message-tool paths to access Matrix profile persistence requiring admin-level authority. Attackers can exploit insufficient access controls to mutate persistent	6.5	More

42433	profile configuration through non-owner message-tool runs.		Details
CVE-2026-26206	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.0.0 to before version 4.14.4, Wazuh's server API brute-force protection for POST /security/user/authenticate can be bypassed by sending concurrent authentication requests. Although the configured threshold (max_login_attempts, default 50) is enforced correctly for sequential requests, a parallel burst allows significantly more failed login attempts to be processed before the IP block is applied. This enables an attacker to perform more password guesses than the configured policy intends (e.g., 100 attempts processed where 50 should be allowed). This issue has been patched in version 4.14.4.	6.5	More Details
CVE-2025-42611	RouterOS provides various services that rely on correct verification of client and server certificates to secure confidentiality and integrity of communications. This includes OpenVPN, CAPsMAN, Dot1x (802.1X), among others. The vulnerability lies in shared certificate validation logic which uses the system certificate store that is shared and equally trusted by all system services. This causes confusion of scope, allowing any certificate authority present in the system-wide trust store to be trusted in any context (with some exceptions), allowing partial or full authentication bypass in CAPsMAN, OpenVPN, Dot1X and potentially others.	6.5	More Details
CVE-2026-42223	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.8, the GetSettings API handler (api/settings/settings.go:24-65) serializes all settings structs to JSON and returns them to authenticated users. Many sensitive fields are tagged with protected:"true" - however, this tag is only enforced during writes (via ProtectedFill in SaveSettings) and is completely ignored during reads. This exposes 40+ protected fields including JwtSecret (enabling auth token forgery), NodeSecret (enabling cluster node impersonation), OIDC ClientSecret (enabling OAuth account takeover), and the IP whitelist configuration. This issue has been patched in version 2.3.8.	6.5	More Details
CVE-2026-42092	titra is an open source time tracking project. In version 0.99.52, the globalsettings Meteor publication returns all global settings without any admin or role check. Any authenticated user can subscribe via DDP and receive sensitive configuration fields such as google_secret, openai_apikey, and google_clientid. At time of publication no public patch is available.	6.5	More Details
CVE-2026-6914	Computing the MD5 checksum of a malformed BSON object under specific conditions may cause loss of availability in MongoDB server. This issue affects all MongoDB Server v8.2 versions, all MongoDB Server v8.1 versions, MongoDB Server v8.0 versions prior to 8.0.21, MongoDB Server v7.0 versions prior to 7.0.32	6.5	More Details
CVE-2026-4409	The Subscribe To Comments Reloaded plugin for WordPress is vulnerable to unauthorized modification of data due to a leaked secret key and usage of a weak hash generation algorithm in all versions up to, and including, 240119. This makes it possible for unauthenticated attackers to extract the global key from any public post page, forge authorization keys and manage comment subscription preferences for arbitrary users	6.5	More Details
CVE-2026-41950	Dify before version 1.14.0 contains an authorization bypass vulnerability that allows authenticated users to read the full contents of files uploaded by other users within the same tenant by supplying an arbitrary file UUID in the files array of a chat-messages request. Attackers can exploit insufficient permission verification in the chat-messages endpoints to access files without ownership validation, bypassing workspace separation and signed URL protections to retrieve sensitive file contents through workflow processing.	6.5	More Details
CVE-2026-5957	The EmailKit plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to and including 1.6.5. This is due to a flawed path traversal validation in the create_template() method of the CheckForm class, where realpath() is called on the allowed base directory (wp-content/uploads/emailkit/templates/) which may not exist, causing it to return false. In PHP 8.x, strpos($real_path, false) implicitly converts false to an empty string, and strpos() with an empty needle always returns 0, causing the check strpos(...) !== 0 to evaluate to false and bypassing the path validation entirely. This makes it possible for authenticated attackers, with Author-level access and above, to read arbitrary files from the server, including sensitive files such as wp-config.php, by supplying an absolute path to the emailkit-editor-template REST API parameter.	6.5	More Details
CVE-2026-38993	Cockpit 2.13.5 and earlier is vulnerable to directory traversal via the Buckets component. This vulnerability allows authenticated attackers to write files to arbitrary locations within the uploads directory or overwrite assets with malicious versions.	6.5	More Details
CVE-2026-4362	The ElementsKit Elementor Addons plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `Live_Action::reset()` function in all versions up to, and including, 3.8.2 The function is hooked to the WordPress `init` action and triggers when both `post` and `action=elementor` GET parameters are present, with no authentication or nonce verification. This makes it possible for unauthenticated attackers to overwrite the Elementor content (`_elementor_data`) of any `elementskit_widget` custom post type by visiting a specially crafted URL. The widget's custom designs, text, and configurations are permanently replaced with a blank template.	6.5	More Details
CVE-2026-7422	Insufficient packet validation in FreeRTOS-Plus-TCP before V4.2.6 and V4.4.1 allows an adjacent network actor to bypass all checksum and minimum-size validation by spoofing the Ethernet source MAC address to match one of the device's own registered endpoints, because the loopback detection mechanism skips all input validation for packets whose source MAC matches a local endpoint. To mitigate this issue, users should upgrade to the fixed version when available.	6.5	More Details
CVE-2026-28221	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.8.0 to before version 4.14.4, a stack-based buffer overflow exists in print_hex_string() in wazuh-remoted. The bug is triggered when formatting attacker-controlled bytes using sprintf(dst_buf + 2*i, "%.2x", src_buf[i]) on platforms where char is treated as signed and the compiled code sign-extends bytes before the variadic call. For input bytes such as 0xFF, the formatting can emit "ffffffff" (8 chars) instead of "ff" (2 chars), causing an out-of-bounds write past a fixed 2049-byte stack buffer. The vulnerable path is reachable remotely prior to any agent authentication/registration logic via TCP/1514 when an oversized length prefix causes the “unexpected message (hex)” diagnostic path to run. Additionally, the same unauthenticated oversized-message diagnostic path logs an attacker-controlled hex dump to /var/ossec/logs/ossec.log for each trigger, allowing remote log amplification that can degrade monitoring fidelity and consume disk/I/O. This log amplification is reachable even without triggering the sign-extension overflow (e.g., using bytes < 0x80). This issue has been patched in version 4.14.4.	6.5	More Details
CVE-2026-42091	goshs is a SimpleHTTPServer written in Go. Prior to version 2.0.2, the PUT upload handler (httpserver/updown.go) lacks the CSRF token validation that was added to the POST upload handler during the CVE-2026-40883 fix. Combined with the unconditional Access-Control-Allow-Origin: * on the OPTIONS preflight handler (httpserver/server.go), any website can write arbitrary files to a goshs instance through the victim's browser — bypassing network isolation (e.g. localhost, internal network). This issue has been patched in version 2.0.2.	6.5	More Details
CVE-2025-47403	Transient DOS when processing a malformed Fast Transition response frame with an invalid header structure during wireless roaming.	6.5	More Details

CVE-2026-20450	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01753620; Issue ID: MSV-6100.	6.5	More Details
CVE-2026-43568	OpenClaw versions 2026.4.5 before 2026.4.10 contain a privilege escalation vulnerability allowing write-scoped operators to modify persistent memory dreaming settings. Attackers with write-scoped gateway access can toggle admin-class configuration mutations through the /dreaming endpoint to escalate privileges.	6.5	More Details
CVE-2026-43567	OpenClaw before 2026.4.10 contains a path traversal vulnerability in the screen_record tool's outPath parameter that bypasses workspace-only filesystem guards. Attackers can exploit this by specifying an outPath outside the workspace boundary to write files to unintended locations on the system.	6.5	More Details
CVE-2025-70070	An issue in Assimp v.6.0.2 allows a remote attacker to cause a denial of service via the FBXMeshGeometry.cpp, MeshGeometry::MeshGeometry()	6.5	More Details
CVE-2025-70072	An issue in Assimp v.6.0.2 allows a remote attacker to cause a denial of service via the FBXConverter.cpp, FBXConverter::ConvertMeshMultiMaterial() components	6.5	More Details
CVE-2026-33523	HTTP response splitting vulnerability in multiple Apache HTTP Server modules with untrusted or compromised backend servers. This issue affects Apache HTTP Server: from through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	6.5	More Details
CVE-2026-37458	Missing input validation in the MP_REACH_NLRI component of FRRouting (FRR) stable/10.0 to stable/10.6 allows authenticated attackers to cause a Denial of Service (DoS) via supplying a crafted UPDATE message.	6.5	More Details
CVE-2025-47401	Transient DOS when processing target power rate tables during channel configuration.	6.5	More Details
CVE-2026-40685	In Exim before 4.99.2, when JSON lookup is enabled, an out-of-bounds heap write can occur when a JSON operator encounters malformed JSON in an untrusted header, because of an incorrect implementation of \ skipping.	6.5	More Details
CVE-2025-47404	Memory corruption when dynamically changing the size of a previously allocated buffer while its contents are being modified.	6.5	More Details
CVE-2018-25312	LifeSize ClearSea 3.1.4 contains directory traversal vulnerabilities that allow authenticated attackers to download and upload arbitrary files by manipulating path parameters in the smartgui interface. Attackers can exploit the upload endpoint with directory traversal sequences to write files to arbitrary locations on the system, enabling remote code execution.	6.5	More Details
CVE-2026-43528	OpenClaw before 2026.4.14 contains a redaction bypass vulnerability that allows authenticated gateway clients to receive unredacted secrets through sourceConfig and runtimeConfig alias fields. Attackers with config read access can exploit this to obtain provider API keys, gateway authentication material, and channel credentials that should have been redacted.	6.5	More Details
CVE-2018-25311	VideoFlow Digital Video Protection DVP 2.10 contains an authenticated directory traversal vulnerability that allows authenticated attackers to disclose arbitrary files by injecting path traversal sequences in the ID parameter. Attackers can submit requests to downloadsys.pl, download_xml.pl, download.pl, downloadmib.pl, or downloadFile.pl with directory traversal payloads to read sensitive system files like /etc/passwd.	6.5	More Details
CVE-2026-7425	Insufficient option length validation in the IPv6 Router Advertisement parser in FreeRTOS-Plus-TCP before V4.2.6 and V4.4.1 allows an adjacent network actor to cause a denial of service (device crash) by sending a crafted Router Advertisement with a truncated PREFIX_INFORMATION option that is smaller than the expected structure size. To mitigate this issue, users should upgrade to the fixed version when available.	6.5	More Details
CVE-2026-4665	The WP Carousel Free plugin for WordPress is vulnerable to Stored Cross-Site Scripting via crafted fancybox `data-caption` attributes in all versions up to, and including, 2.7.10. This is due to the `fancybox-config.js` script reading the carousel container's `id` attribute directly from the DOM to construct a jQuery selector without sanitization. When a Contributor crafts an HTML block with a malformed carousel container ID (containing characters invalid for jQuery selectors), the custom fancybox configuration throws a JavaScript error and fails to initialize. This causes the bundled fancybox library (v3.5.7) to fall back to its default caption handling, which renders the `data-caption` attribute content as raw HTML. Since WordPress allows `data-*` attributes through `wp_kses_post()`, 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 clicks an image in the crafted carousel lightbox.	6.4	More Details
CVE-2026-2311	IBM i 7.6, 7.5, 7.4, 7.3, and 7.2 s vulnerable to privilege escalation caused by an invalid IBM i Web Administration GUI authorization check. A malicious actor could cause user-controlled code to run with administrator privilege.	6.4	More Details
CVE-2026-7209	The Simple Link Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `qcopd-directory` shortcode in all versions up to, and including, 8.9.2. This is due to insufficient input sanitization and output escaping on user supplied attributes such as `title_font_size`. 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-2026-6378	The Maxi Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `/wp-json/maxi-blocks/v1.0/style-card` REST API endpoint in all versions up to, and including, 2.1.9 due to insufficient input sanitization and output escaping of the `sc_styles` parameter. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts that execute on every page where the plugin's style card styles are loaded, including across the entire WordPress admin panel.	6.4	More Details
CVE-2026-	The Royal Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Instagram Feed widget's 'instagram_follow_text' setting in all versions up to, and including, 1.7.1056 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	6.4	More Details

5159	that will execute whenever a user accesses an injected page. Note that exploitation requires that an administrator has previously configured the Instagram Feed widget with a valid Instagram access token on the site.		
CVE-2026-41174	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is a potential vulnerability in Traefik's Kubernetes CRD provider cross-namespace isolation enforcement. When providers.kubernetesCRD.allowCrossNamespace=false, Traefik correctly rejects direct cross-namespace middleware references from IngressRoute objects, but fails to apply the same restriction to middleware references nested inside a Chain middleware's spec.chain.middlewares[]. An actor with permission to create or update Traefik CRDs in their own namespace can exploit this to cause Traefik to resolve and apply middleware objects from another namespace, bypassing the documented isolation boundary. This issue has been patched in versions 2.11.43, 3.6.14, and 3.7.0-rc.2.	6.4	More Details
CVE-2026-2948	The Gutenverse – Ultimate WordPress FSE Blocks Addons & Ecosystem plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 3.5.3 via the import_images() function. This makes it possible for authenticated attackers, with contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	6.4	More Details
CVE-2026-6255	The Simple Owl Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'num' attribute of the 'owls_wrapper' shortcode in all versions up to, and including, 2.1.1 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 pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5505	The WP-Clippy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `clippy` shortcode in all versions up to, and including, 1.0.0. 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-2026-4730	The Charts Ninja: Create Beautiful Graphs & Charts and Easily Add Them to Your Website plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'chartid' shortcode attribute in all versions up to, and including, 2.1.0 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-2026-6916	The Jeg Kit for Elementor – Powerful Addons for Elementor, Widgets & Templates for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sg_content_number_prefix' parameter in all versions up to, and including, 3.1.0 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-2026-4658	The Essential Blocks – Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the className, classHook, and blockId attributes in the Add to Cart block (essential-blocks/add-to-cart) in all versions up to, and including, 6.0.4. This is due to insufficient output escaping in the render_callback() function where these attributes are placed into class and data-id HTML attributes using raw sprintf() and implode() without esc_attr() escaping. While the outer wrapper div uses get_block_wrapper_attributes() which properly escapes, the inner divs do not. 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-2026-3346	IBM Langflow Desktop 1.6.0 through 1.8.4 Lanflow is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2026-2868	The Gutenverse – Ultimate WordPress FSE Blocks Addons & Ecosystem plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'separatorIconSVG' parameter in versions up to, and including, 3.5.3 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-2026-0703	The NextMove Lite – Thank You Page for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'xlwcty_current_date' shortcode in all versions up to, and including, 2.23.0 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-2026-6127	The Elementor Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _elementor_data meta field in versions up to, and including, 4.0.4. This is due to insufficient input sanitization when processing form-encoded REST API requests. The plugin registers the _elementor_data meta field with show_in_rest but omits a sanitize_callback, relying instead on a rest_pre_insert_post filter (sanitize_post_data function) that only sanitizes JSON-encoded request bodies. When a contributor sends a form-encoded PATCH request to the WordPress REST API, the json_decode() call on the raw body returns null, causing all sanitization to be skipped. The unsanitized data is then stored via update_post_meta() and later output without escaping through multiple widget sinks including the HTML widget's print_unescaped_setting() function. 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-2026-7720	A weakness has been identified in Totolink WA300 5.2cu.7112_B20190227. The impacted element is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. This manipulation of the argument langType causes command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-7725	A vulnerability was found in PrefectHQ prefect up to 3.6.25.dev6. Affected by this issue is some unknown functionality of the file src/prefect/runner/storage.py of the component GitRepository Pull Handler. The manipulation of the argument commit_sha/directories results in argument injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. Upgrading to version 3.6.25.dev7 can resolve this issue. The patch is identified as 6a9d9918716ce4ee0297b69f3046f7067ef1faae. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	6.3	More Details
CVE-2026-7729	A security flaw has been discovered in pixelsock directus-mcp 1.0.0. This issue affects the function validateUrl of the file index.ts of the component MCP Interface. Performing a manipulation of the argument fileUrl results in server-side request forgery. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	6.3	More Details

CVE-2026-7730	A weakness has been identified in privsim mcp-test-runner 0.2.0. Impacted is the function child_process.spawn of the file src/index.ts of the component MCP Interface. Executing a manipulation of the argument command 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. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-7604	A vulnerability was identified in JeecgBoot up to 3.9.1. This affects the function OpenApiController.add/OpenApiController.call of the file OpenApiController.java of the component OpenApi Service. Such manipulation of the argument originUrl database leads to server-side request forgery. It is possible to launch the attack remotely. The exploit is publicly available and might be used. It is suggested to upgrade the affected component. The vendor confirmed the issue and will provide a fix in the upcoming release.	6.3	More Details
CVE-2026-7603	A vulnerability was determined in JeecgBoot up to 3.9.1. Affected by this issue is the function checkPathTraversalBatch of the file FileDownloadUtils.jav of the component LoadFile Endpoint. This manipulation of the argument files causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The affected component should be upgraded. The vendor confirmed the issue and will provide a fix in the upcoming release.	6.3	More Details
CVE-2026-7731	A security vulnerability has been detected in code-projects BloodBank Managing System 1.0. The affected element is an unknown function of the file get_state.php. The manipulation of the argument G_STATE_ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-7732	A vulnerability was detected in code-projects BloodBank Managing System 1.0. The impacted element is an unknown function of the file request_blood.php. The manipulation results in unrestricted upload. The attack can be executed remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-7602	A vulnerability was found in JeecgBoot up to 3.9.1. Affected by this vulnerability is an unknown functionality of the file /sys/fillRule/edit of the component FillRuleUtil Component. The manipulation of the argument ruleClass results in improper authorization. The attack may be performed from remote. The exploit has been made public and could be used. You should upgrade the affected component. The vendor confirmed the issue and will provide a fix in the upcoming release.	6.3	More Details
CVE-2026-7600	A flaw has been found in ArtMin96 yii2-mcp-server 1.0.2. This impacts the function yii_command_help/yii_execute_command of the file src/index.ts of the component MCP Interface. Executing a manipulation can lead to os command injection. 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.	6.3	More Details
CVE-2026-7599	A vulnerability was detected in Dayoooun hwpx-mcp 0.2.0. This affects the function save_document/export_to_text/export_to_html of the file mcp-server/src/index.ts of the component MCP Interface. Performing a manipulation of the argument output_path results in path traversal. 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.	6.3	More Details
CVE-2026-7687	A vulnerability was determined in langflow-ai langflow up to 1.8.4. Affected by this issue is the function CodeParser.parse_callable_details of the file src/lfx/src/lfx/custom/code_parser/code_parser.py of the component Full Builtins Module Handler. Executing a manipulation can lead to command injection. The attack can be executed 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-2026-7597	A vulnerability was found in mem0ai mem0 up to 1.0.11. This affects the function pickle.load/pickle.dump of the file mem0/vector_stores/faiss.py. Performing a manipulation results in deserialization. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The patch is named 62dca096f9236010ca15fea9ba369ba740b86b7a. Applying a patch is the recommended action to fix this issue.	6.3	More Details
CVE-2026-7595	A flaw has been found in nextlevelbuilder ui-ux-pro-max-skill up to 2.5.0. Affected by this vulnerability is the function _format_plugins of the file .claude/skills/ui-styling/scripts/tailwind_config_gen.py of the component Tailwind Config Generator. This manipulation causes code injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	6.3	More Details
CVE-2026-7738	A security flaw has been discovered in puchunjie doc-tools-mcp 1.0.18. This affects the function create_document/open_document of the file src/mcp-server.ts of the component MCP Interface. The manipulation of the argument filePath results in path traversal. The attack can 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.	6.3	More Details
CVE-2026-7741	A vulnerability was detected in CodeAstro Online Classroom 1.0. Impacted is an unknown function of the file /OnlineClassroom/studentlogin. Performing a manipulation of the argument sid results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	6.3	More Details
CVE-2026-7742	A flaw has been found in CodeAstro Online Classroom 1.0. The affected element is an unknown function of the file /OnlineClassroom/facultylogin. Executing a manipulation of the argument fid can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-7743	A vulnerability has been found in CodeAstro Online Classroom 1.0. The impacted element is an unknown function of the file /OnlineClassroom/studentdetails. The manipulation of the argument deleteid 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.	6.3	More Details
CVE-2026-7744	A vulnerability was found in CodeAstro Online Classroom 1.0. This affects an unknown function of the file /OnlineClassroom/addnewstudent. The manipulation of the argument fname results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-7745	A vulnerability was determined in CodeAstro Online Classroom 1.0. This impacts an unknown function of the file /OnlineClassroom/facultydetails. This manipulation of the argument deleteid causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-7746	A vulnerability was identified in SourceCodester Web-based Pharmacy Product Management System 1.0. Affected is an unknown function of the file /product_expiry/edit-admin.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-7591	A security flaw has been discovered in TimBroddin astro-mcp-server up to 1.1.1. The impacted element is an unknown function of the file src/index.ts of the component MCP Tool Query Construction. Performing a manipulation of the argument request.params.arguments results in sql injection. The attack may be initiated remotely. The exploit has been released to the public	6.3	More Details

	and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2026-7469	A vulnerability was detected in Tenda 4G300 US_4G300V1.0Mt_V1.01.42_CN_TDC01. This impacts the function sub_425A28 of the file /goform/DelFil. The manipulation of the argument delflag results in command injection. The attack may be launched remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-7447	A flaw has been found in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file /admin/update_customer.php. This manipulation of the argument type/length/business parameter validity 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-2026-7728	A vulnerability was identified in ryanjoachim mcp-rtfm 0.1.0. This vulnerability affects the function get_doc_content/read_doc/update_doc of the component MCP Interface. Such manipulation of the argument docFile leads to path traversal. The attack can be launched remotely. The exploit is publicly available and might be used. The name of the patch is e6f0686fc36012f78236e7fed172c81444904b0b. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-7605	A security flaw has been discovered in JeecgBoot up to 3.9.1. This vulnerability affects the function CommonController.uploadImgByHttp/HttpFileToMultipartFileUtil.httpFileToMultipartFile/HttpFileToMultipartFileUtil.downloadImageData of the file CommonController.java of the component uploadImgByHttpEndpoint. Performing a manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. Upgrading the affected component is recommended. The vendor confirmed the issue and will provide a fix in the upcoming release.	6.3	More Details
CVE-2026-7844	A vulnerability was detected in chatchat-space Langchain-Chatchat up to 0.3.1.3. This vulnerability affects the function files/list_files/retrieve_file/retrieve_file_content/delete_file of the file libs/chatchat-server/chatchat/server/api_server/openai_routes.py of the component Compatible File Service. The manipulation results in missing authentication. The attacker must have access to the local network to execute the attack. 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.	6.3	More Details
CVE-2026-7705	A flaw has been found in JD Cloud JDCOS 4.5.1.r4518. This vulnerability affects the function set_iptv_info of the file /jdcap of the component Service Interface. Executing a manipulation of the argument vid can lead to command injection. It is possible to launch the attack 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-2026-7683	A weakness has been identified in Edimax BR-6428nC up to 1.16. This affects an unknown function of the file /goform/setWAN of the component Web Interface. This manipulation of the argument pppUserName/pptpUserName causes command injection. The attack can be initiated 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.	6.3	More Details
CVE-2026-7682	A security flaw has been discovered in Edimax BR-6208AC 1.02. The impacted element is the function setWAN of the file /goform/setWAN of the component L2TP Mode. The manipulation of the argument L2TPUserName results in command injection. It is possible to launch the attack 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.	6.3	More Details
CVE-2026-7691	A security vulnerability has been detected in Wavlink WL-WN570HA1 R70HA1 V1410_221110. Impacted is the function set_sys_cmd of the file /cgi-bin/adm.cgi. Such manipulation of the argument command leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-7692	A vulnerability was detected in Wavlink WL-WN570HA1 R70HA1 V1410_221110. The affected element is the function ping_ddns of the file /cgi-bin/adm.cgi. Performing a manipulation of the argument DDNS results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-7678	A vulnerability was identified in YunaiV yudao-cloud up to 2026.01. This affects the function getDataBySQL of the file yudao-module-report-biz/src/main/java/io/github/ruoyi/report/service/impl/GoViewDataServiceImpl.java. Such manipulation leads to sql injection. It is possible to launch the attack 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.	6.3	More Details
CVE-2026-7696	A vulnerability was found in Acrel Electrical EEMS Enterprise Power Operation and Maintenance Cloud Platform 1.3.0. This impacts an unknown function of the file /SubstationWEBV2/main/uploadH5Files. The manipulation of the argument File results in unrestricted upload. 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.	6.3	More Details
CVE-2026-7699	A security flaw has been discovered in Dromara MaxKey up to 3.5.13. Affected by this issue is the function StrUtils.checkSqlInjection of the file StrUtils.java. Performing a manipulation of the argument filtersfields 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. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-7672	A security vulnerability has been detected in youlaitech youlai-boot up to 2.21.1. This affects the function getUserList of the file src/main/java/com/youlai/boot/system/controller/UserController.java of the component Users Endpoint. Such manipulation of the argument order leads to sql injection. The attack may be launched 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.	6.3	More Details
CVE-2026-7700	A weakness has been identified in langflow-ai langflow up to 1.8.4. This affects the function eval of the file src/lfx/src/lfx/components/llm_operations/lambda_filter.p of the component LambdaFilterComponent. Executing a manipulation can lead to code injection. The attack may be performed from remote. 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.	6.3	More Details
CVE-2026-7653	A security flaw has been discovered in r-huijts mcp-server-rijksmuseum up to 1.0.4. Affected is the function open_image_in_browser of the file src/index.ts of the component MCP Interface. Performing a manipulation of the argument imageUrl results in os command injection. The attack is possible to be carried out 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.	6.3	More Details
	A vulnerability was detected in pskill9 website-downloader up to 0.1.0. This affects the function download_website of the file		

CVE-2026-7642	src/index.ts of the component MCP Interface. Performing a manipulation of the argument outputPath results in os command injection. The attack may 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.	6.3	More Details
CVE-2026-7721	A security vulnerability has been detected in Totolink WA300 5.2cu.7112_B20190227. This affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument hostTime leads to command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-7629	A flaw has been found in kleneway awesome-cursor-mpc-server up to 2.0.1. Impacted is the function runCodeReviewTool of the file src/tools/codeReview.ts of the component Ccode-Review Tool. Executing a manipulation can lead to command injection. The attack may be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	6.3	More Details
CVE-2026-7709	A vulnerability was identified in janeczku Calibre-Web up to 0.6.26. The impacted element is the function generate_auth_token of the file cps/kobo_auth.py of the component Endpoint. Such manipulation of the argument user_id leads to improper authorization. The attack may be launched 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.	6.3	More Details
CVE-2026-7628	A vulnerability was detected in crazyrabbitLTC mcp-code-review-server up to 0.1.0. This issue affects the function executeRepomix of the file src/repomix.ts of the component RepoMix Command Handler. Performing a manipulation results in command injection. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	6.3	More Details
CVE-2026-7627	A security vulnerability has been detected in 8nite metatrader-4-mcp 1.0.0. This vulnerability affects the function CallToolRequestSchema of the file src/index.ts of the component sync_ea_from_file. Such manipulation of the argument ea_name leads to path traversal. The attack can be launched 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.	6.3	More Details
CVE-2026-7712	A security vulnerability has been detected in MindsDB up to 26.01. Affected is the function pickle.loads of the component Pickle Handler. The manipulation leads to deserialization. The attack is possible to be carried out 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.	6.3	More Details
CVE-2026-7713	A vulnerability was detected in crocodilestick Calibre-Web-Automated up to 4.0.6. Affected by this vulnerability is the function generate_auth_token of the file cps/kobo_auth.py of the component Kobo auth-token Route. The manipulation results in improper authorization. The attack may be performed from remote. The exploit is now public and may be used. Upgrading to version 4.0.7 addresses this issue. The patch is identified as 9f50bb2c16160564c9f8777dc2ceed3eb95e4807. The affected component should be upgraded.	6.3	More Details
CVE-2026-7609	A flaw has been found in TRENDnet TEW-821DAP up to 1.12B01. The impacted element is the function tools_diagnostic of the file /tmp/diagnostic of the component Firmware Udpate. This manipulation causes os command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-7715	A vulnerability has been found in ravenwits mcp-server-arangodb up to 0.4.7. This affects the function arango_backup of the file src/tools.ts of the component MCP Interface. Such manipulation of the argument outputDir leads to path traversal. 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.	6.3	More Details
CVE-2026-7716	A vulnerability was found in code-projects Gym Management System In PHP and Windows NT 1.0. This vulnerability affects unknown code of the file /index.php. Performing a manipulation of the argument day results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-7718	A vulnerability was identified in Totolink WA300 5.2cu.7112_B20190227. Impacted is the function setWebWlanIdx of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument webWlanIdx leads to command injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-7445	A security vulnerability has been detected in ZachHandley ZMCPTools up to 0.2.2. Affected by this issue is some unknown functionality of the file src/managers/ResourceManager.ts of the component MCP Log Resource Handler. The manipulation of the argument dirname leads to path traversal. Remote exploitation of the attack is possible. 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.	6.3	More Details
CVE-2026-7690	A weakness has been identified in Wavlink WL-WN570HA1 R70HA1 V1410_221110. This issue affects the function set_sys_adm of the file /cgi-bin/adm.cgi. This manipulation of the argument Username causes command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-6915	An authorization flaw in the user management command could allow an authenticated user to make limited changes to authentication-related data associated with another user account. This could affect how authentication is performed for the impacted account.	6.3	More Details
CVE-2026-7783	A flaw has been found in CodeCanyon Perfex CRM up to 3.4.1. This vulnerability affects the function AbstractKanban::applySortQuery of the file application/services/AbstractKanban.php of the component Admin Kanban Endpoint. This manipulation of the argument this causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-7508	A vulnerability was found in Bootstrap CMS 0.9.0-alpha. Affected is an unknown function of the file resources/views/pages/show.blade.php of the component Page Creation Handler. Performing a manipulation of the argument body results in code injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The code repository of the project has not been active for many years. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-	A vulnerability was determined in OWAP DefectDojo up to 2.55.4. Affected by this vulnerability is an unknown functionality of the component Benchmark/Engagement/Product/Survey. Executing a manipulation can lead to authorization bypass. The attack can be	6.3	More

7510	executed remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.56.0 addresses this issue. This patch is called eb6120a379185d37eb1af17b69bb5614a830ab1f. Upgrading the affected component is recommended.		Details
CVE-2026-7392	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. This impacts the function delete_supplier of the file /ajax.php?action=delete_supplier. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-7391	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. This affects the function save_supplier of the file /ajax.php?action=save_supplier. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2026-7782	A vulnerability was detected in CodeCanyon Perfex CRM up to 3.4.1. This affects the function Clients::project of the file application/controllers/Clients.php of the component Tenant Handler. The manipulation of the argument ID results in authorization bypass. The attack may be performed from remote. The exploit is now public and may be used.	6.3	More Details
CVE-2026-27105	Dell/Alienware Purchased Apps, versions prior to 1.1.31.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write	6.3	More Details
CVE-2026-7822	A vulnerability was identified in itsourcecode Courier Management System 1.0. This impacts an unknown function of the file /print_pdets.php. The manipulation of the argument ids leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-7410	A vulnerability has been found in SourceCodester Pizzafy Ecommerce System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=add_to_cart. The manipulation of the argument pid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2018-25305	librsvg2-bin 2.40.13 contains a buffer overflow vulnerability that allows local attackers to cause a denial of service by processing malformed SVG files. Attackers can supply crafted SVG input to the rsvg conversion tool to trigger a segmentation fault in the cairo image compositor.	6.2	More Details
CVE-2018-25306	PDFunite 0.41.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by processing malformed PDF files during merge operations. Attackers can trigger a segmentation fault in the XRef::getEntry function within libpoppler by providing a specially crafted PDF file to the pdfunite utility.	6.2	More Details
CVE-2018-25313	SysGauge 4.5.18 contains a buffer overflow vulnerability in the proxy configuration handler that allows local attackers to cause a denial of service by supplying an oversized string. Attackers can inject a large payload through the Proxy Server Host Name field in the Options menu to crash the application.	6.2	More Details
CVE-2025-36335	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.3.0, 5.3.1 stores user credentials in plain text which can be read by a local user.	6.2	More Details
CVE-2026-2902	The WP Meteor Website Speed Optimization Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'frontend_rewrite' function's 'WPMETEOR[N]WPMETEOR' placeholder content in all versions up to, and including, 3.4.16 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2026-6702	The Publish 2 Ping.fm plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the '/wp-admin/options-general.php?page=admin.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-54349	AmazCart CMS 3.4 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting payloads through the search functionality. Attackers can enter script tags in the search box to execute arbitrary JavaScript that fires when search history is viewed or results are displayed.	6.1	More Details
CVE-2025-56534	A cross-site scripting (XSS) vulnerability in the custom authenticator driver of opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2025-56535	A cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the zone attribute parameter.	6.1	More Details
CVE-2024-13362	Multiple plugins and/or themes for WordPress are vulnerable to Reflected Cross-Site Scripting via the url parameter in various versions due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-38669	wCMS v.1.4 is vulnerable to Cross Site Scripting (XSS) when creating a new blog.	6.1	More Details
CVE-2025-56537	A stored cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 and fixed in v.7.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the virtual network template parameter.	6.1	More Details
CVE-2026-7163	A vulnerability in the assisted-service REST API, an optional Assisted Installer (assisted-service) component in the Multicluster Engine (MCE), allows an authenticated user with minimal namespace-scoped privileges to obtain administrative credentials for arbitrary clusters provisioned through the hub. The credentials download endpoint (GET /v2/clusters/{cluster_id}/credentials, which returns the kubeadmin password) and the kubeconfig download endpoint are operational in AUTH_TYPE=local mode, the only authentication mode available in on-premises ACM/MCE hub deployments. The local authenticator unconditionally grants full administrative access to any request bearing a valid JWT, with no per-endpoint restrictions. A valid local JWT is embedded as a plaintext query parameter in InfraEnvStatus.ISODownloadURL and is readable by any user who has get rights on an InfraEnv object in their own namespace. The affected components ship as part of Multicluster Engine (MCE). The Red Hat Advanced Cluster Management (ACM) deployments that include MCE are equally affected. This issue does not affect the hosted SaaS offering (console.redhat.com), which uses a different	6.1	More Details

	authentication mode. Successful exploitation gives the attacker the kubeadmin password and kubeconfig for any OpenShift cluster provisioned through the affected hub, granting unrestricted root-level administrative access to those spoke clusters.		
CVE-2026-38939	Cross Site Scripting vulnerability in andrewtch88 mvc-ecommerce v.1.0 allows a remote attacker to execute arbitrary code and obtain sensitive information via the product_catalogue.php component	6.1	More Details
CVE-2026-38940	Cross Site Scripting vulnerability in RafyMrX TOKO-ONLINE-ROTI v.1.0 allows a remote attacker to execute arbitrary code via the detail_produk.php component	6.1	More Details
CVE-2026-6704	The Blog Settings plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-47406	Information Disclosure while processing IOCTL handler callbacks without verifying buffer size.	6.1	More Details
CVE-2026-42144	CImg Library is a C++ library for image processing. Prior to commit 4ca26bc, there is an integer overflow vulnerability in the W*H*D size computation inside _load_pnm() that can bypass the memory allocation guard. A crafted PNM/PGM/PPM file with large dimension values causes the overflow to wrap around, allocating an undersized buffer and potentially triggering a heap buffer overflow. Any application using CImg to load untrusted image files is affected. This issue has been patched via commit 4ca26bc.	6.1	More Details
CVE-2026-36761	A stored cross-site scripting (XSS) vulnerability in the /msg/msgInner/save endpoint of JeeSite v5.15.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted input into the msgContent parameter.	6.1	More Details
CVE-2026-34000	A flaw was found in the X.Org X server. This out-of-bounds read vulnerability in the XKB geometry processing, specifically within the `CheckSetGeom()` and `XkbAddGeomKeyAlias` functions, allows an attacker to read uninitialized or out-of-bounds memory. An attacker with a connection to the X11 server, either locally or remotely, can exploit this without user interaction. This could lead to the disclosure of memory contents or cause a denial of service by crashing the server.	6.1	More Details
CVE-2025-69606	Cross-Site Scripting (XSS) vulnerability was discovered in the GSVoIP web panel version 2.0.90. The `msg` parameter in the `/painel/gateways.php/error` endpoint does not properly sanitize user-supplied input, allowing attackers to inject arbitrary JavaScript into the HTML response. A remote attacker can exploit this vulnerability by sending a crafted URL to a victim, leading to unauthorized script execution, session hijacking, phishing, or other client-side attacks.	6.1	More Details
CVE-2026-36763	A stored cross-site scripting (XSS) vulnerability in the /api/blade-desk/notice/submit endpoint of SpringBlade v4.8.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted input into the content parameter.	6.1	More Details
CVE-2025-56536	A stored cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the user information parameter.	6.1	More Details
CVE-2026-34002	A flaw was found in the X.Org X server. This vulnerability, an out-of-bounds read, affects the XKB (X Keyboard Extension) modifier map handling. An attacker with access to the X11 server can exploit this by sending a malformed request, which causes the server to read beyond its intended memory boundaries. This can lead to the exposure of sensitive information or cause the server to crash, resulting in a denial of service.	6.1	More Details
CVE-2026-6696	The Zingaya Click-to-Call plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'email', 'first_name', 'last_name', and 'phone' parameters on the plugin's sign-up admin page in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-10503	The authentication endpoint accepts user-supplied input without enforcing expected validation constraints, leading to a lack of proper output encoding. This allows for the injection of malicious JavaScript payloads, enabling reflected cross-site scripting. An attacker can leverage this vulnerability to redirect the user's browser to a malicious website, modify the user interface of the web page, retrieve information from the browser, or cause other harmful actions. However, due to the protection of session-related cookies with the httpOnly flag, session hijacking is not possible.	6.1	More Details
CVE-2026-40684	In Exim before 4.99.2, on systems using musl libc (not glibc), an attacker can crash the connection instance when malformed DNS data is present in PTR records. This is caused by a dn_expand oddity in octal printing.	5.9	More Details
CVE-2026-5080	Dancer::Session::Abstract versions through 1.3522 for Perl generates session ids insecurely. The session id is generated from summing the character codepoints of the absolute pathname with the process id, the epoch time and calls to the built-in rand() function to return a number between 0 and 999-billion, and concatenating that result three times. The path name might be known or guessed by an attacker, especially for applications known to be written using Dancer with standard installation locations. The epoch time can be guessed by an attacker, and may be leaked in the HTTP header. The process id comes from a small set of numbers, and workers may have sequential process ids. The built-in rand() function is seeded with 32-bits and is considered unsuitable for security applications. Predictable session ids could allow an attacker to gain access to systems.	5.9	More Details
CVE-2026-41016	Apache Airflow's SMTP provider `SmtpHook` called Python's `smtplib.SMTP.starttls()` without an SSL context, so no certificate validation was performed on the TLS upgrade. A man-in-the-middle between the Airflow worker and the SMTP server could present a self-signed certificate, complete the STARTTLS upgrade, and capture the SMTP credentials sent during the subsequent `login()` call. Users are advised to upgrade to the `apache-airflow-providers-smtp` version that contains the fix.	5.9	More Details
CVE-2026-28510	eLabFTW is an open source electronic lab notebook. In elabftw versions through 5.4.1, the login flow did not reliably preserve the multi-factor authentication state across authentication steps. Under certain conditions, an attacker with valid primary credentials could complete authentication with an attacker-controlled TOTP secret and bypass the additional factor. This could result in unauthorized account access. This issue is fixed in version 5.4.2.	5.9	More Details

CVE-2026-34956	A flaw was found in Open vSwitch. When Open vSwitch is configured with a conntrack flow using FTP helpers over the userspace datapath, a remote attacker can send a specially crafted FTP stream with an EPASV command exceeding 255 characters. This heap access error can lead to a crash, resulting in a Denial of Service (DoS) for the affected system.	5.9	More Details
CVE-2025-70071	An issue in Assimp v.6.0.2 allows a remote attacker to cause a denial of service via the FBXParser.cpp, ParseVectorDataArray()	5.9	More Details
CVE-2026-32148	Insufficient Verification of Data Authenticity vulnerability in hexpm hex (Hex.RemoteConverger module) allows dependency integrity bypass via unverified lockfile checksums. Hex stores checksums for dependencies in the mix.lock file to ensure reproducible and integrity-checked builds. However, Hex.RemoteConverger.verify_resolved/2 never executes checksum verification because the lock data returned by Hex.Utils.lock/1 uses string-based dependency names, while the verification logic compares against atom-based names. This type mismatch causes the verification code path to be silently skipped. Checksums are still validated when packages are initially downloaded from the registry, but mismatches between the lockfile and resolved dependencies are not detected. An attacker who can influence cached packages (e.g., via local cache poisoning or a compromised registry) can provide modified dependency contents that will be accepted without detection. The mix.lock file is silently rewritten with the checksum values from the registry, erasing evidence of tampering. This issue affects hex: from 0.16.0 before 2.4.2.	5.9	More Details
CVE-2026-42643	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StellarWP Image Widget image-widget allows Stored XSS.This issue affects Image Widget: from n/a through <= 4.4.11.	5.9	More Details
CVE-2026-6817	The Quiz Maker by AYS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rate_reason' parameter in all versions up to, and including, 6.7.1.29 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.8	More Details
CVE-2026-31205	Cross Site Scripting vulnerability in Pluck CMS before v.4.7.21dev allows a remote attacker to escalate privileges via the editpage.php and the sanitizePageContent function	5.7	More Details
CVE-2026-7669	A vulnerability was detected in sgl-project SGLang up to 0.5.9. Impacted is the function get_tokenizer of the file python/sglang/srt/utils/hf_transformers_utils.py of the component HuggingFace Transformer Handler. The manipulation of the argument trust_remote_code with the input False as part of Boolean results in code injection. The attack can be executed remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. In get_tokenizer(), when the caller passes trust_remote_code=False and HuggingFace transformers v5 returns a TokenizersBackend instance (the generic fallback for tokenizer classes not in the registry), SGLang silently re-invokes AutoTokenizer.from_pretrained with trust_remote_code=True, overriding the caller's explicit security setting. A model repository containing a malicious tokenizer.py referenced via auto_map in tokenizer_config.json will execute arbitrary Python in the SGLang process during this second call. No log line or warning is emitted. The override affects all current SGLang versions because transformers==5.3.0 is pinned in pyproject.toml. Both tokenizer_mode="auto" and tokenizer_mode="slow" are affected. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2026-7554	A vulnerability was determined in D-Link M60 up to 1.20B02. Affected by this issue is some unknown functionality of the file /usr/bin/httpd. This manipulation causes weak password recovery. The attack can be initiated remotely. A high degree of complexity is needed for the attack. The exploitation is known to be difficult. The exploit has been publicly disclosed and may be utilized.	5.6	More Details
CVE-2026-21023	Insufficient verification of data authenticity in PackageManagerService prior to SMR Mar-2026 Release 1 allows local attackers to modify the installation restriction of specific application.	5.5	More Details
CVE-2026-6519	MBIM protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5657	iLBC codec crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5655	SDP protocol dissector crash in Wireshark 4.6.0 to 4.6.4 allows denial of service	5.5	More Details
CVE-2026-6524	MySQL protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-7608	A vulnerability was detected in TRENDnet TEW-821DAP up to 1.12B01. The affected element is the function tools_diagnostic. The manipulation results in os command injection. The exploit is now public and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2026-42481	Open CASCADE Technology (OCCT) V8_0_0_rc5 contains multiple vulnerabilities in its IGES and STEP file parsers that can be triggered by crafted IGES or STEP files. These issues include an out-of-bounds read in Geom2d_BSplineCurve::EvalD0 during IGES B-spline curve evaluation, an out-of-bounds read in MakeBSplineCurveCommon during STEP B-spline curve construction, and infinite recursion in StepShape_OrientedEdge::EdgeStart when processing a self-referential OrientedEdge entity. Successful exploitation may result in denial of service or unintended memory disclosure.	5.5	More Details
CVE-2026-7375	UDS protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-7376	Crash in sharkd 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details

CVE-2026-7378	Crash in sharkd 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6868	HTTP protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6523	GNW protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6520	OpenFlow v6 protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5406	FC-SWILS protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6521	OpenFlow v5 protocol dissector infinite loops in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6870	GSM RP protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6869	WebSocket protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6536	DLMS/COSEM protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4	5.5	More Details
CVE-2026-6867	SMB2 protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6525	IEEE 802.11 protocol dissector crash in Wireshark 4.6.0 to 4.6.4	5.5	More Details
CVE-2026-5247	The Schedule Post Changes With PublishPress Future plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wrapper' attribute of the [futureaction] shortcode in all versions up to, and including, 4.10.0. This is due to insufficient input sanitization on the wrapper attribute. The plugin uses esc_html() to escape the value, but esc_html() only encodes HTML entities and does not prevent attribute injection when the value is used as an HTML tag name in a sprintf() call. An attacker can inject event handler attributes via spaces in the wrapper value. 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. Since it is also possible for administrators to make this functionality available to lower-privileged users, this introduces the possibility of abuse by contributors.	5.5	More Details
CVE-2026-6538	BEEP protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5654	AMR-NB codec crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-7379	Memory leak in sharkd 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6531	SANE protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-42480	A stack-based out-of-bounds read vulnerability in VrmlData_Scene::ReadLine in the VRML parser in Open CASCADE Technology (OCCT) V8_0_0_rc5 allows attackers to cause a denial of service via a crafted VRML file. The issue occurs because the quoted-string escape handler uses ptr[++anOffset] without proper bounds checking, which can read past the end of a fixed-size stack buffer.	5.5	More Details
CVE-2026-6527	ASN.1 PER protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5407	SMB2 protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6528	TLS protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 allows denial of service	5.5	More Details

CVE-2026-6533	Dissection engine LZ77 decompression crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5408	BT-DHT protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-42146	CImg Library is a C++ library for image processing. Prior to commit c3aacf5, the nb_colors field read from the BMP file header is used directly to compute an allocation size without validating it against the remaining file size. A crafted BMP file with a large nb_colors value triggers an out-of-memory condition, crashing any application that uses CImg to load untrusted BMP files. This issue has been patched via commit c3aacf5.	5.5	More Details
CVE-2026-42479	An out-of-bounds read vulnerability in VrmlData_IndexedLineSet::TShape in the VRML parser in Open CASCADE Technology (OCCT) V8_0_0_rc5 allows attackers to cause a denial of service via a crafted VRML file. The issue occurs because coordIndex values from parsed input are used as direct array indices without validation against the size of the coordinate array during geometry processing.	5.5	More Details
CVE-2026-33450	CVE-2026-33450 is an out of bounds read vulnerability in the Secure Access MacOS client prior to 14.50. Attackers with control of a modified server can send a malformed packet to the client causing a denial of service.	5.5	More Details
CVE-2026-5401	AFP Spotlight protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6534	USB HID protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6522	RPKI-Router protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6526	RTSP protocol dissector crash in Wireshark 4.6.0 to 4.6.4	5.5	More Details
CVE-2026-6529	iLBC audio codec crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5409	Monero protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6530	DCP-ETSI protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-5653	DCP-ETSI protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-40951	CVE-2026-40951 is a memory corruption vulnerability on Secure Access Windows clients prior to 14.50. Attackers with local control of the Windows client can send malformed data to an API and trigger a denial of service.	5.5	More Details
CVE-2026-6535	Dissection engine zlib decompression crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6532	Kismet protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-33452	CVE-2026-33452 is a buffer overflow vulnerability in the Secure Access Windows client prior to 14.50. Attackers with local control of the Windows client can use it to ‘blue screen’ the system.	5.5	More Details
CVE-2026-25266	Memory corruption while processing IOCTL command when device is in power-save state.	5.5	More Details
CVE-2026-5299	ICMPv6 PvD protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-6537	ZigBee protocol dissector crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	5.5	More Details
CVE-2026-40201	@diplodoc/search-extension 1.0.0 through 3.x before 3.0.3 allows stored XSS via the title in a .md file.	5.4	More Details
CVE-	A vulnerability was found in code-projects Online Hospital Management System 1.0. The impacted element is an unknown function of		More

2026-7631	the component Registration Handler. The manipulation of the argument Username results in improper authorization. The attack can be executed remotely. The exploit has been made public and could be used.	5.4	Details
CVE-2026-36756	A Server-Side Request Forgery (SSRF) in the /plugins/-/install-from-uri endpoint of halo v2.22.14 allows authenticated attackers to scan internal resources via a crafted GET request.	5.4	More Details
CVE-2026-40229	Helpy contains a stored cross-site scripting vulnerability in the post author display logic. Any registered user can persist arbitrary HTML in their account name field and cause it to be rendered unescaped in public forum threads where they participate, in the admin ticket view, and in HTML notification emails sent to other users.This issue affects helpy: 2.8.0.	5.4	More Details
CVE-2026-36766	Multiple authenticated cross-site scripting (XSS) vulnerabilities in the XssHttpServletRequestWrapper class of shopizer v3.2.5 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the getInputStream() or getReader() functions.	5.4	More Details
CVE-2026-4790	The Premium Addons for Elementor – Powerful Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_svg' parameter in versions up to, and including, 4.11.70 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-2026-40230	Helpy contains a stored cross-site scripting vulnerability in the knowledge base Doc rendering logic. An authenticated attacker with admin or agent editor privileges can persist arbitrary HTML or JavaScript in the body field of a knowledge base Doc.This issue affects helpy: 2.8.0.	5.4	More Details
CVE-2026-1493	LEX Baza Dokumentów is vulnerable to DOM-based XSS in "em" cookie parameter. The application unsafely processes the parameter on the client side, allowing an attacker to execute arbitrary JavaScript in the context of the victim's browser. An attacker with ability to set a cookie can perform a more severe attack, so we evaluate the impact and risk of exploitation as minimal. However, the vendor considered this a vulnerability and released a security patch. This issue was fixed in version 1.3.4.	5.4	More Details
CVE-2026-42641	Server-Side Request Forgery (SSRF) vulnerability in ILLID Share This Image share-this-image allows Server Side Request Forgery.This issue affects Share This Image: from n/a through <= 2.14.	5.4	More Details
CVE-2026-7500	When Keycloak is started with `--features-disabled=account,account-api`, the Account REST API is only partially disabled. Five endpoints under the versioned path `/account/v1alpha1` remain fully functional — including both read and write operations — because they lack the `checkAccountApiEnabled()` gate that correctly blocks four other endpoints in the same REST service class. The user needs to have permissions to use the API.	5.4	More Details
CVE-2026-7502	A security vulnerability has been detected in LinkStackOrg LinkStack up to 4.8.6. The affected element is the function saveLink of the file app/Http/Controllers/UserController.php of the component Management Endpoint. The manipulation leads to authorization bypass. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	5.4	More Details
CVE-2026-27693	Traccar is an open source GPS tracking system. In org.traccar:traccar versions starting at 6.11.1 before 6.13.0, the KML and GPX export functionality writes device names to XML output without proper escaping. An attacker with low privileges can create a device with a crafted name that injects XML content into exported files. If another user exports and opens the affected KML or GPX file, this can corrupt the file structure and spoof exported location data. This issue is fixed in version 6.13.0.	5.4	More Details
CVE-2026-27694	Traccar is an open source GPS tracking system. In org.traccar:traccar versions starting at 6.11.1 before 6.13.0, the email notification templates insert user-controlled device, geofence, and driver names into HTML email output without proper escaping. An attacker with low privileges can store crafted HTML in these fields, which is then rendered in notification emails sent to other users with access to the affected devices. This can lead to phishing or spoofed email content. This issue is fixed in version 6.13.0.	5.4	More Details
CVE-2026-6446	The My Social Feeds – Social Feeds Embedder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to and including 1.0.4 via the 'ttp_get_accounts' AJAX action. This is due to the complete absence of authorization checks (no capability verification) and nonce verification in the get_accounts() function, which returns the full contents of the 'ttp_tiktok_accounts' WordPress option. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive TikTok OAuth credentials, including access_token and refresh_token values, that belong to administrator-connected TikTok accounts, enabling them to impersonate the site owner when interacting with the TikTok API.	5.4	More Details
CVE-2026-5077	The Total theme for WordPress is vulnerable to Stored Cross-Site Scripting via post titles in versions up to, and including, 2.2.1 due to insufficient output escaping when rendering the_title() inside HTML attribute context in the home blog section template. 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. Exploitation requires the malicious post to be published and displayed with a featured image in the Home Page blog section.	5.4	More Details
CVE-2026-42642	Missing Authorization vulnerability in StellarWP GiveWP give allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GiveWP: from n/a through <= 4.14.5.	5.3	More Details
CVE-2026-2729	The Forminator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.52.0. This is due to the plugin not properly verifying that a user is authorized to perform an action when processing attacker-supplied Stripe PaymentIntent identifiers in the public payment flow. This makes it possible for unauthenticated attackers to submit high-value paid forms as completed by reusing a previously succeeded low-value Stripe PaymentIntent, resulting in underpayment/payment bypass conditions.	5.3	More Details
CVE-2026-5335	The Magic Export & Import WordPress plugin before 1.2.0 stores exported CSV files at a publicly accessible location, making it possible for any visitors to leak sensitive user information.	5.3	More Details
CVE-2026-3143	The Total Upkeep – WordPress Backup Plugin plus Restore & Migrate by BoldGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_cli_cancel' function in all versions up to, and including, 1.17.1. This makes it possible for unauthenticated attackers to cancel a pending rollback, potentially preventing a WordPress installation from automatically reverting a failed update.	5.3	More Details

CVE-2026-43868	Memory Allocation with Excessive Size Value 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-2026-7580	A vulnerability was detected in Exiftool up to 13.53. Impacted is the function Process_mrld of the file lib/Image/ExifTool/GM.pm of the component JPEG/QuickTime/MOV/MP4. The manipulation of the argument -ee results in code injection. Attacking locally is a requirement. Upgrading to version 13.54 is recommended to address this issue. The patch is identified as 5a8b6b6ead12b39e3f32f978a4efd0233facbb01. It is suggested to upgrade the affected component. The fix in the source code mentions: "[J]ust to be safe, probably never happen".	5.3	More Details
CVE-2026-42644	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in WPDeveloper BetterDocs betterdocs allows Retrieve Embedded Sensitive Data.This issue affects BetterDocs: from n/a through <= 4.3.10.	5.3	More Details
CVE-2026-7734	A vulnerability has been found in osrg GoBGP up to 4.3.0. This impacts the function SRv6L3ServiceAttribute.DecodeFromBytes of the file pkg/packet/bgp/prefix_sid.go of the component SRv6 L3 Service. Such manipulation of the argument data leads to denial of service. The attack may be performed from remote. Upgrading to version 4.4.0 will fix this issue. The name of the patch is f9f7b55ec258e514be0264871fa645a2c3edad11. You should upgrade the affected component.	5.3	More Details
CVE-2026-7423	Integer underflow in the ICMP and ICMPv6 echo reply handlers in FreeRTOS-Plus-TCP before V4.4.1 and V4.2.6 allows an adjacent network user to cause a denial of service (device crash) when outgoing ping support is enabled, because header sizes are subtracted from a packet length field without validating the field is large enough, resulting in a heap out-of-bounds read of up to approximately 65KB. To mitigate this issue, users should upgrade to the fixed version when available.	5.3	More Details
CVE-2026-41572	Note Mark is an open-source note-taking application. Prior to version 0.19.3, after a note-mark owner soft-deletes a public book, its notes and uploaded assets stay readable at /api/notes/{id}, /api/notes/{id}/content, the slug URL, and the asset endpoints. Unauthenticated callers who hold the note ID or the slug path retain access. GORM's soft-delete scope does not reach the raw "JOIN books ..." clauses used by the note and asset queries. This issue has been patched in version 0.19.3.	5.3	More Details
CVE-2018-25298	Merge PACS 7.0 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions by crafting malicious HTML forms targeting the merge-viewer endpoint. Attackers can submit POST requests to /servlet/actions/merge-viewer/summary with login credentials to hijack user sessions and gain unauthorized access to the PACS system.	5.3	More Details
CVE-2026-7737	A vulnerability was identified in osrg GoBGP up to 4.3.0. Affected by this issue is the function BMPPeerUpNotification.ParseBody/BMPStatisticsReport.ParseBody of the file pkg/packet/bmp/bmp.go of the component BMP Parser. The manipulation leads to out-of-bounds read. The attack can be initiated remotely. Upgrading to version 4.4.0 can resolve this issue. The identifier of the patch is bc77597d42335c78464bc8e15a471d887bbdf260. Upgrading the affected component is recommended.	5.3	More Details
CVE-2026-33007	A NULL pointer dereference in the mod_authn_socache in Apache HTTP Server 2.4.66 and earlier allows an unauthenticated remote user to crash a child process in a caching forward proxy configuration. Users are recommended to upgrade to version 2.4.67, which fixes this issue.	5.3	More Details
CVE-2026-7396	A vulnerability was identified in NousResearch hermes-agent 0.8.0. Affected by this issue is some unknown functionality of the file gateway/platforms/wecom.py of the component WeChat Work Platform Adapter. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	5.3	More Details
CVE-2026-7722	A vulnerability was detected in PrefectHQ prefect up to 3.6.21. This impacts the function endswith of the file /api/health of the component Health Check API. Performing a manipulation results in improper authentication. The attack is possible to be carried out remotely. The exploit is now public and may be used. Upgrading to version 3.6.22 will fix this issue. The patch is named e21617125335025b4b27e7d6f0ca028e8e8f3b79. Upgrading the affected component is recommended. 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-2026-44029	An issue was discovered in Nix before 2.34.7. Writing to arbitrary files can occur via "nix-prefetch-url --unpack" or "nix store prefetch-file --unpack" directory traversal. The fixed versions are 2.34.7, 2.33.6, 2.32.8, 2.31.5, 2.30.5, 2.29.4, and 2.28.7 (introduced in 2.24.7);	5.3	More Details
CVE-2026-34032	Improper Null Termination, Out-of-bounds Read vulnerability in Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	5.3	More Details
CVE-2026-7582	A vulnerability was detected in AcademySoftwareFoundation OpenImageIO up to 3.2.0.1-dev. This vulnerability affects unknown code of the file src/dds.imageio/ddsinput.cpp of the component DDS Image Handler. The manipulation results in out-of-bounds write. The attack needs to be approached locally. The exploit is now public and may be used. The patch is identified as 94ec2deec3e3bf2f2e2ff84d008e27425d626fe2. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-2026-7403	A security flaw has been discovered in geldata gel-mcp 0.1.0. This impacts the function list_rules/fetch_rule of the file src/gel_mcp/server.py. The manipulation of the argument rule_name results in path traversal. 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.	5.3	More Details
CVE-2026-33857	Out-of-bounds Read vulnerability in mod_proxy_ajp of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	5.3	More Details
CVE-2026-7702	A vulnerability was detected in toeverything AFFiNE up to 0.26.3. This issue affects the function allowDocPreview of the file /workspace/:workspaceId/:docId of the component Public Markdown Preview Endpoint. The manipulation results in authorization bypass. 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.	5.3	More Details
CVE-2026-7536	A vulnerability was determined in Open5GS up to 2.7.7. This vulnerability affects the function bsf_sess_add_by_ip_address of the file /nbsf-management/v1/pcfBindings of the component BSF. Executing a manipulation of the argument ipv4Addr can lead to denial of service. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
	The Five Star Restaurant Reservations plugin for WordPress is vulnerable to a payment bypass via PHP type juggling in versions up to,		

CVE-2026-6498	and including, 2.7.16 This is due to the valid_payment() function using a PHP loose comparison (==) between the attacker-controlled payment_id POST parameter and the booking's stripe_payment_intent_id property. When an unauthenticated attacker submits a request to the nopriv AJAX handler rtb_stripe_pmt_succeed before the Stripe payment intent has been created for a booking (i.e., before the JavaScript-triggered create_stripe_pmtIntnt() call has stored an intent ID in post meta), the stripe_payment_intent_id property on the booking object remains null. The comparison sanitize_text_field('') == null evaluates to TRUE in PHP loose comparison, causing the payment verification check to pass with zero actual payment. This makes it possible for unauthenticated attackers to mark any existing payment_pending booking as paid without completing a Stripe payment by submitting an empty payment_id parameter.	5.3	More Details
CVE-2026-4024	The Royal Addons for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `wpr_update_form_action_meta` AJAX action in all versions up to, and including, 1.7.1056. The handler is registered on both `wp_ajax` and `wp_ajax_nopriv` hooks, making it accessible to unauthenticated users. Although a nonce is verified, the nonce (`wpr-addons-js`) is publicly exposed in frontend JavaScript via `WprConfig.nonce` on any page that loads Royal Addons widgets, rendering the protection ineffective. The endpoint also lacks any capability or ownership checks and directly calls `update_post_meta()` with user-controlled input on a whitelisted set of form action meta keys. This makes it possible for unauthenticated attackers to modify form action configuration metadata (email, submissions, Mailchimp, and webhook settings) on any post, potentially leading to webhook/email action tampering and data exfiltration via modified webhook URLs.	5.3	More Details
CVE-2026-43572	OpenClaw versions 2026.4.10 before 2026.4.14 contain a missing authorization vulnerability in the Microsoft Teams SSO invoke handler that fails to apply sender allowlist checks. Attackers can bypass sender authorization by sending SSO invoke requests that are processed without proper validation, allowing unauthorized access to Teams SSO signin functionality.	5.3	More Details
CVE-2026-6449	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to Improper Authorization in all versions up to, and including, 2.1.2. This is due to a logical short-circuit flaw in authorization logic that causes token validation to be entirely skipped when a booking has a 'waiting' status. This makes it possible for unauthenticated attackers to approve any booking that is in 'waiting' status by sending a crafted request to the publicly-accessible admin-ajax endpoint.	5.3	More Details
CVE-2026-4650	The FundPress – WordPress Donation Plugin for WordPress is vulnerable to authorization bypass in versions up to and including 2.0.8. This is due to missing authorization and nonce verification in the donate_action_status() AJAX handler, which is registered to be accessible to unauthenticated users via wp_ajax_nopriv. The function only validates that the schema parameter equals 'donate-ajax' and that the required POST parameters are present, but fails to verify user capabilities, nonce tokens, or donation ownership. This makes it possible for unauthenticated attackers to modify the status of any donation by providing its ID (which are sequential integers and easily enumerable), allowing them to mark donations as completed, pending, cancelled, or any arbitrary status, potentially triggering email notifications and related side effects.	5.3	More Details
CVE-2026-3504	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.1 via the '/dokan/v1/stores/{id}/reviews' REST API endpoint. This is due to the 'prepare_reviews_for_response' method including reviewer email addresses, usernames, and user IDs in the API response. This makes it possible for unauthenticated attackers to extract email addresses, usernames, and user IDs of all customers who left reviews on any vendor's store. The Pro version of the plugin must be installed and activated, with store reviews enabled, in order to exploit the vulnerability.	5.3	More Details
CVE-2026-7588	A vulnerability was found in ggerve coding-standards-mcp. This issue affects the function get_style_guide/get_best_practices of the file server.py. The manipulation of the argument Language results in path traversal. 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.	5.3	More Details
CVE-2025-14688	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 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 when certain configurations exist.	5.3	More Details
CVE-2026-37504	Sensitive server_token exposed via GET parameter in V2Board thru 1.7.4. In app/Http/Controllers/Server/UniProxyController.php, the server authentication token is accepted via GET parameter transmission. The token appears in URLs such as /api/v1/server/UniProxy/user?token=SECRET, causing it to be recorded in web server access logs, browser history, HTTP Referer headers, and proxy/CDN logs. An attacker who gains access to any log source can extract the token and impersonate a proxy server node, potentially intercepting all user traffic.	5.3	More Details
CVE-2026-43507	An issue was discovered in Prosody before 0.12.6 and 1.0.0 through 13.0.0 before 13.0.5. A Denial of Service can occur via memory exhaustion caused by XML parsing resource amplification from unauthenticated connections.	5.3	More Details
CVE-2026-43002	An issue was discovered in OpenStack Horizon 25.6 and 25.7 before 25.7.3. There is a write operation to the session storage backend before authentication and thus storage can be exhausted by unauthenticated requests. This is a regression of the CVE-2014-8124 fix.	5.3	More Details
CVE-2026-22745	Spring MVC and WebFlux applications are vulnerable to Denial of Service attacks when resolving static resources. More precisely, an application can be vulnerable when all the following are true: * the application is using Spring MVC or Spring WebFlux * the application is serving static resources from the file system * the application is running on a Windows platform When all the conditions above are met, the attacker can send malicious requests that are slow to resolve and that can keep HTTP connections in use. This can cause a Denial of Service on the application.	5.3	More Details
CVE-2026-7638	The App Builder – Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to and including 5.6.0. This is due to missing authorization validation in the `upload_avatar()` function, which accepts an attacker-controlled `user_id` parameter from the POST request body and uses it to update user meta without verifying that the authenticated requester owns or has permission to modify the target account. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the profile avatar of any arbitrary user on the site, including administrators, by supplying a target `user_id` in the request body to the `/wp-json/app-builder/v1/upload-avatar` endpoint.	5.3	More Details
CVE-2026-5766	An issue was discovered in 6.0 before 6.0.5 and 5.2 before 5.2.14. ASGI requests with a missing or understated `Content-Length` header can bypass the `FILE_UPLOAD_MAX_MEMORY_SIZE` limit, potentially loading large files into memory and causing service degradation. As a reminder, Django expects a limit to be configured at the web server level rather than solely relying on `FILE_UPLOAD_MAX_MEMORY_SIZE`. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Kyle Agronick for reporting this issue.	5.3	More Details

CVE-2026-40561	Starlet versions through 0.31 for Perl allows HTTP Request Smuggling via Improper Header Precedence. Starlet incorrectly prioritizes "Content-Length" over "Transfer-Encoding: chunked" when both headers are present in an HTTP request. Per RFC 7230 3.3.3, Transfer-Encoding must take precedence. An attacker could exploit this to smuggle malicious HTTP requests via a front-end reverse proxy.	5.3	More Details
CVE-2026-4019	The Complianz – GDPR/CCPA Cookie Consent plugin for WordPress is vulnerable to unauthorized data access in all versions up to, and including, 7.4.5 This is due to the REST API endpoint at /wp-json/complianz/v1/consent-area/{post_id}/{block_id} using __return_true as the permission_callback, allowing any unauthenticated user to access it. The cmplz_rest_consented_content() function retrieves a post by ID via get_post() and returns the consentedContent attribute of any complianz/consent-area block found in it, without checking if the post is published or if the user has permission to read it. This makes it possible for unauthenticated attackers to read the consent area block content from private, draft, or unpublished posts.	5.3	More Details
CVE-2026-43506	An issue was discovered in Prosody before 0.12.6 and 1.0.0 through 13.0.0 before 13.0.5. A Denial of Service can occur via memory exhaustion caused by memory leaks from unauthenticated connections.	5.3	More Details
CVE-2025-36180	IBM watsonx.data 2.2 through 2.3 IBM Lakehouse does not properly restrict communication between pods which could allow an attacker to transfer data between pods without restrictions.	5.3	More Details
CVE-2026-7589	A vulnerability was determined in ghantakiran splunk-mcp-integration up to 0b86b09d5e5adf0433acd43c975951224613a1a6. Impacted is the function create_csv_export of the file services/csv-export-service/app/api/v1/endpoints/csv_export.py of the component CSV Export. This manipulation of the argument job_name causes path traversal. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-7686	A vulnerability was found in eyeo Adblock Plus up to 4.36.2 on Chrome. Affected by this vulnerability is the function postMessage of the file premium.preload.js of the component Legacy Premium Activation. Performing a manipulation results in improper access controls. Remote exploitation of the attack is possible. The exploit has been made public and could be used. Upgrading the affected component is recommended. The vendor provides additional details: "The affected code path is a legacy Premium activation flow that has been deprecated. eyeo has already migrated to a new user account-based licensing system. The exploit does not grant permanent Premium access. The licensing server issues a short-lived trial license (valid for approximately 24 hours) for any submitted userId. On the next license check, the server validates against a real subscription and the trial expires if no valid subscription is found. The researcher's claim of permanently unlocking all Premium features is therefore incorrect. (...) The old flow has been present for years and has not been weaponized at scale to our knowledge. The risk to eyeo and to users is minimal."	5.3	More Details
CVE-2026-42077	Evolver is a GEP-powered self-evolving engine for AI agents. Prior to version 1.69.3, a prototype pollution vulnerability in the mailbox store module allows attackers to modify the behavior of all JavaScript objects by injecting malicious properties into Object.prototype. The vulnerability exists in the _applyUpdate() and _updateRecord() functions which use Object.assign() to merge user-controlled data without filtering dangerous keys like __proto__, constructor, or prototype. This issue has been patched in version 1.69.3.	5.2	More Details
CVE-2026-22726	Route Services can be leveraged to send app traffic to network destinations outside of an app's configured egress rules. As a result, a malicious developer with access to Cloudfoundry could configure a route-service that would allow it to send requests to HTTP services on internal networks reachable by the Gorouter, which may not have previously had direct access from outside networks, or from the application. Routing release: affected from v0.118.0 through v0.371.0 (inclusive); upgrade to v0.372.0 or greater. CF Deployment: affected from v0.0.2 through v54.14.0 (inclusive); upgrade to v55.0.0 or greater (includes routing_release v0.372.0).	5.0	More Details
CVE-2026-7724	A vulnerability has been found in PrefectHQ prefect up to 3.6.28.dev1. Affected by this vulnerability is the function validate_restricted_url of the component Webhook/Notification. The manipulation leads to time-of-check time-of-use. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 3.6.28.dev2 addresses this issue. The identifier of the patch is 7c70ac54a5e101431d83b9f2681ec88d5e0021ed. Upgrading the affected component is advised. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	5.0	More Details
CVE-2026-7778	An issue that could allow a dashboard configuration to be viewed from outside of the authorized organization scope has been resolved. This is an instance of CWE-269: Improper Privilege Management, and has an estimated CVSS score of CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N (5.0, Medium). This issue was fixed in version v4.0.260416.0 of the runZero Platform.	5.0	More Details
CVE-2026-7688	A vulnerability was identified in Dolibarr ERP CRM up to 23.0.2. This affects the function _checkValForAPI of the file htdocs/expedition/class/expedition.class.php of the component Shipments API Endpoint. The manipulation of the argument fields leads to sql injection. The attack is possible to be carried out remotely. A high degree of complexity is needed for the attack. It is indicated that the exploitability is 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.	5.0	More Details
CVE-2026-36764	A Server-Side Request Forgery (SSRF) in the /ureport/datasource/testConnection endpoint of SpringBlade v4.8.0 allows authenticated attackers to scan internal resources via a crafted GET request.	5.0	More Details
CVE-2026-6948	Velociraptor versions prior to 0.76.4 contain a resource exhaustion vulnerability in the server's agent control channel. This allows a compromised or rogue Velociraptor client to crash the server via out-of-memory (OOM) by sending crafted messages through the normal client communication channel.	4.9	More Details
CVE-2026-1921	The Loco Translate plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 2.8.2 via the `fsReference` AJAX route. This is due to the `findSourceFile()` method normalizing user-supplied `ref` paths containing `../` directory traversal sequences without validating that the resolved path remains within the intended bundle or content directory. This makes it possible for authenticated attackers, with Translator-level access and above (custom `loco_admin` capability required, granted to the `translator` role and administrators by default), to read arbitrary `.php`, `.js`, `.json`, and `.twig` files from the server filesystem outside the intended translation directory. Files named wp-config.php are excluded.	4.9	More Details
CVE-2026-0206	A post-authentication Stack-based Buffer Overflow vulnerabilities in SonicOS allows a remote attacker to crash a firewall.	4.9	More Details

CVE-2026-37505	SQL Injection via ORDER BY clause in V2Board thru 1.7.4. In app/Http/Controllers/Admin/UserController.php, the sort parameter from user input is passed directly to User::orderBy($sort, $sortType) without validation. An authenticated admin can sort users by any database column including password, remember_token, and other sensitive fields, enabling information disclosure through ordering analysis.	4.9	More Details
CVE-2026-33006	A timing attack against mod_auth_digest in Apache HTTP Server 2.4.66 allows a bypass of Digest authentication by a remote attacker. Users are recommended to upgrade to version 2.4.67, which fixes this issue.	4.8	More Details
CVE-2026-1858	wget2 accepts a server certificate with incorrect Key Usage (KU) or Extended Key Usage (EKU). If the attackers compromise a certificate (with the associated private key) issued for a different purpose, they may be able to reuse it for TLS server authentication.	4.8	More Details
CVE-2026-40687	In Exim before 4.99.2, when the SPA authentication driver is used with an adversarial SPA resource, there can be an out-of-bounds write that crashes the connection instance, or erroneous data processing that divulges data from uninitialized heap memory.	4.8	More Details
CVE-2026-5404	K12 RF5 file parser crash in Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14 allows denial of service	4.7	More Details
CVE-2026-7388	A weakness has been identified in EyouCMS up to 1.7.9. Impacted is the function editFile of the file application/admin/logic/FilemanagerLogic.php of the component Template File Handler. Executing a manipulation can lead to code injection. 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.	4.7	More Details
CVE-2026-7407	A security vulnerability has been detected in SourceCodester Pizzafy Ecommerce System 1.0. Affected by this vulnerability is the function save_settings of the file /pizzafy/admin/ajax.php?action=save_settings of the component Setting Handler. Such manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2026-7408	A vulnerability was detected 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. Performing a manipulation results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	4.7	More Details
CVE-2026-7697	A vulnerability was determined in AMTT Hotel Broadband Operation System 1.0. Affected is an unknown function of the file /manager/card/cardhand_submit.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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.	4.7	More Details
CVE-2026-7553	A vulnerability was found in code-projects Gym Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/edit_exercises.php. The manipulation of the argument edit_exercise results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2026-7409	A flaw has been found in SourceCodester Pizzafy Ecommerce System 1.0. This affects the function save_user of the file /admin/ajax.php?action=save_user. Executing a manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2026-7673	A vulnerability was detected in crmeb_java up to 1.3.4. This vulnerability affects unknown code of the file crmeb/crmeb-service/src/main/java/com/zbkj/service/service/impl/UploadServiceImpl.java of the component Admin Upload. Performing a manipulation of the argument model results in unrestricted upload. Remote exploitation of the attack is possible. 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-2026-7393	A vulnerability was found in SourceCodester Pizzafy Ecommerce System 1.0. Affected is the function save_menu of the file /admin/admin_class_novo.php of the component File Extension Handler. Performing a manipulation of the argument img results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2026-7394	A vulnerability was determined in SourceCodester Pizzafy Ecommerce System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/view_order.php of the component GET Parameter Handler. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-52206	ISPConfig 3.3.0 is vulnerable to Cross Site Scripting (XSS) via the system status webpage.	4.7	More Details
CVE-2026-7578	A weakness has been identified in MacCMS Pro up to 2022.1.3. This vulnerability affects the function install of the file /admi.php/admin/addon/add.html of the component Plugin Installation Handler. Executing a manipulation can lead to unrestricted upload. The attack may be performed from remote. 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.	4.7	More Details
CVE-2026-7612	A vulnerability was determined in itsourcecode Courier Management System 1.0. Affected is an unknown function of the file /edit_user.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-7429	SSCMS v7.4.0 contains a reflected cross-site scripting vulnerability in the STL processing endpoint that allows attackers to execute arbitrary JavaScript by crafting malicious STL template payloads that are decrypted and returned without proper sanitization. Attackers can exploit improper output encoding in the /api/stl/actions/dynamic endpoint to inject executable JavaScript into JSON responses, leading to session hijacking, phishing attacks, and unauthorized actions performed on behalf of users.	4.6	More Details
CVE-2026-42086	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. Prior to version 7.0.0, the Command Sender UI uses an unsafe eval() function on array-like command parameters, which allows a user-supplied payload to execute in the browser when sending a command. This creates a self-XSS risk because an attacker can trigger their own script execution in the victim’s session, if allowed to influence the array parameter input, for example via phishing. If successful, an attacker may read or modify data in the authenticated browser context, including session tokens in local storage. This issue has been patched in version 7.0.0.	4.6	More Details

CVE-2026-42080	PPTAgent is an agentic framework for reflective PowerPoint generation. Prior to commit 418491a, there is an arbitrary file write vulnerability via `save_generated_slides`. This issue has been patched via commit 418491a.	4.6	More Details
CVE-2026-42078	PPTAgent is an agentic framework for reflective PowerPoint generation. Prior to commit 418491a, PPTAgent is vulnerable to arbitrary file write and directory creation via markdown_table_to_image. This issue has been patched via commit 418491a.	4.6	More Details
CVE-2026-6539	Notepad++ 8.9.3 contains a format string injection vulnerability in the Find Results panel handler that allows attackers to cause denial of service and information disclosure by crafting a malicious nativeLang.xml language pack file. Attackers can distribute a poisoned language pack through community channels that triggers format string interpretation when a user performs search operations, leading to access violations and potential leakage of stack or register contents.	4.4	More Details
CVE-2026-40949	CVE-2026-40949 is a buffer overflow vulnerability in the Secure Access Windows client prior to 14.50. Attackers with local control of the Windows client can use it to trigger a denial of service.	4.4	More Details
CVE-2026-35233	An unprivileged attacker can craft a user-space process with a malicious ELF binary containing an out-of-range sh_link field. When root-level dtrace attaches to -- or instruments -- that process (via dtrace -p , pid probes, or USDT), the ELF parser reads heap memory beyond the allocated section cache array without any bounds check. This results in an uninitialized/out-of-bounds heap read that can cause a NULL pointer dereference crash of the dtrace process (DoS), or -- depending on heap layout -- a read-then-use of a garbage pointer controlled by adjacent allocations, providing a foothold toward further exploitation in a privileged context.	4.4	More Details
CVE-2026-26204	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 1.0.0 to before version 4.14.4, a heap-based out-of-bounds WRITE occurs in GetAlertData, resulting in writing a NULL byte exactly 1 byte before the start of the buffer allocated by strdup. Due to unsigned integer underflow and pointer arithmetic wrapping, the write lands at offset -1 from the buffer, corrupting heap metadata. A malicious actor can potentially leverage this issue through a compromised agent to cause denial of service or heap corruption by injecting a specially crafted alert into the alerts log file monitored by wazuh-logcollector. This issue has been patched in version 4.14.4.	4.4	More Details
CVE-2026-6812	The Ona theme for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.26 via the ona_activate_child_theme. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	4.4	More Details
CVE-2026-42140	PlantUML Macro is a macro for rendering UML diagrams from simple textual schemes. Prior to version 2.4.1, the PlantUML Macro is vulnerable to Server-Side Request Forgery (SSRF). The macro allows users to specify an alternative PlantUML server via the server parameter. However, the application does not validate the supplied URL. An attacker can supply an internal IP address or a malicious external URL. The XWiki server will attempt to connect to this URL to "render" the diagram. This issue has been patched in version 2.4.1.	4.4	More Details
CVE-2026-7439	AgentFlow's local web API accepts non-JSON content types on POST /api/runs and POST /api/runs/validate endpoints without enforcing application/json validation, allowing attackers to bypass trust-boundary enforcement on sensitive operations. Attackers can exploit this content-type validation weakness through browser-driven or local cross-origin requests to abuse the localhost API and enable attack chains against the local control plane.	4.4	More Details
CVE-2026-7397	A security flaw has been discovered in NousResearch hermes-agent 0.8.0. This affects the function _check_sensitive_path of the file tools/file_tools.py. The manipulation results in symlink following. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.9.0 is able to mitigate this issue. The patch is identified as 311dac197145e19e07df68feba2cd55d896a3cd1. Upgrading the affected component is recommended.	4.4	More Details
CVE-2026-6447	The Call for Price for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.2.0 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-2026-7401	A vulnerability was detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This vulnerability affects unknown code of the file /index.php?action=register of the component Registration. The manipulation of the argument student_id/full_name/section/username results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-7583	A flaw has been found in Open5GS up to 2.7.7. This issue affects the function bsf_sess_find_by_ipv6prefix of the file /src/bsf/context.c of the component BSF. This manipulation of the argument ipv6Prefix causes denial of service. It is possible to initiate 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.	4.3	More Details
CVE-2026-7518	A flaw has been found in Open5GS up to 2.7.7. This issue affects the function amf_namf_callback_handle_sdm_data_change_notify of the file /namf-callback/v1/{id}/sdmsubscription-notify of the component AMF SBI Endpoint. This manipulation of the argument changeItem.newValue causes denial of service. The attack can be initiated 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.	4.3	More Details
CVE-2026-7587	A vulnerability has been found in Open5GS up to 2.7.7. This vulnerability affects the function amf_nsmf_pdusession_handle_update_sm_context of the file /src/amf/nsmf-handler.c of the component AMF. The manipulation leads to denial of service. 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.	4.3	More Details
CVE-2026-42085	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. Prior to versions 6.10.5 and 7.0.0-rc3, OpenC3 COSMOS contains a design flaw in the save_tool_config() function that allows saving tool configuration files at arbitrary locations inside the shared /plugins directory tree by supplying crafted configuration filenames. Although the implementation sufficiently mitigates standard path traversal attacks, by canonicalizing filename to an absolute path, all plugins share this same root directory. That enables users to create arbitrary file structures and overwrite existing configuration files within the shared /plugins directory. This issue has been patched in versions 6.10.5 and 7.0.0-rc3.	4.3	More Details
CVE-2026-	Incomplete validation of AI rich response messages for Instagram Reels in WhatsApp for iOS v2.25.8.0 to v2.26.15.72 and WhatsApp for Android v2.25.8.0 to v2.26.7.10 could have allowed a user to trigger processing of media content from an arbitrary URL on	4.3	More

23866	another user’s device, including triggering OS-controlled custom URL scheme handlers. We have not seen evidence of exploitation in the wild.		Details
CVE-2026-42525	Jenkins Microsoft Entra ID (previously Azure AD) Plugin 666.v6060de32f87d and earlier does not restrict the redirect URL after login, allowing attackers to perform phishing attacks.	4.3	More Details
CVE-2026-7779	A security flaw has been discovered in Open5GS up to 2.7.7. Affected is the function udm_nudr_dr_handle_subscription_authentication of the file /src/udm/nudr-handler.c of the component authentication-subscription Endpoint. Performing a manipulation results in denial of service. Remote exploitation of the attack is possible. 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.	4.3	More Details
CVE-2026-42522	A missing permission check in Jenkins GitHub Branch Source Plugin 1967.vdea_d580c1a_b_a_ and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL with attacker-specified GitHub App credentials.	4.3	More Details
CVE-2026-3601	The User Registration & Membership plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `embed_form_action()` function in all versions up to, and including, 5.1.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to append shortcode content to arbitrary pages they do not own or have permission to edit.	4.3	More Details
CVE-2026-7781	A security vulnerability has been detected in Open5GS up to 2.7.7. Affected by this issue is the function udm_nudm_uecm_handle_amf_registration_update of the file /src/udm/nudm-handler.c of the component amf-3gpp-access Endpoint. The manipulation leads to denial of service. 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.	4.3	More Details
CVE-2026-42645	Cross-Site Request Forgery (CSRF) vulnerability in Dmitry V. (CEO of "UKR Solution") Barcode Scanner with Inventory & Order Manager barcode-scanner-lite-pos-to-manage-products-inventory-and-orders allows Cross Site Request Forgery.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through <= 1.11.0.	4.3	More Details
CVE-2026-7586	A weakness has been identified in Open5GS up to 2.7.7. Affected is the function ogs_id_get_value of the file /src/amf/nudm-handler.c of the component AMF. This manipulation causes denial of service. 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.	4.3	More Details
CVE-2026-42648	Missing Authorization vulnerability in Brainstorm Force Spectra ultimate-addons-for-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Spectra: from n/a through <= 2.19.22.	4.3	More Details
CVE-2018-25310	VideoFlow Digital Video Protection DVP 2.10 contains an authenticated remote code execution vulnerability that allows authenticated attackers to execute arbitrary system commands by exploiting a cross-site request forgery flaw in the web management interface. Attackers with valid credentials can leverage the CSRF vulnerability to inject and execute system commands through the Tools > System > Shell interface, gaining root-level access to the device.	4.3	More Details
CVE-2026-42519	A missing permission check in Jenkins Script Security Plugin 1399.ve6a_66547f6e1 and earlier allows attackers with Overall/Read permission to enumerate pending and approved Script Security classpaths.	4.3	More Details
CVE-2026-7585	A vulnerability was determined in Open5GS up to 2.7.7. The impacted element is the function amf_nudm_sdm_handle_provisioned of the file /src/amf/nudm-handler.c of the component AMF. Executing a manipulation can lead to denial of service. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-6907	An issue was discovered in 6.0 before 6.0.5 and 5.2 before 5.2.14. `django.middleware.cache.UpdateCacheMiddleware` erroneously caches requests where the `Vary` header contained an asterisk (`'*'`). This can lead to private data being stored and served. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Ahmad Sadeddin for reporting this issue.	4.3	More Details
CVE-2026-7780	A weakness has been identified in Open5GS up to 2.7.7. Affected by this vulnerability is the function udm_state_operational of the file /src/udm/udm-sm.c of the component smf-registrations Endpoint. Executing a manipulation can lead to denial of service. 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.	4.3	More Details
CVE-2026-7581	A security vulnerability has been detected in alexta69 MeTube up to 2026.04.09. This affects the function on_prepare of the file app/main.py of the component CORS Policy. The manipulation leads to permissive cross-domain policy with untrusted domains. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 2026.04.10 is able to mitigate this issue. The identifier of the patch is 0072d3488ae5b8d922d3ee87458d829993742a32. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2026-23773	Dell Disk Library for Mainframe, version(s) DLm 8700/2700 contain(s) a Server-Side Request Forgery (SSRF) vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Server-side request forgery.	4.3	More Details
CVE-2026-36757	A Server-Side Request Forgery (SSRF) in the /plugins/{name}/upgrade-from-uri endpoint of halo v2.22.14 allows authenticated attackers to scan internal resources via a crafted GET request.	4.3	More Details
CVE-2026-36758	A Server-Side Request Forgery (SSRF) in the /themes/-/install-from-uri endpoint of halo v2.22.14 allows authenticated attackers to scan internal resources via a crafted GET request.	4.3	More Details
CVE-2026-7676	A vulnerability was found in kerwincui FastBee up to 1.2.1. The affected element is the function ToolController.download of the file springboot/fastbee-open-api/src/main/java/com/fastbee/data/controller/ToolController.java of the component Tool Download Endpoint. The manipulation of the argument fileName results in path traversal. The attack may be performed from remote. The exploit has	4.3	More Details

	been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-6700	The DX Sources plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.1. This is due to missing or incorrect nonce validation on the settings_page_build function. This makes it possible for unauthenticated attackers to trick a logged-in administrator into submitting a forged request that modifies the plugin's 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-2026-7701	A security vulnerability has been detected in Telegram Desktop up to 6.7.5. This vulnerability affects the function RequestButton of the file Telegram/SourceFiles/boxes/url_auth_box.cpp of the component Bot API. The manipulation of the argument login_url leads to null pointer dereference. 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.	4.3	More Details
CVE-2026-7704	A vulnerability has been found in AV Stumpfl Pixera Two Media Server up to 25.1 R2. The affected element is an unknown function of the component Service Port 1338. Such manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 25.2 R3 is sufficient to fix this issue. It is advisable to upgrade the affected component.	4.3	More Details
CVE-2026-6701	The addfreespace plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.1.3. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts 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-2026-7601	A vulnerability has been found in Open5GS up to 2.7.6. Affected is an unknown function of the file src/amf/gmm-handler.c of the component AMF. The manipulation of the argument reg_type leads to denial of service. The attack is possible to be carried out remotely. Upgrading to version 2.7.7 is able to address this issue. The identifier of the patch is ebc66942b6f8f1fab2d640e71cf4e9f1a423b426. It is advisable to upgrade the affected component.	4.3	More Details
CVE-2026-7643	A flaw has been found in ChatGPTNextWeb NextChat up to 2.16.1. This impacts an unknown function of the file Next.js of the component API Endpoint. Executing a manipulation can lead to permissive cross-domain policy with untrusted domains. The attack may 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.	4.3	More Details
CVE-2026-7706	A vulnerability has been found in Open5GS up to 2.7.7. This issue affects the function gmm_handle_service_request of the file /src/amf/gmm-handler.c of the component AMF. The manipulation leads to denial of service. The attack can be initiated 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.	4.3	More Details
CVE-2026-7596	A vulnerability has been found in nextlevelbuilder ui-ux-pro-max-skill up to 2.5.0. Affected by this issue is the function data.get of the file .claude/skills/design-system/scripts/generate-slide.py of the component Slide Generator. Such manipulation 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 project was informed of the problem early through a pull request but has not reacted yet.	4.3	More Details
CVE-2026-3140	The Ultimate Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.14. This is due to a flawed nonce validation conditional in the 'handle_module_actions' function. This makes it possible for unauthenticated attackers to toggle plugin modules on or off 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-2026-7535	A vulnerability was found in Open5GS up to 2.7.7. This affects the function amf_namf_comm_handle_registration_status_update_request in the library /lib/app/ogs-init.c of the file /namf-comm/v1/ue-contexts/{ueContextId}/transfer-update. Performing a manipulation of the argument ueContextId results in denial of service. 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.	4.3	More Details
CVE-2026-7680	A weakness has been identified in jsbroks COCO Annotator up to 0.11.1. Affected is an unknown function of the file backend/webserver/api/datasets.py of the component Data Endpoint. Executing a manipulation of the argument folder 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 vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-7707	A vulnerability was found in Open5GS up to 2.7.7. Impacted is the function udr_nudr_dr_handle_subscription_context of the file /src/udr/nudr-handler.c of the component UDR. The manipulation of the argument pei results in denial of service. The attack can be launched 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.	4.3	More Details
CVE-2026-7708	A vulnerability was determined in Open5GS up to 2.7.7. The affected element is the function ogs_dbi_subscription_data in the library /lib/dbi/subscription.c of the component UDR. This manipulation of the argument supi_id causes denial of service. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-42798	Little CMS (lcms2) 2.16 through 2.18 before 2.19 has an integer overflow in ParseCube in cmscgats.c.	4.0	More Details
CVE-2026-7611	A vulnerability was found in TRENDnet TEW-821DAP up to 1.12B01. This impacts the function platform_do_upgrade_cameo_dev of the file cameo_dev.sh of the component Firmware Update Handler. Performing a manipulation results in insufficient verification of data authenticity. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is said to be difficult. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	3.7	More Details
CVE-2026-7610	A vulnerability has been found in TRENDnet TEW-821DAP 1.12B01. This affects an unknown function of the file /www/cgi/ssi of the component Firmware Update. Such manipulation leads to cleartext transmission of sensitive information. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is reported as difficult. The exploit has been disclosed to the public and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	3.7	More Details

CVE-2026-43859	mutt before 2.3.2 sometimes uses strfcpy instead of memcpy for the IMAP auth_cram MD5 digest.	3.7	More Details
CVE-2026-43860	mutt before 2.3.2 sometimes truncates the hash_passwd by one byte for IMAP auth_cram MD5 digest.	3.7	More Details
CVE-2026-41263	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is a timing side-channel vulnerability in Traefik's BasicAuth middleware that allows an attacker to enumerate valid usernames through response-time differences. The variable intended to hold a constant-time fallback secret always resolves to an empty string, causing the constant-time comparison to short-circuit in microseconds rather than performing a full bcrypt evaluation. This restores the original timing oracle and makes it possible to distinguish existing users from non-existing ones by measuring authentication response times. This issue has been patched in versions 2.11.43, 3.6.14, and 3.7.0-rc.2.	3.7	More Details
CVE-2026-43861	mutt before 2.3.2 does not check for '\0' in url_pct_decode.	3.7	More Details
CVE-2026-43862	In mutt before 2.3.2, the imap_auth_gss security level is mishandled.	3.7	More Details
CVE-2026-40686	In Exim before 4.99.2, when utf8 operators are enabled, there is an out-of-bounds read if large UTF-8 trailing characters are present (malformed UTF-8 header data). Information might be divulged within an error message produced during handling of an unrelated e-mail message.	3.7	More Details
CVE-2026-43863	mutt before 2.3.2 has an infinite loop in data_object_to_stream in crypt-gpgme.c.	3.7	More Details
CVE-2026-43964	Postfix before 3.8.16, 3.9 before 3.9.10, and 3.10 before 3.10.9 sometimes allows a buffer over-read and process crash via an enhanced status code that lacks text after the third number.	3.7	More Details
CVE-2026-7671	A vulnerability has been found in CodeWise Tornet Scooter Mobile App 4.75 on iOS/Android. The impacted element is an unknown function of the file /TwoFactor. Such manipulation leads to improper restriction of excessive authentication attempts. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is regarded as difficult. 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.	3.7	More Details
CVE-2026-3832	A flaw was found in gnutls. A remote attacker could exploit this vulnerability by presenting a specially crafted Online Certificate Status Protocol (OCSP) response during a TLS handshake. Due to a logic error in how gnutls processes multi-record OCSP responses, a client with OCSP verification enabled may incorrectly accept a revoked server certificate, potentially leading to a compromise of trust.	3.7	More Details
CVE-2026-7606	A weakness has been identified in TRENDnet TEW-821DAP 1.12B01. This issue affects the function find_hwid/new_gui_update_firmware of the component Firmware Update Handler. Executing a manipulation of the argument dest can lead to insufficient verification of data authenticity. The attack can be launched remotely. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	3.7	More Details
CVE-2026-7689	A security flaw has been discovered in Dolibarr ERP CRM up to 23.0.2. This vulnerability affects the function dol_verifyHash in the library htdocs/core/lib/security.lib.php of the component Online Signature Module. The manipulation results in improper verification of cryptographic signature. The attack may be performed from remote. Attacks of this nature are highly complex. It is stated that the exploitability is 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.	3.7	More Details
CVE-2026-7677	A vulnerability was determined in kerwincui FastBee up to 1.2.1. The impacted element is the function Add of the file springboot/fastbee-admin/src/main/java/com/fastbee/web/controller/system/SysNoticeController.java of the component System Notice Handler. This manipulation of the argument noticeContent causes cross site scripting. It is possible to initiate the attack 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.	3.5	More Details
CVE-2026-7501	A weakness has been identified in LinkStackOrg LinkStack up to 4.8.6. Impacted is the function editPage of the file app/Http/Controllers/UserController.php. Executing a manipulation of the argument pageDescription 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. The project was informed of the problem early through a pull request but has not reacted yet.	3.5	More Details
CVE-2026-7390	A vulnerability was detected in SourceCodester Pharmacy Sales and Inventory System 1.0. The impacted element is the function Customer of the file /index.php?page=customer. The manipulation of the argument Name results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2026-21996	An unprivileged attacker can reliably trigger a crash of the dtrace process with a malicious ELF binary due to an integer Divide-by-Zero in Pbuild_file_symtab()	3.3	More Details
CVE-2026-7739	A weakness has been identified in justdan96 tsMuxer up to 2.7.0. This vulnerability affects the function HevcVpsUnit::setFPS of the file /AFLplusplus/tsMuxer_prev/tsMuxer/hevc.cpp. This manipulation of the argument track_id causes denial of service. The attack requires local access. The exploit has been made available to the public and could be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	3.3	More Details
CVE-2026-7740	A security vulnerability has been detected in justdan96 tsMuxer up to 2.7.0. This issue affects the function VvcVpsUnit::setFPS of the file tsMuxer/vvc.cpp. Such manipulation of the argument track_id leads to denial of service. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	3.3	More Details

CVE-2026-33448	CVE-2026-33448 is a format string vulnerability in the logging subsystem of Secure Access client for MacOS prior to 14.50. Attackers with control of a modified server can force the client to dump the contents of a small portion of memory to the log files potentially revealing secrets.	3.3	More Details
CVE-2026-22741	Spring MVC and WebFlux applications are vulnerable to cache poisoning when resolving static resources. More precisely, an application can be vulnerable when all the following are true: * the application is using Spring MVC or Spring WebFlux * the application is configuring the resource chain support https://docs.spring.io/spring-framework/reference/web/webmvc/mvc-config/static-resources.html#page-title with caching enabled * the application adds support for encoded resources resolution * the resource cache must be empty when the attacker has access to the application When all the conditions above are met, the attacker can send malicious requests and poison the resource cache with resources using the wrong encoding. This can cause a denial of service by breaking the front-end application for clients.	3.1	More Details
CVE-2026-7846	A vulnerability has been found in chatchat-space Langchain-Chatchat up to 0.3.1.3. Impacted is the function files of the file libs/chatchat-server/chatchat/server/api_server/openai_routes.py of the component OpenAI-Compatible File Upload API. Such manipulation of the argument file.filename leads to time-of-check time-of-use. Access to the local network is required for this attack to succeed. The attack requires a high level of complexity. The exploitability is considered difficult. 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.	2.6	More Details
CVE-2026-7845	A flaw has been found in chatchat-space Langchain-Chatchat up to 0.3.1.3. This issue affects the function PIL.Image.tobytes of the file libs/chatchat-server/chatchat/webui_pages/dialogue/dialogue.py of the component Vision Chat Paste Image Handler. This manipulation of the argument paste_image.image_data causes use of weak hash. The attacker needs to be present on the local network. The attack is considered to have high complexity. The exploitability is assessed as difficult. 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.	2.6	More Details
CVE-2026-7847	A vulnerability was found in chatchat-space Langchain-Chatchat up to 0.3.1.3. The affected element is the function _get_file_id of the file libs/chatchat-server/chatchat/server/api_server/openai_routes.py of the component Uploaded File Handler. Performing a manipulation results in insufficiently random values. Access to the local network is required for this attack. The attack's complexity is rated as high. The exploitability is described as difficult. 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.	2.6	More Details
CVE-2026-43529	OpenClaw before 2026.4.10 contains a time-of-check-time-of-use vulnerability in the validateScriptFileForShellBleed function that allows local attackers to bypass workspace boundary checks. An attacker with workspace write access can race-condition swap the target file between validation and preflight read, causing the validator to inspect a different file identity than the one that passed the initial boundary check.	2.5	More Details
CVE-2026-43864	mutt before 2.3.2 has a show_sig_summary NULL pointer dereference.	2.5	More Details
CVE-2026-6180	A race condition exists in PaperCut MF when processing badge-swipe data from certain HP multifunction devices. Under specific network conditions involving dropped packets and out-of-order sequence counters, the server may incorrectly process fragmented data chunks. If a sequence reset notification fails to reach the server, the server may reject the initial data chunk while erroneously accepting subsequent chunks before a connection reset completes. This leads to the registration of a truncated badge ID string. While this typically results in an authentication failure, the vulnerability is compounded in environments utilizing custom badge-ID post-processing scripts. In such configurations, the truncated string may be transformed into a valid ID belonging to a different user, leading to unauthorized session establishment (Incorrect User Login) on the device.	N/A	More Details
CVE-2026-40330	Masa CMS is an open source content management system. In versions 7.2.0 through 7.2.9, 7.3.0 through 7.3.14, 7.4.0 through 7.4.9, and 7.5.0 through 7.5.2, a SQL injection vulnerability exists in the beanFeed.cfc component within the getQuery function's handling of the sortDirection parameter. The parameter value is concatenated directly into SQL queries without sanitization or parameterization. An unauthenticated remote attacker can exploit this to extract sensitive information, modify or delete database records, or potentially achieve remote code execution on the underlying database server. This issue has been fixed in versions 7.2.10, 7.3.15, 7.4.10, and 7.5.3. As a workaround, use a WAF to block or restrict access to the beanFeed.cfc component, or deploy rules to detect SQL injection patterns targeting the sortDirection parameter.	N/A	More Details
CVE-2026-43062	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix type confusion in l2cap_ecred_reconf_rsp() l2cap_ecred_reconf_rsp() casts the incoming data to struct l2cap_ecred_conn_rsp (the ECRED *connection* response, 8 bytes with result at offset 6) instead of struct l2cap_ecred_reconf_rsp (2 bytes with result at offset 0). This causes two problems: - The sizeof(*rsp) length check requires 8 bytes instead of the correct 2, so valid L2CAP_ECRED_RECONF_RSP packets are rejected with -EPROTO. - rsp->result reads from offset 6 instead of offset 0, returning wrong data when the packet is large enough to pass the check. Fix by using the correct type. Also pass the already byte-swapped result variable to BT_DBG instead of the raw __le16 field.	N/A	More Details
CVE-2026-43870	Origin Validation Error, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting'), Uncontrolled Resource Consumption 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.	N/A	More Details
CVE-2026-40331	Masa CMS is an open source content management system. In versions 7.2.0 through 7.2.9, 7.3.0 through 7.3.14, 7.4.0 through 7.4.9, and 7.5.0 through 7.5.2, the unauthenticated JSON API accepts an altTable parameter that is stored via the setAltTable() method without validation or sanitization. This value is injected directly into a SQL FROM clause within feedGateway.cfc. An unauthenticated attacker can pass an arbitrary subquery into the altTable parameter to read sensitive data from any table in the database in a single HTTP request, including administrative credentials and password reset tokens. This issue has been fixed in versions 7.2.10, 7.3.15, 7.4.10, and 7.5.3. As a workaround, apply validation to the setAltTable function in core/mura/content/feed/feedBean.cfc to restrict input to simple alphanumeric table names, or disable the JSON API if it is not required.	N/A	More Details
CVE-2026-43869	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.	N/A	More Details
CVE-2026-7824	An issue was discovered in the PaperCut Hive Ricoh embedded application. When the "Deep Logging" (diagnostic) mode is enabled, the application inadvertently records administrative credentials in plain text within the log files. An attacker with administrative access to the PaperCut Hive management portal could remotely enable deep logging and subsequently retrieve sensitive device passwords from the logs after an authorized user authenticates at the device. This exposure allows for the lateral movement or unauthorized configuration of the physical print hardware.	N/A	More Details

CVE-2026-40110	Jupyter Server is the backend for Jupyter web applications. In versions 2.17.0 and earlier, the Origin header validation uses Python's re.match() to check incoming origins against the allow_origin_pat configuration value. Because re.match() only anchors at the start of the string and does not require a full match, a pattern intended to match only a trusted domain (e.g., trusted.example.com) will also match any origin that begins with that domain followed by additional characters (e.g., trusted.example.com.evil.com). An attacker who controls such a domain can bypass the CORS origin restriction and make cross-origin requests to the Jupyter Server API from an untrusted site. This issue has been fixed in version 2.18.0.	N/A	More Details
CVE-2026-43060	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_ct: drop pending enqueued packets on removal Packets sitting in nfqueue might hold a reference to: - templates that specify the conntrack zone, because a percpu area is used and module removal is possible. - conntrack timeout policies and helper, where object removal leave a stale reference. Since these objects can just go away, drop enqueued packets to avoid stale reference to them. If there is a need for finer grain removal, this logic can be revisited to make selective packet drop upon dependencies.	N/A	More Details
CVE-2026-40075	OpenMRS Core is an open source electronic medical record system platform. In versions 2.7.8 and earlier and versions 2.8.0 through 2.8.5, the `/openmrs/moduleResources/{moduleid}` endpoint is vulnerable to a path traversal attack. The ModuleResourcesServlet constructs a filesystem path from user-controlled input without performing path boundary validation — the getFile() method concatenates the user-supplied path into an absolute filesystem path without calling normalize() or checking that the result stays within the allowed module resources directory. Because this endpoint serves static resources required for rendering the login page, it is not protected by authentication filters, allowing unauthenticated exploitation. An attacker can traverse directories and read arbitrary files from the server filesystem, including /etc/passwd and application configuration files containing database credentials. Successful exploitation requires the target deployment to run on Apache Tomcat versions prior to 8.5.31, where the ..; path parameter bypass is not mitigated by the container. Deployments on Tomcat 8.5.31 or later and Tomcat 9.0.10 or later are protected at the container level, though the underlying code defect remains. This issue has been fixed in versions after 2.7.8 (within the 2.7.x branch) and in version 2.8.6 and later.	N/A	More Details
CVE-2026-6418	An issue was discovered in the Shared Account Synchronization component of PaperCut MF (version 25.0.4). The application allows administrative users to configure a source path for account data synchronization. Due to a lack of proper path validation and sanitization, an authenticated user with administrative privileges can specify arbitrary file paths on the local file system. This allows for the enumeration of directory structures and the unauthorized reading of sensitive text-based configuration or system files. When the synchronization process is triggered, the application attempts to parse the contents of the specified file, subsequently exposing the data within the application's account management interface. This vulnerability could lead to the disclosure of sensitive system information or configuration details, depending on the permissions of the service account under which the application is running.	N/A	More Details
CVE-2026-39402	lxc is a Linux container runtime. In the setuid helper lxc-user-nic, the delete path contains a logic flaw in the find_line() function that allows an unprivileged user to delete OVS-attached network interfaces belonging to other users. When lxc-user-nic delete scans its NIC database to authorize a deletion request, the interface name comparison can set the authorization flag based on a name match alone, even when the ownership, type, and link fields in that database entry belong to a different user. The vulnerable check sits after the goto next label handling, meaning it is reachable on lines where earlier ownership checks failed or were skipped. Because nothing downstream of this authorization signal re-verifies that the matched database line actually belongs to the caller, an unprivileged attacker with a valid lxc-usernet policy entry can trigger deletion of another user's OVS port on the same bridge. This is limited to multi-tenant environments using lxc-user-nic with OpenVSwitch bridges. The impact is denial of service - one tenant can repeatedly disconnect networking from containers run by another tenant on shared infrastructure. This is patched in version 7.0.0.	N/A	More Details
CVE-2026-35579	CoreDNS is a DNS server written in Go. In versions prior to 1.14.3, the gRPC, QUIC, DoH, and DoH3 transport implementations incorrectly handle TSIG authentication. For gRPC and QUIC, the server checks whether the TSIG key name exists in the configuration but never calls dns.TsigVerify() to validate the HMAC. If the key name matches a configured key, the tsigStatus field remains nil and the tsig plugin treats the request as successfully authenticated regardless of the MAC value. For DoH and DoH3, the issue is more severe: the DoHWriter.TsigStatus() method unconditionally returns nil, and the server never inspects the TSIG record at all. Any request containing a TSIG record is treated as authenticated over DoH and DoH3, even if the key name is invalid and the MAC is arbitrary. An unauthenticated network attacker can exploit this to bypass TSIG-protected functionality such as AXFR/IXFR zone transfers, dynamic DNS updates, or other TSIG-gated plugin behavior. The DoH and DoH3 variants have a lower exploitation bar because the attacker does not need to know a valid TSIG key name. This issue has been fixed in version 1.14.3. As a workaround, disable gRPC, QUIC, DoH, and DoH3 listeners where TSIG authentication is required, or restrict network-level access to affected transport ports to trusted sources only.	N/A	More Details
CVE-2026-32689	Allocation of Resources Without Limits or Throttling vulnerability in phoenixframework phoenix allows a denial of service via the long-poll transport's NDJSON body handling. In 'Elixir.Phoenix.Transports.LongPoll':publish/4, when a POST request is received with Content-Type: application/x-ndjson, the request body is split on newline characters using String.split/2 with no limit on the number of resulting segments. An attacker can send a body consisting entirely of newline bytes, causing a 1:1 amplification into a list of empty binaries — a 1 MB body produces approximately one million list elements, an 8 MB body approximately 8.4 million. Each element is then walked by Enum.map, materializing another list of the same size. This exhausts BEAM memory and schedulers, crashing the node and terminating all active sessions. A session token required to reach the vulnerable endpoint is freely obtainable by any client via an unauthenticated GET request to the same URL with a matching Origin header, making this attack effectively unauthenticated. This issue affects phoenix: from 1.7.0 before 1.7.22 and 1.8.6.	N/A	More Details
CVE-2026-35527	Incus is an open source container and virtual machine manager. In versions prior to 7.0.0, the image import flow issues an outbound HEAD request to a user-supplied URL before validating the request against project restrictions such as restricted.images.servers. The imgPostURLInfo function constructs and sends a HEAD request directly from the attacker-supplied source URL to resolve image metadata, and this network interaction occurs before the flow reaches the point where the import would be rejected by policy. Although the actual image download is blocked by the project restriction, an authenticated user can coerce the daemon into making blind HEAD requests to arbitrary destinations. These requests include server metadata in custom headers (Incus-Server-Architectures, Incus-Server-Version), which discloses information about the host environment to the attacker-controlled endpoint. This blind SSRF primitive can be used to probe internal services, unroutable address space, or cloud metadata endpoints reachable from the host. This vulnerability pattern is similar to CVE-2026-24767. This issue has been fixed in version 7.0.0.	N/A	More Details
CVE-2026-43067	In the Linux kernel, the following vulnerability has been resolved: ext4: handle wraparound when searching for blocks for indirect mapped blocks Commit 4865c768b563 ("ext4: always allocate blocks only from groups inode can use") restricts what blocks will be allocated for indirect block based files to block numbers that fit within 32-bit block numbers. However, when using a review bot running on the latest Gemini LLM to check this commit when backporting into an LTS based kernel, it raised this concern: If ac->ac_g_ex.fe_group is >= ngroups (for instance, if the goal group was populated via stream allocation from s_mb_last_groups), then start will be >= ngroups. Does this allow allocating blocks beyond the 32-bit limit for indirect block mapped files? The commit message mentions that ext4_mb_scan_groups_linear() takes care to not select unsupported groups. However, its loop uses group = *start, and the very first iteration will call ext4_mb_scan_group() with this unsupported group because next_linear_group() is only	N/A	More Details

	called at the end of the iteration. After reviewing the code paths involved and considering the LLM review, I determined that this can happen when there is a file system where some files/directories are extent-mapped and others are indirect-block mapped. To address this, add a safety clamp in ext4_mb_scan_groups().		
CVE-2026-39849	Pi-hole FTL is the core engine of the Pi-hole network-level advertisement and tracker blocker. In versions before 6.6.1, the `dns.interface` configuration field in Pi-hole FTL accepted newline characters without validation, allowing an attacker to inject arbitrary directives into the generated dnsmasq configuration file. On installations with no admin password set (the default for many deployments), the configuration API is fully accessible without credentials, allowing a network-adjacent attacker to inject the payload, enable the built-in DHCP server, and achieve arbitrary command execution on the host the next time any device on the network requests a DHCP lease. The injected value is persisted to /etc/pihole/pihole.toml and survives restarts. The strncpy in the code path limits the total interface field to 31 bytes, but payloads such as wlan0\ndhcp-script=/tmp/p fit within this constraint. The dnsmasq config validation introduced in FTL 6.6 only checks syntactic validity, so valid directives injected via newline pass validation successfully. This issue has been fixed in version 6.6.1.	N/A	More Details
CVE-2026-43066	In the Linux kernel, the following vulnerability has been resolved: ext4: fix iloc.bh leak in ext4_fc_replay_inode() error paths During code review, Joseph found that ext4_fc_replay_inode() calls ext4_get_fc_inode_loc() to get the inode location, which holds a reference to iloc.bh that must be released via brelse(). However, several error paths jump to the 'out' label without releasing iloc.bh: - ext4_handle_dirty_metadata() failure - sync_dirty_buffer() failure - ext4_mark_inode_used() failure - ext4_iget() failure Fix this by introducing an 'out_brelse' label placed just before the existing 'out' label to ensure iloc.bh is always released. Additionally, make ext4_fc_replay_inode() propagate errors properly instead of always returning 0.	N/A	More Details
CVE-2026-35192	An issue was discovered in 6.0 before 6.0.5 and 5.2 before 5.2.14. Response headers do not vary on cookies if a session is not modified, but `SESSION_SAVE_EVERY_REQUEST` is `True`. A remote attacker can steal a user's session after that user visits a cached public page. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Cantina for reporting this issue.	N/A	More Details
CVE-2026-31196	The traceroute diagnostic handler in /bin/httpd_clientside for ALTICE LABS / SFR France GR140DG and GR140IG fibre CPE/Router/Gateway, inserts unsanitized user input into a system() call, allowing authenticated remote attackers to execute arbitrary commands as root via crafted destAddr parameters using shell command substitution.	N/A	More Details
CVE-2026-31195	The ping diagnostic handler in /bin/httpd_clientside for ALTICE LABS / SFR France GR140DG and GR140IG fibre CPE/Router/Gateway, inserts unsanitized user input into a system() call, allowing authenticated remote attackers to execute arbitrary commands as root via crafted destAddr parameters using shell command substitution.	N/A	More Details
CVE-2026-43068	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid allocate block from corrupted group in ext4_mb_find_by_goal() There's issue as follows: ... EXT4-fs (mmcblk0p1): Delayed block allocation failed for inode 206 at logical offset 0 with max blocks 1 with error 117 EXT4-fs (mmcblk0p1): This should not happen!! Data will be lost EXT4-fs (mmcblk0p1): Delayed block allocation failed for inode 206 at logical offset 0 with max blocks 1 with error 117 EXT4-fs (mmcblk0p1): This should not happen!! Data will be lost EXT4-fs (mmcblk0p1): Delayed block allocation failed for inode 206 at logical offset 0 with max blocks 1 with error 117 EXT4-fs (mmcblk0p1): This should not happen!! Data will be lost EXT4-fs (mmcblk0p1): Delayed block allocation failed for inode 206 at logical offset 0 with max blocks 1 with error 117 EXT4-fs (mmcblk0p1): This should not happen!! Data will be lost EXT4-fs (mmcblk0p1): Delayed block allocation failed for inode 2243 at logical offset 0 with max blocks 1 with error 117 EXT4-fs (mmcblk0p1): This should not happen!! Data will be lost EXT4-fs (mmcblk0p1): Delayed block allocation failed for inode 2239 at logical offset 0 with max blocks 1 with error 117 EXT4-fs (mmcblk0p1): This should not happen!! Data will be lost EXT4-fs (mmcblk0p1): error count since last fsck: 1 EXT4-fs (mmcblk0p1): initial error at time 1765597433: ext4_mb_generate_buddy:760 EXT4-fs (mmcblk0p1): last error at time 1765597433: ext4_mb_generate_buddy:760 ... According to the log analysis, blocks are always requested from the corrupted block group. This may happen as follows: ext4_mb_find_by_goal ext4_mb_load_buddy ext4_mb_load_buddy_gfp ext4_mb_init_cache ext4_read_block_bitmap_nowait ext4_wait_block_bitmap ext4_validate_block_bitmap if (!grp || EXT4_MB_GRP_BBITMAP_CORRUPT(grp)) return -EFSCORRUPTED; // There's no logs. if (err) return err; // Will return error ext4_lock_group(ac->ac_sb, group); if (unlikely(EXT4_MB_GRP_BBITMAP_CORRUPT(e4b->bd_info))) // Unreachable goto out; After commit 9008a58e5dce ("ext4: make the bitmap read routines return real error codes") merged, Commit 163a203ddb36 ("ext4: mark block group as corrupt on block bitmap error") is no real solution for allocating blocks from corrupted block groups. This is because if 'EXT4_MB_GRP_BBITMAP_CORRUPT(e4b->bd_info)' is true, then 'ext4_mb_load_buddy()' may return an error. This means that the block allocation will fail. Therefore, check block group if corrupted when ext4_mb_load_buddy() returns error.	N/A	More Details
CVE-2025-66369	An issue was discovered in MM in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. Incorrect handling of 5G NR NAS registration accept messages leads to a Denial of Service.	N/A	More Details
CVE-2026-39103	Buffer Overflow vulnerability in GPAC before commit v391dc7f4d234988ea0bc3cc294eb725eddf8f702 allows an attacker to cause a denial of service via the src/scenegraph/svg_attributes.c, svg_parse_strings(), gf_svg_parse_attribute()	N/A	More Details
CVE-2026-43059	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix list corruption and UAF in command complete handlers Commit 302a1f674c00 ("Bluetooth: MGMT: Fix possible UAFs") introduced mgmt_pending_valid(), which not only validates the pending command but also unlinks it from the pending list if it is valid. This change in semantics requires updates to several completion handlers to avoid list corruption and memory safety issues. This patch addresses two left-over issues from the aforementioned rework: 1. In mgmt_add_adv_patterns_monitor_complete(), mgmt_pending_remove() is replaced with mgmt_pending_free() in the success path. Since mgmt_pending_valid() already unlinks the command at the beginning of the function, calling mgmt_pending_remove() leads to a double list_del() and subsequent list corruption/kernel panic. 2. In set_mesh_complete(), the use of mgmt_pending_foreach() in the error path is removed. Since the current command is already unlinked by mgmt_pending_valid(), this foreach loop would incorrectly target other pending mesh commands, potentially freeing them while they are still being processed concurrently (leading to UAFs). The redundant mgmt_cmd_status() is also simplified to use cmd->opcode directly.	N/A	More Details
CVE-2026-39383	Gotenberg is an API-based document conversion tool. In version 8.29.1, an unauthenticated attacker with network access can force the server to make outbound HTTP POST requests to arbitrary internal or external destinations by supplying a crafted URL in the Gotenberg-Webhook-Url request header. The FilterDeadline function in filter.go is intended to gate outbound URLs, but when both the allow-list and deny-list are empty (the default configuration), it returns nil unconditionally and permits any URL. This is a blind SSRF: Gotenberg POSTs the converted document to the webhook URL and only checks whether the response status code is an error, but never returns the target's response body to the attacker. An attacker can use this to probe internal network infrastructure by observing whether the error callback is invoked, force POST requests against internal services that perform side effects, and confirm reachability of cloud metadata endpoints. The retryable HTTP client issues up to 4 automatic retries per request, amplifying each	N/A	More Details

	probe. This issue has been fixed in version 8.31.0. As a workaround, configure the GOTENBERG_API_WEBHOOK_ALLOW_LIST environment variable to restrict webhook URLs to known receivers, or set GOTENBERG_API_WEBHOOK_DENY_LIST to block RFC-1918 and link-local address ranges.		
CVE-2026-43065	In the Linux kernel, the following vulnerability has been resolved: ext4: always drain queued discard work in ext4_mb_release() While reviewing recent ext4 patch[1], Sashiko raised the following concern[2]: > If the filesystem is initially mounted with the discard option, > deleting files will populate sbi->s_discard_list and queue > s_discard_work. If it is then remounted with nodiscard, the > EXT4_MOUNT_DISCARD flag is cleared, but the pending s_discard_work is > neither cancelled nor flushed. [1] https://lore.kernel.org/r/20260319094545.19291-1-qiang.zhang@linux.dev/ [2] https://sashiko.dev/#/patchset/20260319094545.19291-1-qiang.zhang%40linux.dev The concern was valid, but it had nothing to do with the patch[1]. One of the problems with Sashiko in its current (early) form is that it will detect pre-existing issues and report it as a problem with the patch that it is reviewing. In practice, it would be hard to hit deliberately (unless you are a malicious syzkaller fuzzer), since it would involve mounting the file system with -o discard, and then deleting a large number of files, remounting the file system with -o nodiscard, and then immediately unmounting the file system before the queued discard work has a change to drain on its own. Fix it because it's a real bug, and to avoid Sashiko from raising this concern when analyzing future patches to mballoc.c.	N/A	More Details
CVE-2026-39852	Quarkus is a Java framework for building cloud-native applications. In versions prior to 3.20.6.1, 3.27.3.1, 3.33.1.1, 3.35.1.1, 3.34.7, and 3.35.2, a path normalization inconsistency between the security layer and the routing layer allows unauthenticated or lower-privileged users to bypass HTTP path-based authorization policies. Quarkus's security layer performs authorization checks on the raw URL path which preserves matrix parameters (semicolons), while RESTEasy Reactive's routing layer strips matrix parameters before matching endpoints. An attacker can append a semicolon and arbitrary text to a request URL (e.g., /api/admin;anything) to bypass policies protecting /api/admin while still routing to the protected endpoint. This issue has been fixed in versions 3.20.6.1, 3.27.3.1, 3.33.1.1, 3.35.1.1, 3.34.7, and 3.35.2.	N/A	More Details
CVE-2025-61669	Jupyter Server is the backend for Jupyter web applications. In jupyter_server versions through 2.17.0, the next query parameter in the login flow is insufficiently validated in `LoginFormHandler._redirect_safe()`, which allows redirects to arbitrary external domains via values such as `///example.com`. An attacker can use a crafted login URL to redirect users to a malicious site and facilitate phishing attacks. This issue is fixed in version 2.18.0.	N/A	More Details
CVE-2026-43061	In the Linux kernel, the following vulnerability has been resolved: serial: 8250: Fix TX deadlock when using DMA `dmaengine_terminate_async` does not guarantee that the `__dma_tx_complete` callback will run. The callback is currently the only place where `dma->tx_running` gets cleared. If the transaction is canceled and the callback never runs, then `dma->tx_running` will never get cleared and we will never schedule new TX DMA transactions again. This change makes it so we clear `dma->tx_running` after we terminate the DMA transaction. This is "safe" because `serial8250_tx_dma_flush` is holding the UART port lock. The first thing the callback does is also grab the UART port lock, so access to `dma->tx_running` is serialized.	N/A	More Details
CVE-2026-40068	In versions 2.1.63 through 2.1.83 of Claude Code, the folder trust determination logic used the git worktree commondir file without validating its contents. An attacker could craft a malicious repository with a commondir file pointing to a path the victim had previously trusted, causing Claude Code to bypass its trust confirmation dialog and immediately execute hooks defined in `.claude/settings.json`. Exploitation requires the victim to clone the malicious repository and run Claude Code within it, and the attacker must know or guess a path the victim had already trusted. This issue has been fixed in version 2.1.84.	N/A	More Details
CVE-2026-28780	Heap-based Buffer Overflow vulnerability in mod_proxy_ajp of Apache HTTP Server. If mod_proxy_ajp connects to a malicious AJP server this AJP server can send a malicious AJP message back to mod_proxy_ajp and cause it to write 4 attacker controlled bytes after the end of a heap based buffer. This issue affects Apache HTTP Server: through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	N/A	More Details
CVE-2026-40329	Masa CMS is an open source content management system. In versions 7.5.2 and earlier, a SQL injection vulnerability exists in the beanFeed.cfc component within the getQuery function's processing of the sortBy parameter. The application fails to properly sanitize or parameterize this input before incorporating it into dynamic SQL statements. An unauthenticated remote attacker can execute arbitrary SQL commands against the database, potentially gaining access to sensitive data, modifying or deleting records, or escalating privileges to administrative control. This issue has been fixed in versions 7.2.10, 7.3.15, 7.4.10, and 7.5.3. As a workaround, configure WAF rules to block malicious SQL patterns in the sortBy parameter sent to beanFeed.cfc.	N/A	More Details
CVE-2026-34084	PhpSpreadsheet is a library for reading and writing spreadsheet files. In versions 1.30.2 and earlier, 2.0.0 through 2.1.14, 2.2.0 through 2.4.3, 3.3.0 through 3.10.3, and 4.0.0 through 5.5.0, when the filename argument to IOFactory::load() is user-controlled, an attacker can supply a PHP stream wrapper path (such as phar://, ftp://, or ssh2.sftp://) that passes the is_file() check in File::assertFile(). The phar:// wrapper triggers deserialization of the PHAR metadata, which can lead to remote code execution if a suitable gadget chain is available in the application. The ftp:// and ssh2.sftp:// wrappers can be used for server-side request forgery. This issue has been fixed in versions 1.30.3, 2.1.15, 2.4.4, 3.10.4, and 5.6.0.	N/A	More Details
CVE-2026-43069	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_ll: Fix firmware leak on error path Smatch reports: drivers/bluetooth/hci_ll.c:587 download_firmware() warn: 'fw' from request_firmware() not released on lines: 544. In download_firmware(), if request_firmware() succeeds but the returned firmware content is invalid (no data or zero size), the function returns without releasing the firmware, resulting in a resource leak. Fix this by calling release_firmware() before returning when request_firmware() succeeded but the firmware content is invalid.	N/A	More Details
CVE-2026-23479	Redis is an in-memory data structure store. In redis-server from 7.2.0 until 8.6.3, the unblock client flow does not handle an error return from `processCommandAndResetClient` when re-executing a blocked command. If a blocked client is evicted during this flow, an authenticated attacker can trigger a use-after-free that may lead to remote code execution. This has been patched in version 8.6.3.	N/A	More Details
CVE-2026-32699	FacturaScripts is an open source accounting and invoicing software. In versions 2025.92 and earlier, the application fails to validate the nick parameter during a POST request to the EditUser controller. Although the user interface prevents editing this field, a user can bypass this restriction by intercepting the request and modifying the nick form-data parameter to rename any account, including the administrator account. This leads to unauthorized modification of a field intended to be immutable.	N/A	More Details
CVE-2026-32603	Sandboxie is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, a local denial of service vulnerability exists in the Sandboxie kernel driver. An unprivileged process running inside a Standard Sandbox can send a malformed IOCTL to the \Device\SandboxieDriverApi driver, triggering an immediate kernel crash (BSOD). The vulnerability affects the Standard Sandbox configuration both with and without dropped administrator privileges, but does not affect the Security Hardened Sandbox configuration. This issue has been fixed in version 1.17.3. Users who cannot update can use the Security Hardened Sandbox configuration as a workaround.	N/A	More Details

CVE-2026-42515	This vulnerability exists in e-Sushrut due to improper access control in resource access validation. An authenticated attacker could exploit this vulnerability by manipulating parameter in the API request URL to gain unauthorized access to sensitive information of patients on the targeted system.	N/A	More Details
CVE-2026-42516	This vulnerability exists in e-Sushrut due to improper authorization checks during resource access. An authenticated attacker could exploit this vulnerability by manipulating encoded parameters in the request URL to gain unauthorized access to patient accounts on the targeted system.	N/A	More Details
CVE-2026-34408	An issue was discovered in Gambio 4.9.2.0 (patched in 2024-02 v1.0.0 for GX4 v4.0.0.0 to v4.9.2.0). The password reset function can be bypassed to set arbitrary passwords for arbitrary accounts if the ID is known.	N/A	More Details
CVE-2026-42517	This vulnerability exists in e-Sushrut due to the use of reversible Base64 encoding for protecting sensitive data. An authenticated attacker could exploit this vulnerability by decoding and manipulating Base64-encoded parameters in the request URL to gain unauthorized access to sensitive information on the targeted system.	N/A	More Details
CVE-2026-42518	This vulnerability exists in e-Sushrut due to disclosure of sensitive information and hardcoded AES encryption keys in client-side JavaScript. An unauthenticated remote attacker could exploit this vulnerability by accessing the client-side code to extract sensitive information and cryptographic keys. Successful exploitation of this vulnerability could lead to exposure of sensitive data and compromise of cryptographic protections on the targeted system.	N/A	More Details
CVE-2026-7865	A hidden console command is vulnerable to command injection flaw when control characters are passed to its second argument. A third party researcher Eugene Lim had discovered vulnerability in the way console command passes to a popen function call. Attackers with authenticated access to SSH console of Crestron devices may use to run underlying OS commands.	N/A	More Details
CVE-2026-31893	Tunnelblick is an open source graphic user interface for OpenVPN on macOS. In versions 3.3beta26 through 9.0beta01, any local user can read arbitrary root-owned files by exploiting a symlink following vulnerability in tunnelblick-helper, reachable through the world-accessible tunnelblickd Unix socket. The socket is configured with mode 0666, allowing any local user to connect. No authorization check is performed on the connecting client. The tunnelblick-helper process constructs a path to config.ovpn inside a user-controlled .tblk directory and reads it as root without symlink validation. An attacker can create a .tblk configuration with a symlinked config.ovpn pointing to any file and request tunnelblickd to read it. This issue has been fixed in versions 9.0beta02.	N/A	More Details
CVE-2024-52911	Bitcoin Core through 28.x has a security issue, the details of which are not disclosed. The earliest affected version is 0.14.	N/A	More Details
CVE-2026-3325	SQL injection (SQLi) in MegaCMS v12.0.0, specifically in the “id_territorio” parameter of the “/web_comunications/cms/get_provincias” endpoint. The vulnerability arises from inadequate validation and sanitisation of user input. Specifically, via a POST request, the “id_territorio” parameter, used immediately after the registration form is submitted, could be manipulated by an unauthenticated attacker to execute arbitrary SQL queries.	N/A	More Details
CVE-2026-38428	Kestra v1.3.3 and before is vulnerable to SQL Injection. The vulnerability occurs because user-controlled input from a GET parameter is directly concatenated into an SQL query without proper sanitization or parameterization. As a result, attackers can inject arbitrary SQL expressions into the database query.	N/A	More Details
CVE-2026-41952	Local privilege escalation due to improper input validation. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.93212, Acronis Cyber Protect Cloud Agent (Windows) before build 42183.	N/A	More Details
CVE-2026-23631	Redis is an in-memory data structure store. In all versions of redis-server with Lua scripting, an authenticated attacker can exploit the master-replica synchronization mechanism to trigger a use-after-free on replicas where replica-read-only is disabled or can be disabled, which may lead to remote code execution. A workaround is to prevent users from executing Lua scripts or avoid using replicas where replica-read-only is disabled. This is patched in version 8.6.3.	N/A	More Details
CVE-2026-25243	Redis is an in-memory data structure store. In versions of redis-server up to 8.6.3, the RESTORE command does not properly validate serialized values. An authenticated attacker with permission to execute RESTORE can supply a crafted serialized payload that triggers invalid memory access and may lead to remote code execution. A workaround is to restrict access to the RESTORE command with ACL rules. This is patched in version 8.6.3.	N/A	More Details
CVE-2026-25588	RedisTimeSeries is a time-series module for Redis. In all versions before 1.12.14 of RedisTimeSeries, the module does not properly validate serialized values processed through the Redis RESTORE command. An authenticated attacker with permission to execute RESTORE on a server with the RedisTimeSeries module loaded can supply a crafted serialized payload that triggers invalid memory access and may lead to remote code execution. A workaround is to restrict access to the RESTORE command with ACL rules. This has been patched in version 1.12.14.	N/A	More Details
CVE-2026-25589	RedisBloom is a probabilistic data structures module for Redis. In all versions of RedisBloom before 2.8.20, the module does not properly validate serialized values processed through the Redis RESTORE command. An authenticated attacker with permission to execute RESTORE on a server with the RedisBloom module loaded can supply a crafted serialized payload that triggers invalid memory access and may lead to remote code execution. A workaround is to restrict access to the RESTORE command with ACL rules. This issue is fixed in version 2.8.20.	N/A	More Details
CVE-2026-38429	OpenCMS v20 and before is vulnerable to XML External Entity (XXE) in the Admin Import DB feature due to insecure XML parsing of user supplied .zip files containing a manifest.xml.	N/A	More Details
CVE-2026-31835	Vaultwarden is a Bitwarden-compatible server written in Rust. In versions 1.35.4 and earlier, the WebAuthn authentication flow in `validate_webauthn_login()` updates persistent credential metadata (1backup_eligible1 and 1backup_state flags1) based on unverified `authenticatorData` before signature validation is performed. An attacker who knows a user's password but cannot produce a valid WebAuthn signature can permanently modify the stored backup flags for that user's credential. If signature verification fails, the database update is not rolled back. This can result in a persistent denial of service of WebAuthn two-factor authentication for affected credentials. This issue has been fixed in version 1.35.5.	N/A	More Details
CVE-2026-	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. Libmodsecurity is one component of the ModSecurity v3 project. A segmentation fault occurs when a rule using the t:hexDecode transformation inspects a query string parameter containing a single character. An attacker can exploit this to crash worker processes, causing a denial of	N/A	More

30923	service. Service resumes once the attack stops as worker processes recover from the segfault. All versions before 3.0.15 of libModSecurity3 are affected. This has been patched in version 3.0.15.		Details
CVE-2026-42513	This vulnerability exists in e-Sushrut due to improper authentication logic that relies on client-side response parameters to determine authentication status. A remote attacker could exploit this vulnerability by intercepting and modifying the server response. Successful exploitation of this vulnerability could allow the attacker to bypass authentication and gain unauthorized access to user accounts on the targeted system.	N/A	More Details
CVE-2026-38431	ERPNext v15.103.1 and before is vulnerable to Server-Side Template Injection (SSTI). An attacker with permission to create or edit email templates can inject template expressions that are executed on the server when the template is rendered.	N/A	More Details
CVE-2026-38432	ERPNext v15.103.1 and before is vulnerable to Cross Site Scripting (XSS) in the Email Template engine. An attacker with permission to create or edit email templates can inject malicious JavaScript code that are executed on the victim's browser when the template is applied.	N/A	More Details
CVE-2026-43063	In the Linux kernel, the following vulnerability has been resolved: xfs: don't irele after failing to iget in xfs_attri_recover_work xlog_recovery_iget* never set @ip to a valid pointer if they return an error, so this irele will walk off a dangling pointer. Fix that.	N/A	More Details
CVE-2026-32934	CoreDNS is a DNS server that chains plugins. In versions prior to 1.14.3, the DNS-over-QUIC (DoQ) server can be driven into unbounded goroutine and memory growth by a remote client that opens many QUIC streams and sends only 1 byte per stream. When the worker pool is full, CoreDNS still spawns a goroutine per accepted stream to wait for a worker token. Additionally, active workers block indefinitely in io.ReadFull() with no per-stream read deadline, allowing an attacker to pin all workers by sending a single byte so the read blocks waiting for the second byte of the DoQ length prefix. This enables an unauthenticated remote attacker to cause memory exhaustion and OOM-kill. This issue has been fixed in version 1.14.3. No known workarounds exist.	N/A	More Details
CVE-2026-42248	Ollama for Windows does not perform integrity or authenticity verification of downloaded update executables. Unlike other platforms, the Windows implementation of the update verification routine unconditionally returns success so no digital signature or trust validation is performed before staging or executing update payloads, enabling attacker-supplied executables to be accepted and later executed by the application. Critically, Ollama for Windows performs silent automatic updates, so the malicious payload may be installed automatically without user awareness. Maintainers of this project were notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Versions from 0.12.10 to 0.17.5 were tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	N/A	More Details
CVE-2026-42249	Ollama for Windows contains a Remote Code Execution vulnerability in its update mechanism due to improper handling of attacker-controlled HTTP response headers. When downloading updates, the application constructs local file paths using values derived from HTTP headers without validation. These values are passed directly to filepath.Join, allowing path traversal sequences (../) to be resolved and enabling files to be written outside the intended update staging directory. An attacker who can influence update responses can exploit this flaw to write arbitrary executables to attacker-chosen locations accessible to the current user, including the Windows Startup directory. This allows execution of arbitrary executables. Critically, when chained with CVE-2026-42248 (Missing Signature Verification for Updates), an attacker can deliver malicious payloads that are written to sensitive locations and executed automatically. Because Ollama for Windows performs silent automatic updates and executes staged binaries without user interaction, this results in automatic and persistent code execution without user awareness. Maintainers of this project were notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Versions from 0.12.10 to 0.17.5 were tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	N/A	More Details
CVE-2026-32936	CoreDNS is a DNS server that chains plugins. In versions prior to 1.14.3, the DNS-over-HTTPS (DoH) GET path accepts oversized dns= query parameter values and performs URL query parsing, base64 decoding, and DNS message unpacking before rejecting the request. Unlike the POST path, which applies a bounded read via http.MaxBytesReader limited to 65536 bytes, the GET path has no equivalent size validation before expensive processing. A remote, unauthenticated attacker can repeatedly send oversized DoH GET requests to force high CPU usage, large transient memory allocations, and elevated garbage-collection pressure, leading to denial of service. This issue has been fixed in version 1.14.3.	N/A	More Details
CVE-2026-41220	Local privilege escalation due to improper input validation. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.93212, Acronis Cyber Protect Cloud Agent (Windows) before build 42183.	N/A	More Details
CVE-2026-25852	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.93212.	N/A	More Details
CVE-2026-40280	Gotenberg is an API-based document conversion tool. In versions 8.30.1 and earlier, the default private-IP deny-lists for the --webhook-deny-list and --api-download-from-deny-list flags use a case-sensitive regular expression (^https?://) to match URL schemes. Because Go's net/url.Parse() normalizes the scheme to lowercase before establishing the outbound TCP connection, an attacker can bypass the deny-list by simply capitalizing part of the URL scheme (e.g., HTTP://, HTTPS://, or Http://). This allows unauthenticated requests to reach internal network services, including private IP ranges, loopback addresses, and cloud instance metadata endpoints such as HTTP://169.254.169.254/latest/meta-data/. This bypasses the same security control that was patched in CVE-2026-27018. This issue has been fixed in version 8.31.0.	N/A	More Details
CVE-2026-38947	FluentCMS 1.2.3 is vulnerable to Cross Site Scripting (XSS) in TextHTML plugin.	N/A	More Details
CVE-2026-35453	PhpSpreadsheet is a library for reading and writing spreadsheet files. In versions 1.30.3 and earlier, 2.0.0 through 2.1.15, 2.2.0 through 2.4.4, 3.3.0 through 3.10.4, and 4.0.0 through 5.6.0, the HTML Writer skips htmlspecialchars() output escaping when a cell uses a custom number format containing the @ text placeholder with additional literal text (e.g., @ "items"). The escaping is only applied when the formatted output strictly equals the original cell value. When the format code contains @ with quoted literal text, the formatter substitutes the raw cell value into the format string and returns early without invoking the escaping callback. An attacker who can control cell content in a spreadsheet processed by the HTML Writer can inject arbitrary HTML and JavaScript into the generated output. This issue has been fixed in versions 1.30.4, 2.1.16, 2.4.5, 3.10.5, and 5.7.0.	N/A	More Details
	Jupyter Server is the backend for Jupyter web applications. In versions 2.17.0 and earlier, a path traversal vulnerability in the REST API allows an authenticated user to escape the configured root_dir and access sibling directories whose names begin with the same		

CVE-2026-35397	prefix as the root_dir. For example, with a root_dir named "test", the API permits access to a sibling directory named "testtest" through a crafted request to the /api/contents endpoint using encoded path components. An attacker can read, write, and delete files in affected sibling directories. Multi-tenant deployments using predictable naming schemes are particularly at risk, as a user with a directory named "user1" could access directories for user10 through user19 and beyond. A user who can choose a single-character folder name could gain access to a significant number of sibling directories. Version 2.18.0 contains a fix. As a workaround, ensure folder names do not share a common prefix with any sibling directory.	N/A	More Details
CVE-2026-34596	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, a Time-of-Check-to-Time-of-Use (TOCTOU) race condition exists during addon installation. When a user installs an addon through the SandMan interface, UpdUtil.exe is spawned as SYSTEM by SbieSvc but stages files in the user-writable %TEMP%\sandboxie-updater directory. After UpdUtil verifies file hashes against the signed addon manifest, install.bat extracts files.cab and executes config.exe from its contents. Between hash verification and extraction, an unprivileged user can replace files.cab with a crafted cabinet containing a malicious executable, which is then run as SYSTEM. No UAC prompt is required. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-34527	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, SbieIniServer::HashPassword converts a SHA-1 digest to hexadecimal incorrectly. The high nibble of each byte is shifted right by 8 instead of 4, which always produces zero for an 8-bit value. As a result, the stored EditPassword hash only preserves the low nibble of each digest byte, reducing the effective entropy from 160 bits to 80 bits. This is layered on top of an unsalted SHA-1 scheme. The reduced entropy makes leaked or backed-up password hashes materially easier to brute-force. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-43070	In the Linux kernel, the following vulnerability has been resolved: bpf: Reset register ID for BPF_END value tracking When a register undergoes a BPF_END (byte swap) operation, its scalar value is mutated in-place. If this register previously shared a scalar ID with another register (e.g., after an `r1 = r0` assignment), this tie must be broken. Currently, the verifier misses resetting `dst_reg->id` to 0 for BPF_END. Consequently, if a conditional jump checks the swapped register, the verifier incorrectly propagates the learned bounds to the linked register, leading to false confidence in the linked register's value and potentially allowing out-of-bounds memory accesses. Fix this by explicitly resetting `dst_reg->id` to 0 in the BPF_END case to break the scalar tie, similar to how BPF_NEG handles it via `__mark_reg_known`.	N/A	More Details
CVE-2026-34464	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, NamedPipeServer::OpenHandler copies the server field from NAMED_PIPE_OPEN_REQ into a fixed WCHAR pipename[160] stack buffer using wcscat without verifying null termination. The handler only enforces a minimum packet size, and since the service pipe accepts variable-length messages, a sandboxed caller can fill the server[48] field with non-zero data and append additional controlled wide characters after the structure. wcscat then reads past the fixed field and overflows the stack buffer in the SYSTEM service. This message is restricted to sandboxed callers, making it a sandbox escape vector. This can lead to a crash of the SbieSvc service or potential code execution as SYSTEM. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-34462	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, several ProcessServer handlers (KillAllHandler, SuspendAllHandler, and RunSandboxedHandler) copy a WCHAR boxname[34] field from request structures into WCHAR[40] stack buffers using wcscpy without verifying null termination. Because the service pipe accepts variable-length packets larger than the request structure, an attacker can fill the boxname field with non-zero data and append additional controlled wide characters after the structure. wcscpy then reads past the fixed field and overflows the destination stack buffer. The service pipe is created with a NULL DACL, allowing any local process to connect, and the unsafe copy occurs before authorization checks. This can lead to a crash of the SbieSvc service or potential code execution as SYSTEM. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-43071	In the Linux kernel, the following vulnerability has been resolved: dcache: Limit the minimal number of bucket to two There is an OOB read problem on dentry_hashtable when user sets 'dhash_entries=1': BUG: unable to handle page fault for address: ffff888b30b774b0 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page Oops: Oops: 0000 [#1] SMP PTI RIP: 0010:__d_lookup+0x56/0x120 Call Trace: d_lookup.cold+0x16/0x5d lookup_dcache+0x27/0xf0 lookup_one_qstr_excl+0x2a/0x180 start_dirop+0x55/0xa0 simple_start_creating+0x8d/0xa0 debugfs_start_creating+0x8c/0x180 debugfs_create_dir+0x1d/0x1c0 pinctrl_init+0x6d/0x140 do_one_initcall+0x6d/0x3d0 kernel_init_freeable+0x39f/0x460 kernel_init+0x2a/0x260 There will be only one bucket in dentry_hashtable when dhash_entries is set as one, and d_hash_shift is calculated as 32 by dcache_init(). Then, following process will access more than one buckets(which memory region is not allocated) in dentry_hashtable: d_lookup b = d_hash(hash) dentry_hashtable + ((u32)hashlen >> d_hash_shift) // The C standard defines the behavior of right shift amounts // exceeding the bit width of the operand as undefined. The // result of '(u32)hashlen >> d_hash_shift' becomes 'hashlen', // so 'b' will point to an unallocated memory region. hlist_bl_for_each_entry_rcu(b) hlist_bl_first_rcu(head) h->first // read OOB! Fix it by limiting the minimal number of dentry_hashtable bucket to two, so that 'd_hash_shift' won't exceeds the bit width of type u32.	N/A	More Details
CVE-2026-43072	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: platform_get_irq_byname() returns an int platform_get_irq_byname() will return a negative value if an error happens, so it should be checked and not just passed directly into devm_request_threaded_irq() hoping all will be ok.	N/A	More Details
CVE-2026-43073	In the Linux kernel, the following vulnerability has been resolved: x86-64: rename misleadingly named '__copy_user_nocache()' function This function was a masterclass in bad naming, for various historical reasons. It claimed to be a non-cached user copy. It is literally _neither_ of those things. It's a specialty memory copy routine that uses non-temporal stores for the destination (but not the source), and that does exception handling for both source and destination accesses. Also note that while it works for unaligned targets, any unaligned parts (whether at beginning or end) will not use non-temporal stores, since only words and quadwords can be non-temporal on x86. The exception handling means that it _can_ be used for user space accesses, but not on its own - it needs all the normal "start user space access" logic around it. But typically the user space access would be the source, not the non-temporal destination. That was the original intention of this, where the destination was some fragile persistent memory target that needed non-temporal stores in order to catch machine check exceptions synchronously and deal with them gracefully. Thus that non-descriptive name: one use case was to copy from user space into a non-cached kernel buffer. However, the existing users are a mix of that intended use-case, and a couple of random drivers that just did this as a performance tweak. Some of those random drivers then actively misused the user copying version (with STAC/CLAC and all) to do kernel copies without ever even caring about the exception handling, _just_ for the non-temporal destination. Rename it as a first small step to actually make it halfway sane, and change the prototype to be more normal: it doesn't take a user pointer unless the caller has done the proper conversion, and the argument size is the full size_t (it still won't actually copy more than 4GB in one go, but there's also no reason to silently truncate the size argument in the caller). Finally, use this now sanely named function in the NTB code, which mis-used a user copy version (with STAC/CLAC and all) of this interface despite it not actually being a user copy at all.	N/A	More Details
CVE-	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, the SbieIniServer RunSbieCtrl handler contains a stack buffer overflow. The MSGID_SBIE_INI_RUN_SBIE_CTRL message is handled before normal		

2026-34461	sandbox and impersonation checks, and for non-sandboxed callers, the handler copies the trailing message payload into a fixed-size WCHAR ctrlCmd[128] stack buffer using memcpy without verifying the length fits within the buffer. The service pipe is created with a NULL DACL, allowing any local interactive process to connect and send an oversized payload to overflow the stack. This can lead to a crash of the SbieSvc service or potential code execution as SYSTEM. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-34459	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, the SbieSvc proxy service's GetRawInputDeviceInfoSlave handler contains two vulnerabilities that can be chained for sandbox escape. First, when a sandboxed process sends an IPC request with cbSize set to 0, up to 32KB of uninitialized stack memory from the service process is returned, leaking return addresses and stack cookies which bypass ASLR and /GS protections. Second, the handler performs a memcpy with an attacker-controlled length without verifying it fits within the 32KB stack buffer, enabling a stack buffer overflow. By chaining the information leak with the overflow, a sandboxed process can execute a ROP chain to achieve SYSTEM privilege escalation, even from a Security Hardened Sandbox. Hardware-enforced shadow stacks (Intel CET) prevent the ROP chain execution but do not mitigate the information leak. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-34458	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. In versions 1.17.2 and earlier, an INI injection vulnerability allows any standard local user to bypass configuration restrictions (EditAdminOnly and ConfigPassword) and inject arbitrary directives into the global Sandboxie.ini configuration file. The background service skips authorization checks for IPC messages targeting sections beginning with UserSettings_, but does not sanitize CRLF characters in either the value parameter (via MSGID_SBIE_INI_ADD_SETTING) or the setting name parameter (via MSGID_SBIE_INI_SET_SETTING). An attacker can inject a new sandbox section header with unrestricted permissions, enabling sandbox escape and SYSTEM privilege escalation. This issue has been fixed in version 1.17.3.	N/A	More Details
CVE-2026-33975	Twenty is an open source CRM built with NestJS (Node.js). In versions 1.18.0 and earlier, the SSRF protection in twenty-server's SecureHttpClientService can be bypassed using IPv4-mapped IPv6 addresses in URL IP literals. Node.js's URL parser normalizes IPv4-mapped IPv6 addresses to compressed hex form (e.g., ::ffff:169.254.169.254 becomes ::ffff:a9fe:a9fe), but the isPrivateIp utility only recognizes the dotted-decimal notation. As a result, the hex form passes the SSRF check unchecked. Additionally, the socket lookup validation event does not fire for IP literal addresses, bypassing the second validation layer. An authenticated user can reach any internal IP, including cloud metadata endpoints, to exfiltrate credentials such as IAM keys.	N/A	More Details
CVE-2026-33489	CoreDNS is a DNS server that chains plugins. In versions prior to 1.14.3, the transfer plugin can select the wrong ACL stanza when both a parent zone and a more-specific subzone are configured. The longestMatch() function in plugin/transfer/transfer.go uses a lexicographic string comparison instead of an actual longest-suffix match to select the winning zone. As a result, a permissive parent-zone transfer rule can override a restrictive subzone rule depending on zone name ordering (e.g., "example.org." > "a.example.org." lexicographically). This allows an unauthorized remote client to perform AXFR/IXFR for the subzone and retrieve its full zone contents. This issue has been fixed in version 1.14.3.	N/A	More Details
CVE-2026-42514	This vulnerability exists in e-Sushrut due to exposure of OTPs in plaintext within API responses. A remote attacker could exploit this vulnerability by intercepting API responses containing valid OTPs. Successful exploitation of this vulnerability could allow an attacker to impersonate the target user and gain unauthorized access to user accounts on the targeted system.	N/A	More Details
CVE-2026-33420	Vaultwarden is a Bitwarden-compatible server written in Rust. In version 1.35.4 and earlier, the get_org_collections_details endpoint (GET /api/organizations/{org_id}/collections/details) is missing the has_full_access() authorization check that exists on the sibling get_org_collections endpoint. This allows any Manager-role user with accessAll=False and no collection assignments to retrieve the names, UUIDs, user-to-collection mappings, and group-to-collection mappings for all collections in the organization. This issue has been fixed in version 1.35.5.	N/A	More Details
CVE-2026-33324	SQLBot is an intelligent Text-to-SQL system based on large language models and RAG. In versions 1.7.0 and earlier, the Text2SQL chat interface is vulnerable to prompt injection. The user-provided question parameter is directly concatenated into the LLM prompt without filtering or escaping, and the SQL extracted from the LLM response is executed against the database without validation or sanitization. An authenticated attacker can craft a malicious question to manipulate the LLM into generating and executing arbitrary SQL statements. When connected to a PostgreSQL data source, this can lead to remote code execution via COPY FROM PROGRAM. This issue has been fixed in version 1.7.1.	N/A	More Details
CVE-2026-33190	CoreDNS is a DNS server that chains plugins. In versions prior to 1.14.3, the tsig plugin can be bypassed on non-plain-DNS transports (DoT, DoH, DoH3, DoQ, and gRPC) because it trusts the transport writer's TsigStatus() instead of performing verification itself. The DoH and DoH3 writer's TsigStatus() always returns nil, the DoT server does not set TsigSecret on the dns.Server, and the DoQ and gRPC writers also unconditionally return nil. This allows an unauthenticated remote client to bypass TSIG-based authentication and access resources intended to be restricted behind a tsig require all policy. Plain DNS over TCP and UDP are not affected. This issue has been fixed in version 1.14.3.	N/A	More Details
CVE-2026-43064	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix not releasing workqueue on .release() The workqueue associated with an DSA/IAA device is not released when the object is freed.	N/A	More Details
CVE-2026-31710	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix dir separator in SMB1 UNIX mounts When calling cifs_mount_get_tcon() with SMB1 UNIX mounts, @cifs_sb->mnt_cifs_flags needs to be read or updated only after calling reset_cifs_unix_caps(), otherwise it might end up with missing CIFS_MOUNT_POSIXACL and CIFS_MOUNT_POSIX_PATHS bits. This fixes the wrong dir separator used in paths caused by the missing CIFS_MOUNT_POSIX_PATHS bit in cifs_sb_info::mnt_cifs_flags.	N/A	More Details
CVE-2026-2810	Netskope was notified about a potential gap in the Endpoint DLP Module for Netskope Client on Windows systems. The successful exploitation of the gap can potentially allow an unprivileged user to trigger an out-of-bounds read within a driver, leading to a Blue-Screen-of-Death (BSOD). Successful exploitation would require the Endpoint DLP module to be enabled in the client configuration. A successful exploit can potentially result in a denial-of-service for the local machine.	N/A	More Details
CVE-2026-42238	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.8, nginx-ui exposes a backup restore endpoint (POST /api/restore) that is completely unauthenticated during the first 10 minutes after process startup on any fresh installation. An unauthenticated remote attacker can upload a crafted backup archive that overwrites the application's configuration file (app.ini) and SQLite database. Because the attacker controls the restored app.ini, they can inject an arbitrary OS command into the TestConfigCmd setting. After the application automatically restarts to apply the restored config, a single follow-up request triggers that command as the user running nginx-ui — typically root in Docker deployments. This issue has been patched in version 2.3.8.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Don't enumerate SPDIF1 at DAIO initialization The recent refactoring of xfi driver changed the assignment of atc->daios[] at atc_get_resources(); now it loops over all enum DAIOTYP		

CVE-2026-31775	entries while it looped formerly only a part of them. The problem is that the last entry, SPDIF1, is a special type that is used only for hw20k1 CTSB073X model (as a replacement of SPDIFIO), and there is no corresponding definition for hw20k2. Due to the lack of the info, it caused a kernel crash on hw20k2, which was already worked around by the commit b045ab3dff97 ("ALSA: ctxfi: Fix missing SPDIFI1 index handling"). This patch addresses the root cause of the regression above properly, simply by skipping the incorrect SPDIF1 type in the parser loop. For making the change clearer, the code is slightly arranged, too.	N/A	More Details
CVE-2026-42996	JS8Call through 2.3.1 and JS8Call-improved before 3.0 have a stack-based buffer overflow via a radio transmission of @APRSIS GRID followed by a long Maidenhead locator. This occurs in grid2deg in APRSISClient.cpp.	N/A	More Details
CVE-2026-31770	In the Linux kernel, the following vulnerability has been resolved: hwmon: (occ) Fix division by zero in occ_show_power_1() In occ_show_power_1() case 1, the accumulator is divided by update_tag without checking for zero. If no samples have been collected yet (e.g. during early boot when the sensor block is included but hasn't been updated), update_tag is zero, causing a kernel divide-by-zero crash. The 2019 fix in commit 211186cae14d ("hwmon: (occ) Fix division by zero issue") only addressed occ_get_powr_avg() used by occ_show_power_2() and occ_show_power_a0(). This separate code path in occ_show_power_1() was missed. Fix this by reusing the existing occ_get_powr_avg() helper, which already handles the zero-sample case and uses mul_u64_u32_div() to multiply before dividing for better precision. Move the helper above occ_show_power_1() so it is visible at the call site. [groeck: Fix alignment problems reported by checkpatch]	N/A	More Details
CVE-2026-31767	In the Linux kernel, the following vulnerability has been resolved: drm/i915/dsi: Don't do DSC horizontal timing adjustments in command mode Stop adjusting the horizontal timing values based on the compression ratio in command mode. Bspec seems to be telling us to do this only in video mode, and this is also how the Windows driver does things. This should also fix a div-by-zero on some machines because the adjusted htotal ends up being so small that we end up with line_time_us==0 when trying to determine the vtotal value in command mode. Note that this doesn't actually make the display on the Huawei Matebook E work, but at least the kernel no longer explodes when the driver loads. (cherry picked from commit 0b475e91ecc2313207196c6d7fd5c53e1a878525)	N/A	More Details
CVE-2026-31765	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Change AMDGPU_VA_RESERVED_TRAP_SIZE to 64KB Currently, AMDGPU_VA_RESERVED_TRAP_SIZE is hardcoded to 8KB, while KFD_CWSR_TBA_TMA_SIZE is defined as 2 * PAGE_SIZE. On systems with 4K pages, both values match (8KB), so allocation and reserved space are consistent. However, on 64K page-size systems, KFD_CWSR_TBA_TMA_SIZE becomes 128KB, while the reserved trap area remains 8KB. This mismatch causes the kernel to crash when running rocminfo or rccl unit tests. Kernel attempted to read user page (2) - exploit attempt? (uid: 1001) BUG: Kernel NULL pointer dereference on read at 0x00000002 Faulting instruction address: 0xc0000000002c8a64 Oops: Kernel access of bad area, sig: 11 [#1] LE PAGE_SIZE=64K MMU=Radix SMP NR_CPUS=2048 NUMA pSeries CPU: 34 UID: 1001 PID: 9379 Comm: rocminfo Tainted: G E 6.19.0-rc4-amdgpu-00320-gf23176405700 #56 VOLUNTARY Tainted: [E]=UNSIGNED_MODULE Hardware name: IBM,9105-42A POWER10 (architected) 0x800200 0xf000006 of:IBM,FW1060.30 (ML1060_896) hv:phyp pSeries NIP: c0000000002c8a64 LR: c00000000125dbc8 CTR: c00000000125e730 REGS: c0000001e0957580 TRAP: 0300 Tainted: G E MSR: 8000000000009033 <SF,EE,ME,IR,DR,RI,LE> CR: 24008268 XER: 00000036 CFAR: c00000000125dbc4 DAR: 0000000000000002 DSISR: 40000000 IRQMASK: 1 GPR00: c00000000125d908 c0000001e0957820 c0000000016e8100 c00000013d814540 GPR04: 0000000000000002 c00000013d814550 0000000000000045 0000000000000000 GPR08: c00000013444d000 c00000013d814538 c00000013d814538 0000000084002268 GPR12: c00000000125e730 c000007e2ffd5f00 ffffffffffffffff 0000000000020000 GPR16: 0000000000000000 0000000000000002 c00000015f653000 0000000000000000 GPR20: c000000138662400 c00000013d814540 0000000000000000 c00000013d814500 GPR24: 0000000000000000 0000000000000002 c0000001e0957888 c0000001e0957878 GPR28: c00000013d814548 0000000000000000 c00000013d814540 c0000001e0957888 NIP [c0000000002c8a64] __mutex_add_waiter+0x24/0xc0 LR [c00000000125dbc8] __mutex_lock.constprop.0+0x318/0xd00 Call Trace: 0xc0000001e0957890 (unreliable) __mutex_lock.constprop.0+0x58/0xd00 amdgpu_amdkfd_gpuvm_alloc_memory_of_gpu+0x6fc/0xb60 [amdgpu] kfd_process_alloc_gpuvm+0x54/0x1f0 [amdgpu] kfd_process_device_init_cwsr_dgpu+0xa4/0x1a0 [amdgpu] kfd_process_device_init_vm+0xd8/0x2e0 [amdgpu] kfd_ioctl_acquire_vm+0xd0/0x130 [amdgpu] kfd_ioctl+0x514/0x670 [amdgpu] sys_ioctl+0x134/0x180 system_call_exception+0x114/0x300 system_call_vectored_common+0x15c/0x2ec This patch changes AMDGPU_VA_RESERVED_TRAP_SIZE to 64 KB and KFD_CWSR_TBA_TMA_SIZE to the AMD GPU page size. This means we reserve 64 KB for the trap in the address space, but only allocate 8 KB within it. With this approach, the allocation size never exceeds the reserved area. (cherry picked from commit 31b8de5e55666f26ea7ece5f412b83eab3f56dbb)	N/A	More Details
CVE-2026-31764	In the Linux kernel, the following vulnerability has been resolved: iio: imu: st_lsm6dsx: Set buffer sampling frequency for accelerometer only The st_lsm6dsx_hwfifo_odr_store() function, which is called when userspace writes the buffer sampling frequency sysfs attribute, calls st_lsm6dsx_check_odr(), which accesses the odr_table array at index `sensor->id`; since this array is only 2 entries long, an access for any sensor type other than accelerometer or gyroscope is an out-of-bounds access. The motivation for being able to set a buffer frequency different from the sensor sampling frequency is to support use cases that need accurate event detection (which requires a high sampling frequency) while retrieving sensor data at low frequency. Since all the supported event types are generated from acceleration data only, do not create the buffer sampling frequency attribute for sensor types other than the accelerometer.	N/A	More Details
CVE-2026-31763	In the Linux kernel, the following vulnerability has been resolved: iio: gyro: mpu3050: Fix incorrect free_irq() variable The handler for the IRQ part of this driver is mpu3050->trig but, in the teardown free_irq() is called with handler mpu3050. Use correct IRQ handler when calling free_irq().	N/A	More Details
CVE-2026-31762	In the Linux kernel, the following vulnerability has been resolved: iio: gyro: mpu3050: Fix irq resource leak The interrupt handler is setup but only a few lines down if iio_trigger_register() fails the function returns without properly releasing the handler. Add cleanup goto to resolve resource leak. Detected by Smatch: drivers/iio/gyro/mpu3050-core.c:1128 mpu3050_trigger_probe() warn: 'irq' from request_threaded_irq() not released on lines: 1124.	N/A	More Details
CVE-2026-31760	In the Linux kernel, the following vulnerability has been resolved: gpib: lpvo_usb: fix memory leak on disconnect The driver iterates over the registered USB interfaces during GPIB attach and takes a reference to their USB devices until a match is found. These references are never released which leads to a memory leak when devices are disconnected. Fix the leak by dropping the unnecessary references.	N/A	More Details
CVE-2026-31759	In the Linux kernel, the following vulnerability has been resolved: usb: ulpi: fix double free in ulpi_register_interface() error path When device_register() fails, ulpi_register() calls put_device() on ulpi->dev. The device release callback ulpi_dev_release() drops the OF node reference and frees ulpi, but the current error path in ulpi_register_interface() then calls kfree(ulpi) again, causing a double free. Let put_device() handle the cleanup through ulpi_dev_release() and avoid freeing ulpi again in ulpi_register_interface().	N/A	More Details
CVE-2026-31757	In the Linux kernel, the following vulnerability has been resolved: usb: misc: usbio: Fix URB memory leak on submit failure When usb_submit_urb() fails in usbio_probe(), the previously allocated URB is never freed, causing a memory leak. Fix this by jumping to err_free_urb label to properly release the URB on the error path.	N/A	More Details

CVE-2026-31756	In the Linux kernel, the following vulnerability has been resolved: usb: dwc2: gadget: Fix spin_lock/unlock mismatch in dwc2_hsotg_udc_stop() dwc2_gadget_exit_clock_gating() internally calls call_gadget() macro, which expects hsotg->lock to be held since it does spin_unlock/spin_lock around the gadget driver callback invocation. However, dwc2_hsotg_udc_stop() calls dwc2_gadget_exit_clock_gating() without holding the lock. This leads to: - spin_unlock on a lock that is not held (undefined behavior) - The lock remaining held after dwc2_gadget_exit_clock_gating() returns, causing a deadlock when spin_lock_irqsave() is called later in the same function. Fix this by acquiring hsotg->lock before calling dwc2_gadget_exit_clock_gating() and releasing it afterwards, which satisfies the locking requirement of the call_gadget() macro.	N/A	More Details
CVE-2026-31755	In the Linux kernel, the following vulnerability has been resolved: usb: cdns3: gadget: fix NULL pointer dereference in ep_queue When the gadget endpoint is disabled or not yet configured, the ep->desc pointer can be NULL. This leads to a NULL pointer dereference when __cdns3_gadget_ep_queue() is called, causing a kernel crash. Add a check to return -ESHUTDOWN if ep->desc is NULL, which is the standard return code for unconfigured endpoints. This prevents potential crashes when ep_queue is called on endpoints that are not ready.	N/A	More Details
CVE-2026-31754	In the Linux kernel, the following vulnerability has been resolved: usb: cdns3: gadget: fix state inconsistency on gadget init failure When cdns3_gadget_start() fails, the DRD hardware is left in gadget mode while software state remains INACTIVE, creating hardware/software state inconsistency. When switching to host mode via sysfs: echo host > /sys/class/usb_role/13180000.usb-role-switch/role The role state is not set to CDNS_ROLE_STATE_ACTIVE due to the error, so cdns_role_stop() skips cleanup because state is still INACTIVE. This violates the DRD controller design specification (Figure22), which requires returning to idle state before switching roles. This leads to a synchronous external abort in xhci_gen_setup() when setting up the host controller: [516.440698] configfs-gadget 13180000.usb: failed to start g1: -19 [516.442035] cdns-usb3 13180000.usb: Failed to add gadget [516.443278] cdns-usb3 13180000.usb: set role 2 has failed ... [1301.375722] xhci-hcd xhci-hcd.1.auto: xHCI Host Controller [1301.377716] Internal error: synchronous external abort: 96000010 [#1] PREEMPT SMP [1301.382485] pc : xhci_gen_setup+0xa4/0x408 [1301.393391] backtrace: ... xhci_gen_setup+0xa4/0x408 <-- CRASH xhci_plat_setup+0x44/0x58 usb_add_hcd+0x284/0x678 ... cdns_role_set+0x9c/0xbc <-- Role switch Fix by calling cdns_drd_gadget_off() in the error path to properly clean up the DRD gadget state.	N/A	More Details
CVE-2026-31753	In the Linux kernel, the following vulnerability has been resolved: auxdisplay: line-display: fix NULL dereference in linedisp_release linedisp_release() currently retrieves the enclosing struct linedisp via to_linedisp(). That lookup depends on the attachment list, but the attachment may already have been removed before put_device() invokes the release callback. This can happen in linedisp_unregister(), and can also be reached from some linedisp_register() error paths. In that case, to_linedisp() returns NULL and linedisp_release() dereferences it while freeing the display resources. The struct device released here is the embedded linedisp->dev used by linedisp_register(), so retrieve the enclosing object directly with container_of() instead.	N/A	More Details
CVE-2026-31776	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Fix missing SPDIFI1 index handling SPDIF1 DAIO type isn't properly handled in daio_device_index() for hw20k2, and it returned -EINVAL, which ended up with the out-of-bounds array access. Follow the hw20k1 pattern and return the proper index for this type, too.	N/A	More Details
CVE-2026-31777	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Check the error for index mapping The ctxfi driver blindly assumed a proper value returned from daio_device_index(), but it's not always true. Add a proper error check to deal with the error from the function.	N/A	More Details
CVE-2026-31778	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: fix stack out-of-bounds read in init_card The loop creates a whitespace-stripped copy of the card shortname where `len < sizeof(card->id)` is used for the bounds check. Since sizeof(card->id) is 16 and the local id buffer is also 16 bytes, writing 16 non-space characters fills the entire buffer, overwriting the terminating nullbyte. When this non-null-terminated string is later passed to snd_card_set_id() -> copy_valid_id_string(), the function scans forward with `while (*nid && ...)` and reads past the end of the stack buffer, reading the contents of the stack. A USB device with a product name containing many non-ASCII, non-space characters (e.g. multibyte UTF-8) will reliably trigger this as follows: BUG: KASAN: stack-out-of-bounds in copy_valid_id_string sound/core/init.c:696 [inline] BUG: KASAN: stack-out-of-bounds in snd_card_set_id_no_lock+0x698/0x74c sound/core/init.c:718 The off-by-one has been present since commit bafeee5b1f8d ("ALSA: snd_usb_caiaq: give better shortname") from June 2009 (v2.6.31-rc1), which first introduced this whitespace-stripping loop. The original code never accounted for the null terminator when bounding the copy. Fix this by changing the loop bound to `sizeof(card->id) - 1`, ensuring at least one byte remains as the null terminator.	N/A	More Details
CVE-2026-43010	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject sleepable kprobe_multi programs at attach time kprobe.multi programs run in atomic/RCU context and cannot sleep. However, bpf_kprobe_multi_link_attach() did not validate whether the program being attached had the sleepable flag set, allowing sleepable helpers such as bpf_copy_from_user() to be invoked from a non-sleepable context. This causes a "sleeping function called from invalid context" splat: BUG: sleeping function called from invalid context at ./include/linux/uaccess.h:169 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 1787, name: sudo preempt_count: 1, expected: 0 RCU nest depth: 2, expected: 0 Fix this by rejecting sleepable programs early in bpf_kprobe_multi_link_attach(), before any further processing.	N/A	More Details
CVE-2026-4178	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-43017	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: validate mesh send advertising payload length mesh_send() currently bounds MGMT_OP_MESH_SEND by total command length, but it never verifies that the bytes supplied for the flexible adv_data[] array actually match the embedded adv_data_len field. MGMT_MESH_SEND_SIZE only covers the fixed header, so a truncated command can still pass the existing 20..50 byte range check and later drive the async mesh send path past the end of the queued command buffer. Keep rejecting zero-length and oversized advertising payloads, but validate adv_data_len explicitly and require the command length to exactly match the flexible array size before queueing the request.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: macb: fix clk handling on PCI glue driver removal platform_device_unregister() may still want to use the registered clks during runtime resume callback. Note that there is a commit d82d5303c4c5 ("net: macb: fix use after free on rmmod") that addressed the similar problem of clk vs platform device unregistration but just moved the bug to another place. Save the pointers to clks into local variables for reuse after platform device is unregistered. BUG: KASAN: use-after-free in clk_prepare+0x5a/0x60 Read of size 8 at addr ffff888104f85e00 by task modprobe/597 CPU: 2 PID: 597 Comm: modprobe Not tainted 6.1.164+ #114 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.1-0-g3208b098f51a-prebuilt.qemu.org 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x8d/0xba print_report+0x17f/0x496 kasan_report+0xd9/0x180 clk_prepare+0x5a/0x60 macb_runtime_resume+0x13d/0x410 [macb] pm_generic_runtime_resume+0x97/0xd0 __rpm_callback+0xc8/0x4d0 rpm_callback+0xf6/0x230 rpm_resume+0xeeb/0x1a70 __pm_runtime_resume+0xb4/0x170 bus_remove_device+0x2e3/0x4b0 device_del+0x5b3/0xdc0 platform_device_del+0x4e/0x280		

CVE-2026-43015	platform_device_unregister+0x11/0x50 pci_device_remove+0xae/0x210 device_remove+0xcb/0x180 device_release_driver_internal+0x529/0x770 driver_detach+0xd4/0x1a0 bus_remove_driver+0x135/0x260 driver_unregister+0x72/0xb0 pci_unregister_driver+0x26/0x220 __do_sys_delete_module+0x32e/0x550 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x6e/0xd8 </TASK> Allocated by task 519: kasan_save_stack+0x2c/0x50 kasan_set_track+0x21/0x30 __kasan_kmalloc+0x8e/0x90 __clk_register+0x458/0x2890 clk_hw_register+0x1a/0x60 __clk_hw_register_fixed_rate+0x255/0x410 clk_register_fixed_rate+0x3c/0xa0 macb_probe+0x1d8/0x42e [macb_pci] local_pci_probe+0xd7/0x190 pci_device_probe+0x252/0x600 really_probe+0x255/0x7f0 __driver_probe_device+0x1ee/0x330 driver_probe_device+0x4c/0x1f0 __driver_attach+0x1df/0x4e0 bus_for_each_dev+0x15d/0x1f0 bus_add_driver+0x486/0x5e0 driver_register+0x23a/0x3d0 do_one_initcall+0xfd/0x4d0 do_init_module+0x18b/0x5a0 load_module+0x5663/0x7950 __do_sys_finit_module+0x101/0x180 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x6e/0xd8 Freed by task 597: kasan_save_stack+0x2c/0x50 kasan_set_track+0x21/0x30 kasan_save_free_info+0x2a/0x50 __kasan_slab_free+0x106/0x180 __kmem_cache_free+0xbc/0x320 clk_unregister+0x6de/0x8d0 macb_remove+0x73/0xc0 [macb_pci] pci_device_remove+0xae/0x210 device_remove+0xcb/0x180 device_release_driver_internal+0x529/0x770 driver_detach+0xd4/0x1a0 bus_remove_driver+0x135/0x260 driver_unregister+0x72/0xb0 pci_unregister_driver+0x26/0x220 __do_sys_delete_module+0x32e/0x550 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x6e/0xd8	N/A	More Details
CVE-2026-43014	In the Linux kernel, the following vulnerability has been resolved: net: macb: properly unregister fixed rate clocks The additional resources allocated with clk_register_fixed_rate() need to be released with clk_unregister_fixed_rate(), otherwise they are lost.	N/A	More Details
CVE-2026-43013	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: lag: Check for LAG device before creating debugfs __mlx5_lag_dev_add_mdev() may return 0 (success) even when an error occurs that is handled gracefully. Consequently, the initialization flow proceeds to call mlx5_ldev_add_debugfs() even when there is no valid LAG context. mlx5_ldev_add_debugfs() blindly created the debugfs directory and attributes. This exposed interfaces (like the members file) that rely on a valid ldev pointer, leading to potential NULL pointer dereferences if accessed when ldev is NULL. Add a check to verify that mlx5_lag_dev(dev) returns a valid pointer before attempting to create the debugfs entries.	N/A	More Details
CVE-2026-43012	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix switchdev mode rollback in case of failure If for some internal reason switchdev mode fails, we rollback to legacy mode, before this patch, rollback will unregister the uplink netdev and leave it unregistered causing the below kernel bug. To fix this, we need to avoid netdev unregister by setting the proper rollback flag 'MLX5_PRIV_FLAGS_SWITCH_LEGACY' to indicate legacy mode. devlink (431) used greatest stack depth: 11048 bytes left mlx5_core 0000:00:03.0: E-Switch: Disable: mode(LEGACY), nvfs(0), \ necvfs(0), active vports(0) mlx5_core 0000:00:03.0: E-Switch: Supported tc chains and prios offload mlx5_core 0000:00:03.0: Loading uplink representor for vport 65535 mlx5_core 0000:00:03.0: mlx5_cmd_out_err:816:(pid 456): \ QUERY_HCA_CAP(0x100) op_mod(0x0) failed, \ status bad parameter(0x3), syndrome (0x3a3846), err(-22) mlx5_core 0000:00:03.0 enp0s3np0 (unregistered): Unloading uplink \ representor for vport 65535 ------------[cut here]------------ kernel BUG at net/core/dev.c:12070! Oops: invalid opcode: 0000 [#1] SMP NOPTI CPU: 2 UID: 0 PID: 456 Comm: devlink Not tainted 6.16.0-rc3+ \ #9 PREEMPT(voluntary) RIP: 0010:unregister_netdevice_many_notify+0x123/0xae0 ... Call Trace: [90.923094] unregister_netdevice_queue+0xad/0xf0 [90.923323] unregister_netdev+0x1c/0x40 [90.923522] mlx5e_vport_rep_unload+0x61/0xc6 [90.923736] esw_offloads_enable+0x8e6/0x920 [90.923947] mlx5_eswitch_enable_locked+0x349/0x430 [90.924182] ? is_mp_supported+0x57/0xb0 [90.924376] mlx5_devlink_eswitch_mode_set+0x167/0x350 [90.924628] devlink_nl_eswitch_set_doit+0x6f/0xf0 [90.924862] genl_family_rcv_msg_doit+0xe8/0x140 [90.925088] genl_rcv_msg+0x18b/0x290 [90.925269] ? __pfx_devlink_nl_pre_doit+0x10/0x10 [90.925506] ? __pfx_devlink_nl_eswitch_set_doit+0x10/0x10 [90.925766] ? __pfx_devlink_nl_post_doit+0x10/0x10 [90.926001] ? __pfx_genl_rcv_msg+0x10/0x10 [90.926206] netlink_rcv_skb+0x52/0x100 [90.926393] genl_rcv+0x28/0x40 [90.926557] netlink_unicast+0x27d/0x3d0 [90.926749] netlink_sendmsg+0x1f7/0x430 [90.926942] __sys_sendto+0x213/0x220 [90.927127] ? __sys_recvmsg+0x6a/0xd0 [90.927312] __x64_sys_sendto+0x24/0x30 [90.927504] do_syscall_64+0x50/0x1c0 [90.927687] entry_SYSCALL_64_after_hwframe+0x76/0x7e [90.927929] RIP: 0033:0x7f7d0363e047	N/A	More Details
CVE-2026-43008	In the Linux kernel, the following vulnerability has been resolved: gpio: qixis-fpga: Fix error handling for devm_regmap_init_mmio() devm_regmap_init_mmio() returns an ERR_PTR() on failure, not NULL. The original code checked for NULL which would never trigger on error, potentially leading to an invalid pointer dereference. Use IS_ERR() and PTR_ERR() to properly handle the error case.	N/A	More Details
CVE-2026-31781	In the Linux kernel, the following vulnerability has been resolved: drm/ioc32: stop speculation on the drm_compat_ioctl path The drm compat ioctl path takes a user controlled pointer, and then dereferences it into a table of function pointers, the signature method of spectre problems. Fix this up by calling array_index_nospec() on the index to the function pointer list.	N/A	More Details
CVE-2026-43007	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Handle DBC deactivation if the owner went away When a DBC is released, the device sends a QAIC_TRANS_DEACTIVATE_FROM_DEV transaction to the host over the QAIC_CONTROL MHI channel. QAIC handles this by calling decode_deactivate() to release the resources allocated for that DBC. Since that handling is done in the qaic_manage_ioctl() context, if the user goes away before receiving and handling the deactivation, the host will be out-of-sync with the DBCs available for use, and the DBC resources will not be freed unless the device is removed. If another user loads and requests to activate a network, then the device assigns the same DBC to that network, QAIC will "indefinitely" wait for dbc->in_use = false, leading the user process to hang. As a solution to this, handle QAIC_TRANS_DEACTIVATE_FROM_DEV transactions that are received after the user has gone away.	N/A	More Details
CVE-2026-43005	In the Linux kernel, the following vulnerability has been resolved: hwmon: (tps53679) Fix array access with zero-length block read i2c_smbus_read_block_data() can return 0, indicating a zero-length read. When this happens, tps53679_identify_chip() accesses buf[ret - 1] which is buf[-1], reading one byte before the buffer on the stack. Fix by changing the check from "ret < 0" to "ret <= 0", treating a zero-length read as an error (-EIO), which prevents the out-of-bounds array access. Also fix a typo in the adjacent comment: "if present" instead of duplicate "if".	N/A	More Details
CVE-2026-43004	In the Linux kernel, the following vulnerability has been resolved: spi: stm32-ospi: Fix resource leak in remove() callback The remove() callback returned early if pm_runtime_resume_and_get() failed, skipping the cleanup of spi controller and other resources. Remove the early return so cleanup completes regardless of PM resume result.	N/A	More Details
CVE-2026-31785	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_pagefault: Disallow writes to read-only VMAs The page fault handler should reject write/atomic access to read only VMAs. Add code to handle this in xe_pagefault_service after the VMA lookup. v2: - Apply max line length (Matthew) (cherry picked from commit 714ee6754ac5fa3dc078856a196a6b124cd797a0)	N/A	More Details
CVE-2026-31784	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pxp: Clear restart flag in pxp_start after jumping back If we don't clear the flag we'll keep jumping back at the beginning of the function once we reach the end. (cherry picked from commit 0850ec7bb2459602351639dccf7a68a03c9d1ee0)	N/A	More Details

CVE-2026-31783	In the Linux kernel, the following vulnerability has been resolved: spi: amlogic: spifc-a4: unregister ECC engine on probe failure and remove() callback aml_sfc_probe() registers the on-host NAND ECC engine, but teardown was missing from both probe unwind and remove-time cleanup. Add a devm cleanup action after successful registration so nand_ecc_unregister_on_host_hw_engine() runs automatically on probe failures and during device removal.	N/A	More Details
CVE-2026-31752	In the Linux kernel, the following vulnerability has been resolved: bridge: br_nd_send: validate ND option lengths br_nd_send() walks ND options according to option-provided lengths. A malformed option can make the parser advance beyond the computed option span or use a too-short source LLADDR option payload. Validate option lengths against the remaining NS option area before advancing, and only read source LLADDR when the option is large enough for an Ethernet address.	N/A	More Details
CVE-2026-31751	In the Linux kernel, the following vulnerability has been resolved: comedi: dt2815: add hardware detection to prevent crash The dt2815 driver crashes when attached to I/O ports without actual hardware present. This occurs because syzkaller or users can attach the driver to arbitrary I/O addresses via COMEDI_DEVCONFIG ioctl. When no hardware exists at the specified port, inb() operations return 0xff (floating bus), but outb() operations can trigger page faults due to undefined behavior, especially under race conditions: BUG: unable to handle page fault for address: 000000007fffff90 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page RIP: 0010:dt2815_attach+0x6e0/0x1110 Add hardware detection by reading the status register before attempting any write operations. If the read returns 0xff, assume no hardware is present and fail the attach with -ENODEV. This prevents crashes from outb() operations on non-existent hardware.	N/A	More Details
CVE-2026-31750	In the Linux kernel, the following vulnerability has been resolved: comedi: runflags cannot determine whether to reclaim chanlist syzbot reported a memory leak [1], because commit 4e1da516debb ("comedi: Add reference counting for Comedi command handling") did not consider the exceptional exit case in do_cmd_ioctl() where runflags is not set. This caused chanlist not to be properly freed by do_become_nonbusy(), as it only frees chanlist when runflags is correctly set. Added a check in do_become_nonbusy() for the case where runflags is not set, to properly free the chanlist memory. [1] BUG: memory leak backtrace (crc 844a0efa): __comedi_get_user_chanlist drivers/comedi/comedi_fops.c:1815 [inline] do_cmd_ioctl.part.0+0x112/0x350 drivers/comedi/comedi_fops.c:1890 do_cmd_ioctl drivers/comedi/comedi_fops.c:1858 [inline]	N/A	More Details
CVE-2026-31721	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_hid: move list and spinlock inits from bind to alloc There was an issue when you did the following: - setup and bind an hid gadget - open /dev/hidg0 - use the resulting fd in EPOLL_CTL_ADD - unbind the UDC - bind the UDC - use the fd in EPOLL_CTL_DEL When CONFIG_DEBUG_LIST was enabled, a list_del corruption was reported within remove_wait_queue (via ep_remove_wait_queue). After some debugging I found out that the queues, which f_hid registers via poll_wait were the problem. These were initialized using init_waitqueue_head inside hidg_bind. So effectively, the bind function re-initialized the queues while there were still items in them. The solution is to move the initialization from hidg_bind to hidg_alloc to extend their lifetimes to the lifetime of the function instance. Additionally, I found many other possibly problematic init calls in the bind function, which I moved as well.	N/A	More Details
CVE-2026-31727	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_ether: Fix NULL pointer deref in eth_get_drvinfo Commit ec35c1969650 ("usb: gadget: f_ncm: Fix net_device lifecycle with device_move") reparents the gadget device to /sys/devices/virtual during unbind, clearing the gadget pointer. If the userspace tool queries on the surviving interface during this detached window, this leads to a NULL pointer dereference. Unable to handle kernel NULL pointer dereference Call trace: eth_get_drvinfo+0x50/0x90 ethtool_get_drvinfo+0x5c/0x1f0 __dev_ethtool+0xaec/0x1fe0 dev_ethtool+0x134/0x2e0 dev_ioctl+0x338/0x560 Add a NULL check for dev->gadget in eth_get_drvinfo(). When detached, skip copying the fw_version and bus_info strings, which is natively handled by ethtool_get_drvinfo for empty strings.	N/A	More Details
CVE-2026-31726	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: uvc: fix NULL pointer dereference during unbind race Commit b81ac4395bbe ("usb: gadget: uvc: allow for application to cleanly shutdown") introduced two stages of synchronization waits totaling 1500ms in uvc_function_unbind() to prevent several types of kernel panics. However, this timing-based approach is insufficient during power management (PM) transitions. When the PM subsystem starts freezing user space processes, the wait_event_interruptible_timeout() is aborted early, which allows the unbind thread to proceed and nullify the gadget pointer (cdev->gadget = NULL): [814.123447][T947] configfs-gadget.g1 gadget.0: uvc: uvc_function_unbind() [814.178583][T3173] PM: suspend entry (deep) [814.192487][T3173] Freezing user space processes [814.197668][T947] configfs-gadget.g1 gadget.0: uvc: uvc_function_unbind no clean disconnect, wait for release When the PM subsystem resumes or aborts the suspend and tasks are restarted, the V4L2 release path is executed and attempts to access the already nullified gadget pointer, triggering a kernel panic: [814.292597][C0] PM: pm_system_irq_wakeup: 479 triggered dhdpcie_host_wake [814.386727][T3173] Restarting tasks ... [814.403522][T4558] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000030 [814.404021][T4558] pc : usb_gadget_deactivate+0x14/0xf4 [814.404031][T4558] lr : usb_function_deactivate+0x54/0x94 [814.404078][T4558] Call trace: [814.404080][T4558] usb_gadget_deactivate+0x14/0xf4 [814.404083][T4558] usb_function_deactivate+0x54/0x94 [814.404087][T4558] uvc_function_disconnect+0x1c/0x5c [814.404092][T4558] uvc_v4l2_release+0x44/0xac [814.404095][T4558] v4l2_release+0xcc/0x130 Address the race condition and NULL pointer dereference by: 1. State Synchronization (flag + mutex) Introduce a 'func_unbound' flag in struct uvc_device. This allows uvc_function_disconnect() to safely skip accessing the nullified cdev->gadget pointer. As suggested by Alan Stern, this flag is protected by a new mutex (uvc->lock) to ensure proper memory ordering and prevent instruction reordering or speculative loads. This mutex is also used to protect 'func_connected' for consistent state management. 2. Explicit Synchronization (completion) Use a completion to synchronize uvc_function_unbind() with the uvc_vdev_release() callback. This prevents Use-After-Free (UAF) by ensuring struct uvc_device is freed after all video device resources are released.	N/A	More Details
CVE-2026-31725	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ecm: Fix net_device lifecycle with device_move The net_device is allocated during function instance creation and registered during the bind phase with the gadget device as its sysfs parent. When the function unbinds, the parent device is destroyed, but the net_device survives, resulting in dangling sysfs symlinks: console:/ # ls -l /sys/class/net/usb0 lrwxrwxrwx ... /sys/class/net/usb0 -> /sys/devices/platform/.../gadget.0/net/usb0 console:/ # ls -l /sys/devices/platform/.../gadget.0/net/usb0 ls: .../gadget.0/net/usb0: No such file or directory Use device_move() to reparent the net_device between the gadget device tree and /sys/devices/virtual across bind and unbind cycles. During the final unbind, calling device_move(NULL) moves the net_device to the virtual device tree before the gadget device is destroyed. On rebinding, device_move() reparents the device back under the new gadget, ensuring proper sysfs topology and power management ordering. To maintain compatibility with legacy composite drivers (e.g., multi.c), the bound flag is used to indicate whether the network device is shared and pre-registered during the legacy driver's bind phase.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_eem: Fix net_device lifecycle with device_move The net_device is allocated during function instance creation and registered during the bind phase with the gadget device as its sysfs parent. When the function unbinds, the parent device is destroyed, but the net_device survives, resulting in dangling sysfs symlinks: console:/ # ls -l /sys/class/net/usb0 lrwxrwxrwx ... /sys/class/net/usb0 -> /sys/devices/platform/.../gadget.0/net/usb0 console:/ # ls -l /sys/devices/platform/.../gadget.0/net/usb0 ls: .../gadget.0/net/usb0: No such file or directory Use device_move() to reparent the net_device between the gadget device tree and /sys/devices/virtual across bind and unbind cycles. During the final unbind, calling	N/A	More Details

31724	device_move(NULL) moves the net_device to the virtual device tree before the gadget device is destroyed. On rebinding, device_move() reparents the device back under the new gadget, ensuring proper sysfs topology and power management ordering. To maintain compatibility with legacy composite drivers (e.g., multi.c), the bound flag is used to indicate whether the network device is shared and pre-registered during the legacy driver's bind phase.		
CVE-2026-31723	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_subset: Fix net_device lifecycle with device_move The net_device is allocated during function instance creation and registered during the bind phase with the gadget device as its sysfs parent. When the function unbinds, the parent device is destroyed, but the net_device survives, resulting in dangling sysfs symlinks: console:/ # ls -l /sys/class/net/usb0 lrwxrwxrwx ... /sys/class/net/usb0 -> /sys/devices/platform/.../gadget.0/net/usb0 console:/ # ls -l /sys/devices/platform/.../gadget.0/net/usb0 ls: .../gadget.0/net/usb0: No such file or directory Use device_move() to reparent the net_device between the gadget device tree and /sys/devices/virtual across bind and unbind cycles. During the final unbind, calling device_move(NULL) moves the net_device to the virtual device tree before the gadget device is destroyed. On rebinding, device_move() reparents the device back under the new gadget, ensuring proper sysfs topology and power management ordering. To maintain compatibility with legacy composite drivers (e.g., multi.c), the bound flag is used to indicate whether the network device is shared and pre-registered during the legacy driver's bind phase.	N/A	More Details
CVE-2026-31722	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_rndis: Fix net_device lifecycle with device_move The net_device is allocated during function instance creation and registered during the bind phase with the gadget device as its sysfs parent. When the function unbinds, the parent device is destroyed, but the net_device survives, resulting in dangling sysfs symlinks: console:/ # ls -l /sys/class/net/usb0 lrwxrwxrwx ... /sys/class/net/usb0 -> /sys/devices/platform/.../gadget.0/net/usb0 console:/ # ls -l /sys/devices/platform/.../gadget.0/net/usb0 ls: .../gadget.0/net/usb0: No such file or directory Use device_move() to reparent the net_device between the gadget device tree and /sys/devices/virtual across bind and unbind cycles. During the final unbind, calling device_move(NULL) moves the net_device to the virtual device tree before the gadget device is destroyed. On rebinding, device_move() reparents the device back under the new gadget, ensuring proper sysfs topology and power management ordering. To maintain compatibility with legacy composite drivers (e.g., multi.c), the borrowed_net flag is used to indicate whether the network device is shared and pre-registered during the legacy driver's bind phase.	N/A	More Details
CVE-2026-31720	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_uac1_legacy: validate control request size f_audio_complete() copies req->length bytes into a 4-byte stack variable: u32 data = 0; memcpy(&data, req->buf, req->length); req->length is derived from the host-controlled USB request path, which can lead to a stack out-of-bounds write. Validate req->actual against the expected payload size for the supported control selectors and decode only the expected amount of data. This avoids copying a host-influenced length into a fixed-size stack object.	N/A	More Details
CVE-2026-31729	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: validate connector number in ucsi_notify_common() The connector number extracted from CCI via UCSI_CCI_CONNECTOR() is a 7-bit field (0-127) that is used to index into the connector array in ucsi_connector_change(). However, the array is only allocated for the number of connectors reported by the device (typically 2-4 entries). A malicious or malfunctioning device could report an out-of-range connector number in the CCI, causing an out-of-bounds array access in ucsi_connector_change(). Add a bounds check in ucsi_notify_common(), the central point where CCI is parsed after arriving from hardware, so that bogus connector numbers are rejected before they propagate further.	N/A	More Details
CVE-2026-31701	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: take a reference on the USB device in create_card() The caiaq driver stores a pointer to the parent USB device in cdev->chip.dev but never takes a reference on it. The card's private_free callback, snd_usb_caiaq_card_free(), can run asynchronously via snd_card_free_when_closed() after the USB device has already been disconnected and freed, so any access to cdev->chip.dev in that path dereferences a freed usb_device. On top of the refcounting issue, the current card_free implementation calls usb_reset_device(cdev->chip.dev). A reset in a free callback is inappropriate: the device is going away, the call takes the device lock in a teardown context, and the reset races with the disconnect path that the callback is already cleaning up after. Take a reference on the USB device in create_card() with usb_get_dev(), drop it with usb_put_dev() in the free callback, and remove the usb_reset_device() call.	N/A	More Details
CVE-2026-31702	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix use-after-free of sbi in f2fs_compress_write_end_io() In f2fs_compress_write_end_io(), dec_page_count(sbi, type) can bring the F2FS_WB_CP_DATA counter to zero, unblocking f2fs_wait_on_all_pages() in f2fs_put_super() on a concurrent unmount CPU. The unmount path then proceeds to call f2fs_destroy_page_array_cache(sbi), which destroys sbi->page_array_slab via kmem_cache_destroy(), and eventually kfree(sbi). Meanwhile, the bio completion callback is still executing: when it reaches page_array_free(sbi, ...), it dereferences sbi->page_array_slab — a destroyed slab cache — to call kmem_cache_free(), causing a use-after-free. This is the same class of bug as CVE-2026-23234 (which fixed the equivalent race in f2fs_write_end_io() in data.c), but in the compressed writeback completion path that was not covered by that fix. Fix this by moving dec_page_count() to after page_array_free(), so that all sbi accesses complete before the counter decrement that can unblock unmount. For non-last folios (where atomic_dec_return on cic->pending_pages is nonzero), dec_page_count is called immediately before returning — page_array_free is not reached on this path, so there is no post-decrement sbi access. For the last folio, page_array_free runs while the F2FS_WB_CP_DATA counter is still nonzero (this folio has not yet decremented it), keeping sbi alive, and dec_page_count runs as the final operation.	N/A	More Details
CVE-2026-31715	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix UAF caused by decrementing sbi->nr_pages[] in f2fs_write_end_io() The xfstests case "generic/107" and syzbot have both reported a NULL pointer dereference. The concurrent scenario that triggers the panic is as follows: F2FS_WB_CP_DATA write callback umount - f2fs_write_checkpoint - f2fs_wait_on_all_pages(sbi, F2FS_WB_CP_DATA) - blk_mq_end_request - bio_endio - f2fs_write_end_io : dec_page_count(sbi, F2FS_WB_CP_DATA) : wake_up(&sbi->cp_wait) - kill_f2fs_super - kill_block_super - f2fs_put_super : iput(sbi->node_inode) : sbi->node_inode = NULL : f2fs_in_warm_node_list - is_node_folio // sbi->node_inode is NULL and panic The root cause is that f2fs_put_super() calls iput(sbi->node_inode) and sets sbi->node_inode to NULL after sbi->nr_pages[F2FS_WB_CP_DATA] is decremented to zero. As a result, f2fs_in_warm_node_list() may dereference a NULL node_inode when checking whether a folio belongs to the node inode, leading to a panic. This patch fixes the issue by calling f2fs_in_warm_node_list() before decrementing sbi->nr_pages[F2FS_WB_CP_DATA], thus preventing the use-after-free condition.	N/A	More Details
CVE-2026-31714	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid memory leak in f2fs_rename() syzbot reported a f2fs bug as below: BUG: memory leak unreferenced object 0xffff888127f70830 (size 16): comm "syz.0.23", pid 6144, jiffies 4294943712 hex dump (first 16 bytes): 3c af 57 72 5b e6 8f ad 6e 8e fd 33 42 39 03 ff <.Wr[...n..3B9.. backtrace (crc 925f8a80): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4520 [inline] slab_alloc_node mm/slub.c:4844 [inline] __do_kmalloc_node mm/slub.c:5237 [inline] __kmalloc_noprof+0x3bd/0x560 mm/slub.c:5250 kmalloc_noprof include/linux/slab.h:954 [inline] fscrypt_setup_filename+0x15e/0x3b0 fs/crypto/fname.c:364 f2fs_setup_filename+0x52/0xb0 fs/f2fs/dir.c:143 f2fs_rename+0x159/0xca0 fs/f2fs/namei.c:961 f2fs_rename2+0xd5/0xf20 fs/f2fs/namei.c:1308 vfs_rename+0x7ff/0x1250 fs/namei.c:6026 filename_renameat2+0x4f4/0x660 fs/namei.c:6144 __do_sys_renameat2 fs/namei.c:6173 [inline] __se_sys_renameat2 fs/namei.c:6168 [inline] __x64_sys_renameat2+0x59/0x80 fs/namei.c:6168 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe2/0xf80 arch/x86/entry/syscall_64.c:94	N/A	More Details

	entry_SYSCALL_64_after_hwframe+0x77/0x7f The root cause is in commit 40b2d55e0452 ("f2fs: fix to create selinux label during whiteout initialization"), we added a call to f2fs_setup_filename() without a matching call to f2fs_free_filename(), fix it.		
CVE-2026-31713	In the Linux kernel, the following vulnerability has been resolved: fuse: abort on fatal signal during sync init When sync init is used and the server exits for some reason (error, crash) while processing FUSE_INIT, the filesystem creation will hang. The reason is that while all other threads will exit, the mounting thread (or process) will keep the device fd open, which will prevent an abort from happening. This is a regression from the async mount case, where the mount was done first, and the FUSE_INIT processing afterwards, in which case there's no such recursive syscall keeping the fd open.	N/A	More Details
CVE-2026-31704	In the Linux kernel, the following vulnerability has been resolved: ksmbd: use check_add_overflow() to prevent u16 DACL size overflow set_posix_acl_entries_dacl() and set_ntacl_dacl() accumulate ACE sizes in u16 variables. When a file has many POSIX ACL entries, the accumulated size can wrap past 65535, causing the pointer arithmetic (char *)pndace + *size to land within already-written ACEs. Subsequent writes then overwrite earlier entries, and pndacl->size gets a truncated value. Use check_add_overflow() at each accumulation point to detect the wrap before it corrupts the buffer, consistent with existing check_mul_overflow() usage elsewhere in smbacl.c.	N/A	More Details
CVE-2026-31728	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_ether: Fix race between gether_disconnect and eth_stop A race condition between gether_disconnect() and eth_stop() leads to a NULL pointer dereference. Specifically, if eth_stop() is triggered concurrently while gether_disconnect() is tearing down the endpoints, eth_stop() attempts to access the cleared endpoint descriptor, causing the following NPE: Unable to handle kernel NULL pointer dereference Call trace: __dwc3_gadget_ep_enable+0x60/0x788 dwc3_gadget_ep_enable+0x70/0xe4 usb_ep_enable+0x60/0x15c eth_stop+0xb8/0x108 Because eth_stop() crashes while holding the dev->lock, the thread running gether_disconnect() fails to acquire the same lock and spins forever, resulting in a hardlockup: Core - Debugging Information for Hardlockup core(7) Call trace: queued_spin_lock_slowpath+0x94/0x488 _raw_spin_lock+0x64/0x6c gether_disconnect+0x19c/0x1e8 ncm_set_alt+0x68/0x1a0 composite_setup+0x6a0/0xc50 The root cause is that the clearing of dev->port_usb in gether_disconnect() is delayed until the end of the function. Move the clearing of dev->port_usb to the very beginning of gether_disconnect() while holding dev->lock. This cuts off the link immediately, ensuring eth_stop() will see dev->port_usb as NULL and safely bail out.	N/A	More Details
CVE-2026-31730	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: possible double-free of cctx->remote_heap fastrpc_init_create_static_process() may free cctx->remote_heap on the err_map path but does not clear the pointer. Later, fastrpc_rpmsg_remove() frees cctx->remote_heap again if it is non-NULL, which can lead to a double-free if the INIT_CREATE_STATIC ioctl hits the error path and the rpmsg device is subsequently removed/unbound. Clear cctx->remote_heap after freeing it in the error path to prevent the later cleanup from freeing it again. This issue was found by an in-house analysis workflow that extracts AST-based information and runs static checks, with LLM assistance for triage, and was confirmed by manual code review. No hardware testing was performed.	N/A	More Details
CVE-2026-31749	In the Linux kernel, the following vulnerability has been resolved: comedi: ni_atmio16d: Fix invalid clean-up after failed attach If the driver's COMEDI "attach" handler function (`atmio16d_attach()`) returns an error, the COMEDI core will call the driver's "detach" handler function (`atmio16d_detach()`) to clean up. This calls `reset_atmio16d()` unconditionally, but depending on where the error occurred in the attach handler, the device may not have been sufficiently initialized to call `reset_atmio16d()`. It uses `dev->iobase` as the I/O port base address and `dev->private` as the pointer to the COMEDI device's private data structure. `dev->iobase` may still be set to its initial value of 0, which would result in undesired writes to low I/O port addresses. `dev->private` may still be `NULL`, which would result in null pointer dereferences. Fix `atmio16d_detach()` by checking that `dev->private` is valid (non-null) before calling `reset_atmio16d()`. This implies that `dev->iobase` was set correctly since that is set up before `dev->private`.	N/A	More Details
CVE-2026-31741	In the Linux kernel, the following vulnerability has been resolved: counter: rz-mtu3-cnt: prevent counter from being toggled multiple times Runtime PM counter is incremented / decremented each time the sysfs enable file is written to. If user writes 0 to the sysfs enable file multiple times, runtime PM usage count underflows, generating the following message. rz-mtu3-counter rz-mtu3-counter.0: Runtime PM usage count underflow! At the same time, hardware registers end up being accessed with clocks off in rz_mtu3_terminate_counter() to disable an already disabled channel. If user writes 1 to the sysfs enable file multiple times, runtime PM usage count will be incremented each time, requiring the same number of 0 writes to get it back to 0. If user writes 0 to the sysfs enable file while PWM is in progress, PWM is stopped without counter being the owner of the underlying MTU3 channel. Check against the cached count_is_enabled value and exit if the user is trying to set the same enable value.	N/A	More Details
CVE-2026-31748	In the Linux kernel, the following vulnerability has been resolved: comedi: me_daq: Fix potential overrun of firmware buffer `me2600_xilinx_download()` loads the firmware that was requested by `request_firmware()`. It is possible for it to overrun the source buffer because it blindly trusts the file format. It reads a data stream length from the first 4 bytes into variable `file_length` and reads the data stream contents of length `file_length` from offset 16 onwards. Although it checks that the supplied firmware is at least 16 bytes long, it does not check that it is long enough to contain the data stream. Add a test to ensure that the supplied firmware is long enough to contain the header and the data stream. On failure, log an error and return `-EINVAL`.	N/A	More Details
CVE-2026-31747	In the Linux kernel, the following vulnerability has been resolved: comedi: me4000: Fix potential overrun of firmware buffer `me4000_xilinx_download()` loads the firmware that was requested by `request_firmware()`. It is possible for it to overrun the source buffer because it blindly trusts the file format. It reads a data stream length from the first 4 bytes into variable `file_length` and reads the data stream contents of length `file_length` from offset 16 onwards. Add a test to ensure that the supplied firmware is long enough to contain the header and the data stream. On failure, log an error and return `-EINVAL`. Note: The firmware loading was totally broken before commit ac584af59945 ("staging: comedi: me4000: fix firmware downloading"), but that is the most sensible target for this fix.	N/A	More Details
CVE-2026-31746	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Fix memory leak with CCA cards used as accelerator Tests showed that there is a memory leak if CCA cards are used as accelerator for clear key RSA requests (ME and CRT). With the last rework for the memory allocation the AP messages are allocated by ap_init_apmsg() but for some reason on two places (ME and CRT) the older allocation was still in place. So the first allocation simple was never freed.	N/A	More Details
CVE-2026-31745	In the Linux kernel, the following vulnerability has been resolved: reset: gpio: fix double free in reset_add_gpio_aux_device() error path When __auxiliary_device_add() fails, reset_add_gpio_aux_device() calls auxiliary_device_uninit(adev). The device release callback reset_gpio_aux_device_release() frees adev, but the current error path then calls kfree(adev) again, causing a double free. Keep kfree(adev) for the auxiliary_device_init() failure path, but avoid freeing adev after auxiliary_device_uninit().	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: PM: EM: Fix NULL pointer dereference when perf domain ID is not found dev_energymodel_nl_get_perf_domains_doit() calls em_perf_domain_get_by_id() but does not check the return value before passing it to __em_nl_get_pd_size(). When a caller supplies a non-existent perf domain ID, em_perf_domain_get_by_id() returns NULL, and __em_nl_get_pd_size() immediately dereferences pd->cpus (struct offset 0x30), causing a NULL pointer dereference. The sister	N/A	More Details

31744	handler dev_energymodel_nl_get_perf_table_doit() already handles this correctly via __em_nl_get_pd_table_id(), which returns NULL and causes the caller to return -EINVAL. Add the same NULL check in the get-perf-domains do handler. [rjw: Subject and changelog edits]		
CVE-2026-31696	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix missing validation of ticket length in non-XDR key preparsing In rxrpc_preparse(), there are two paths for parsing key payloads: the XDR path (for large payloads) and the non-XDR path (for payloads <= 28 bytes). While the XDR path (rxrpc_preparse_xdr_rxkad()) correctly validates the ticket length against AFSTOKEN_RK_TIX_MAX, the non-XDR path fails to do so. This allows an unprivileged user to provide a very large ticket length. When this key is later read via rxrpc_read(), the total token size (toksize) calculation results in a value that exceeds AFSTOKEN_LENGTH_MAX, triggering a WARN_ON(). [2001.302904] WARNING: CPU: 2 PID: 2108 at net/rxrpc/key.c:778 rxrpc_read+0x109/0x5c0 [rxrpc] Fix this by adding a check in the non-XDR parsing path of rxrpc_preparse() to ensure the ticket length does not exceed AFSTOKEN_RK_TIX_MAX, bringing it into parity with the XDR parsing logic.	N/A	More Details
CVE-2026-31740	In the Linux kernel, the following vulnerability has been resolved: counter: rz-mtu3-cnt: do not use struct rz_mtu3_channel's dev member The counter driver can use HW channels 1 and 2, while the PWM driver can use HW channels 0, 1, 2, 3, 4, 6, 7. The dev member is assigned both by the counter driver and the PWM driver for channels 1 and 2, to their own struct device instance, overwriting the previous value. The sub-drivers race to assign their own struct device pointer to the same struct rz_mtu3_channel's dev member. The dev member of struct rz_mtu3_channel is used by the counter sub-driver for runtime PM. Depending on the probe order of the counter and PWM sub-drivers, the dev member may point to the wrong struct device instance, causing the counter sub-driver to do runtime PM actions on the wrong device. To fix this, use the parent pointer of the counter, which is assigned during probe to the correct struct device, not the struct device pointer inside the shared struct rz_mtu3_channel.	N/A	More Details
CVE-2026-31731	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Address thermal zone removal races with resume Since thermal_zone_pm_complete() and thermal_zone_device_resume() re-initialize the poll_queue delayed work for the given thermal zone, the cancel_delayed_work_sync() in thermal_zone_device_unregister() may miss some already running work items and the thermal zone may be freed prematurely [1]. There are two failing scenarios that both start with running thermal_pm_notify_complete() right before invoking thermal_zone_device_unregister() for one of the thermal zones. In the first scenario, there is a work item already running for the given thermal zone when thermal_pm_notify_complete() calls thermal_zone_pm_complete() for that thermal zone and it continues to run when thermal_zone_device_unregister() starts. Since the poll_queue delayed work has been re-initialized by thermal_pm_notify_complete(), the running work item will be missed by the cancel_delayed_work_sync() in thermal_zone_device_unregister() and if it continues to run past the freeing of the thermal zone object, a use-after-free will occur. In the second scenario, thermal_zone_device_resume() queued up by thermal_pm_notify_complete() runs right after the thermal_zone_exit() called by thermal_zone_device_unregister() has returned. The poll_queue delayed work is re-initialized by it before cancel_delayed_work_sync() is called by thermal_zone_device_unregister(), so it may continue to run after the freeing of the thermal zone object, which also leads to a use-after-free. Address the first failing scenario by ensuring that no thermal work items will be running when thermal_pm_notify_complete() is called. For this purpose, first move the cancel_delayed_work() call from thermal_zone_pm_complete() to thermal_zone_pm_prepare() to prevent new work from entering the workqueue going forward. Next, switch over to using a dedicated workqueue for thermal events and update the code in thermal_pm_notify() to flush that workqueue after thermal_pm_notify_prepare() has returned which will take care of all leftover thermal work already on the workqueue (that leftover work would do nothing useful anyway because all of the thermal zones have been flagged as suspended). The second failing scenario is addressed by adding a tz->state check to thermal_zone_device_resume() to prevent it from re-initializing the poll_queue delayed work if the thermal zone is going away. Note that the above changes will also facilitate relocating the suspend and resume of thermal zones closer to the suspend and resume of devices, respectively.	N/A	More Details
CVE-2026-31738	In the Linux kernel, the following vulnerability has been resolved: vxlan: validate ND option lengths in vxlan_na_create vxlan_na_create() walks ND options according to option-provided lengths. A malformed option can make the parser advance beyond the computed option span or use a too-short source LLADDR option payload. Validate option lengths against the remaining NS option area before advancing, and only read source LLADDR when the option is large enough for an Ethernet address.	N/A	More Details
CVE-2026-31737	In the Linux kernel, the following vulnerability has been resolved: net: ftgmac100: fix ring allocation unwind on open failure ftgmac100_alloc_rings() allocates rx_skbs, tx_skbs, rxdes, txdes, and rx_scratch in stages. On intermediate failures it returned -ENOMEM directly, leaking resources allocated earlier in the function. Rework the failure path to use staged local unwind labels and free allocated resources in reverse order before returning -ENOMEM. This matches common netdev allocation cleanup style.	N/A	More Details
CVE-2026-31736	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_ppe: avoid NULL deref when gmac0 is disabled If the gmac0 is disabled, the precheck for a valid ingress device will cause a NULL pointer deref and crash the system. This happens because eth->netdev[0] will be NULL but the code will directly try to access netdev_ops. Instead of just checking for the first net_device, it must be checked if any of the mtk_eth net_devices is matching the netdev_ops of the ingress device.	N/A	More Details
CVE-2026-31734	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix is_bpf_migration_disabled() false negative on non-PREEMPT_RCU Since commit 8e4f0b1ebcf2 ("bpf: use rcu_read_lock_dont_migrate() for trampoline.c"), the BPF prolog (__bpf_prog_enter) calls migrate_disable() only when CONFIG_PREEMPT_RCU is enabled, via rcu_read_lock_dont_migrate(). Without CONFIG_PREEMPT_RCU, the prolog never touches migration_disabled, so migration_disabled == 1 always means the task is truly migration-disabled regardless of whether it is the current task. The old unconditional p == current check was a false negative in this case, potentially allowing a migration-disabled task to be dispatched to a remote CPU and triggering scx_error in task_can_run_on_remote_rq(). Only apply the p == current disambiguation when CONFIG_PREEMPT_RCU is enabled, where the ambiguity with the BPF prolog still exists.	N/A	More Details
CVE-2026-31733	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix stale direct dispatch state in ddsp_dsq_id @p->scx.ddsp_dsq_id can be left set (non-SCX_DSQ_INVALID) triggering a spurious warning in mark_direct_dispatch() when the next wakeup's ops.select_cpu() calls scx_bpf_dsq_insert(), such as: WARNING: kernel/sched/ext.c:1273 at scx_dsq_insert_commit+0xcd/0x140 The root cause is that ddsp_dsq_id was only cleared in dispatch_enqueue(), which is not reached in all paths that consume or cancel a direct dispatch verdict. Fix it by clearing it at the right places: - direct_dispatch(): cache the direct dispatch state in local variables and clear it before dispatch_enqueue() on the synchronous path. For the deferred path, the direct dispatch state must remain set until process_ddsp_deferred_locals() consumes them. - process_ddsp_deferred_locals(): cache the dispatch state in local variables and clear it before calling dispatch_to_local_dsq(), which may migrate the task to another rq. - do_enqueue_task(): clear the dispatch state on the enqueue path (local/global/bypass fallbacks), where the direct dispatch verdict is ignored. - dequeue_task_scx(): clear the dispatch state after dispatch_dequeue() to handle both the deferred dispatch cancellation and the holding_cpu race, covering all cases where a pending direct dispatch is cancelled. - scx_disable_task(): clear the direct dispatch state when transitioning a task out of the current scheduler. Waking tasks may have had the direct dispatch state set by the outgoing scheduler's ops.select_cpu() and then been queued on a wake_list via ttwu_queue_wakelist(), when SCX_OPS_ALLOW_QUEUED_WAKEUP is set. Such tasks are not on the runqueue and are not iterated by scx_bypass(), so their direct dispatch state won't be cleared. Without this clear, any subsequent SCX scheduler that tries to direct dispatch the task will trigger the	N/A	More Details

	WARN_ON_ONCE() in mark_direct_dispatch().		
CVE-2026-31732	In the Linux kernel, the following vulnerability has been resolved: gpio: Fix resource leaks on errors in gpiochip_add_data_with_key() Since commit aab5c6f20023 ("gpio: set device type for GPIO chips"), `gdev->dev.release` is unset. As a result, the reference count to `gdev->dev` isn't dropped on the error handling paths. Drop the reference on errors. Also reorder the instructions to make the error handling simpler. Now gpiochip_add_data_with_key() roughly looks like: >>> Some memory allocation. Go to ERR ZONE 1 on errors. >>> device_initialize(). gpiodev_release() takes over the responsibility for freeing the resources of `gdev->dev`. The subsequent error handling paths shouldn't go through ERR ZONE 1 again which leads to double free. >>> Some initialization mainly on `gdev`. >>> The rest of initialization. Go to ERR ZONE 2 on errors. >>> Chip registration success and exit. >>> ERR ZONE 2. gpio_device_put() and exit. >>> ERR ZONE 1.	N/A	More Details
CVE-2026-43020	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: validate LTK enc_size on load Load Long Term Keys stores the user-provided enc_size and later uses it to size fixed-size stack operations when replying to LE LTK requests. An enc_size larger than the 16-byte key buffer can therefore overflow the reply stack buffer. Reject oversized enc_size values while validating the management LTK record so invalid keys never reach the stored key state.	N/A	More Details
CVE-2026-43021	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: fix leaks when hci_cmd_sync_queue_once fails When hci_cmd_sync_queue_once() returns with error, the destroy callback will not be called. Fix leaking references / memory on these failures.	N/A	More Details
CVE-2026-43022	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hci_cmd_sync_queue_once() return -EEXIST if exists hci_cmd_sync_queue_once() needs to indicate whether a queue item was added, so caller can know if callbacks are called, so it can avoid leaking resources. Change the function to return -EEXIST if queue item already exists. Modify all callsites to handle that.	N/A	More Details
CVE-2026-6501	Improper restriction of XML external entity reference vulnerability in ILM Informatique jOpenDocument allows Data Serialization External Entities Blowup. This issue affects jOpenDocument: 1.5.	N/A	More Details
CVE-2026-42226	n8n is an open source workflow automation platform. Prior to versions 1.123.33 and 2.17.5, the dynamic-node-parameters endpoints did not verify whether the authenticated caller was authorized to use a supplied credential reference. An authenticated user with access to a shared workflow could supply a foreign credential ID in the request body, causing the backend to decrypt and use that credential in a helper execution path where the caller also controls the destination URL. This allowed the caller to force the backend to authenticate against attacker-controlled infrastructure using a credential belonging to another user, effectively exfiltrating a reusable API key. The issue is not limited to any single node type; any node that resolves credentials dynamically through these endpoints may be affected. This issue has been patched in versions 1.123.33, 2.17.5, and 2.18.0.	N/A	More Details
CVE-2026-41686	Claude SDK for TypeScript provides access to the Claude API from server-side TypeScript or JavaScript applications. From version 0.79.0 to before version 0.91.1, the BetaLocalFilesystemMemoryTool in the Anthropic TypeScript SDK created memory files and directories using the Node.js default modes (0o666 for files, 0o777 for directories), leaving them world-readable on systems with a standard umask and world-writable in environments with a permissive umask such as many Docker base images. A local attacker on a shared host could read persisted agent state, and in containerized deployments could modify memory files to influence subsequent model behavior. This issue has been patched in version 0.91.1.	N/A	More Details
CVE-2026-42138	Dify is an open-source LLM app development platform. Prior to version 1.13.1, using the method POST /api/files/upload, any unauthenticated user can upload an SVG file with XSS. The method POST /v1/files/upload, which requires authentication through the application API, is also vulnerable. This issue has been patched in version 1.13.1.	N/A	More Details
CVE-2026-42052	Beets is the media library management system. Prior to version 2.10.0, the bundled web UI uses Underscore template interpolation mode <%= ... %> for untrusted metadata fields. In this runtime, <%= ... %> is raw insertion and HTML escaping is only performed by <%- ... %>. Rendered output is then inserted with .html(...), allowing attacker-controlled markup to become active DOM. This issue has been patched in version 2.10.0.	N/A	More Details
CVE-2026-2828	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-2026-6221	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-6500	Plaintext storage of a password vulnerability in ILM Informatique OpenConcerto allows Retrieve Embedded Sensitive Data. This issue affects OpenConcerto: 1.7.5.	N/A	More Details
CVE-2026-42228	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, the /chat WebSocket endpoint used by the Chat Trigger node's Hosted Chat feature did not verify that an incoming connection was authorized to interact with the target execution. An unauthenticated remote attacker who could identify a valid execution ID for a workflow in a waiting state could attach to that execution, receive the pending prompt intended for the legitimate user, and submit arbitrary input to resume or influence downstream workflow behavior. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2025-13605	3onedata modbus gateway device model GW1101-1D(RS-485)-TB-P (hardware version V2.2.0) allows authenticated users to execute arbitrary shell commands in the context of the root user by providing payload in the "IP address" field of the diagnosis test tools. This issue has been resolved in firmware version 3.0.59B2024080600R4353	N/A	More Details
CVE-2026-6499	Incorrect Permission Assignment for Critical Resource vulnerability in ILM Informatique OpenConcerto allows Replace Binaries. This issue affects OpenConcerto: 1.7.5.	N/A	More Details
CVE-2026-4928	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-2026-41226	Open redirect vulnerability exists in Multiple laser printers and MFPs which implement Ricoh Web Image Monitor. When accessing a specially crafted URL, the user may be redirected to an arbitrary website. As a result, the user may become a victim of a phishing attack.	N/A	More Details

CVE-2026-29200	A critical IDOR vulnerability has been discovered in Comet Backup affecting all versions from 20.11.0 to 26.1.1 and 26.2.1. The vulnerability allows a tenant administrator to impersonate any end-user account of other tenants on the same server via a vulnerable API call.	N/A	More Details
CVE-2026-6481	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-42227	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, an authenticated user with a valid API key scoped to variable:list could read variables from projects they are not a member of by supplying an arbitrary projectId query parameter to the public API variables endpoint. The handler queried the variables repository directly without enforcing project membership checks, bypassing the authorization-aware service layer used by the internal enterprise controller. If variables were misused to store sensitive information such as credentials or tokens, they should be rotated immediately. This issue only affects licensed enterprise or team deployments with multiple projects and the variables feature enabled. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42229	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, a flaw in the SeaTable node's row:search and row:get operations allowed user-controlled input to be concatenated directly into SQL query strings without escaping or parameterization. In workflows where external user input is passed via expressions into the SeaTable node's search or row retrieval parameters, an attacker could manipulate the constructed query to retrieve unintended rows from the connected SeaTable base, bypassing row-level filtering logic implemented in the workflow. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-31787	In the Linux kernel, the following vulnerability has been resolved: xen/privcmd: fix double free via VMA splitting privcmd_vm_ops defines .close (privcmd_close), but neither .may_split nor .open. When userspace does a partial munmap() on a privcmd mapping, the kernel splits the VMA via __split_vma(). Since may_split is NULL, the split is allowed. vm_area_dup() copies vm_private_data (a pages array allocated in alloc_empty_pages()) into the new VMA without any fixup, because there is no .open callback. Both VMAs now point to the same pages array. When the unmapped portion is closed, privcmd_close() calls: - xen_unmap_domain_gfn_range() - xen_free_unpopulated_pages() - kvfree(pages) The surviving VMA still holds the dangling pointer. When it is later destroyed, the same sequence runs again, which leads to a double free. Fix this issue by adding a .may_split callback denying the VMA split. This is XSA-487 / CVE-2026-31787	N/A	More Details
CVE-2026-34882	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2026-6074. Reason: This record is a reservation duplicate of CVE-2026-6074. Notes: All CVE users should reference CVE-2026-6074 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-41927	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains a stack-based buffer overflow vulnerability in the firewall.cgi and makeRequest.cgi binaries that allows unauthenticated attackers to overwrite the saved return address by sending a POST request with a Content-Length header exceeding 512 bytes. Attackers can exploit insufficient length validation in the fgets() call to achieve arbitrary code execution through return-oriented programming or return-to-libc techniques.	N/A	More Details
CVE-2026-41926	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains an OS command injection vulnerability in the firewall.cgi binary across five request handlers that apply insufficient input validation. Attackers can inject arbitrary shell commands through vulnerable parameters like websURLFilter, websHostFilter, portForward, singlePortForward, and ipportFilter using subshell syntax or unfiltered parameters, with payloads persisting in NVRAM and re-executing on every subsequent firewall.cgi request.	N/A	More Details
CVE-2026-41925	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains an OS command injection vulnerability in the adm.cgi binary's reboot_time function that allows unauthenticated remote attackers to execute arbitrary shell commands by injecting malicious input into the reboot_time POST parameter. Attackers can send a crafted request with shell metacharacters in the reboot_time parameter when reboot_enabled=1 to achieve remote code execution.	N/A	More Details
CVE-2026-41924	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains an OS command injection vulnerability in the makeRequest.cgi binary that allows unauthenticated remote attackers to execute arbitrary shell commands by injecting malicious input into the set_time or StartSniffer functions. Attackers can craft a POST request with specially crafted ampersand-delimited parameters to bypass input sanitization and execute commands with a maximum length of 31 bytes through the date command or channel parameter processing.	N/A	More Details
CVE-2026-41923	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains an OS command injection vulnerability in the internet.cgi binary that allows unauthenticated remote attackers to execute arbitrary shell commands by injecting malicious input into the gateway POST parameter. Attackers can exploit unsanitized parameter concatenation in the set_add_routing function to inject shell commands that are executed via popen() with partial output reflected in the HTTP response.	N/A	More Details
CVE-2026-41922	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains an OS command injection vulnerability in the wireless.cgi binary that allow unauthenticated remote attackers to execute arbitrary shell commands by injecting malicious input into the sz11gChannel or PIN POST parameters. Attackers can exploit unsanitized parameter handling in the set_wifi_basic and set_wifi_do_wps functions to achieve remote code execution without authentication.	N/A	More Details
CVE-2026-42237	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, the fix for GHSA-f3f2-mcxc-pwjx did not cover the Snowflake node or the legacy MySQL v1 node. Both nodes construct SQL queries by directly interpolating user-controlled table names, column names, and update keys into query strings without identifier escaping, enabling SQL injection against the connected database. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42230	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, the /mcp-oauth/register endpoint accepted OAuth client registrations without authentication, allowing arbitrary redirect_uri values to be registered. When a user denies the MCP OAuth consent dialog, the handleDeny handler redirects the user to the registered redirect_uri without validation, enabling an open redirect to an attacker-controlled URL. An attacker can craft a phishing link and send it to a victim; if the victim clicks "Deny" on the consent page, they are silently redirected to an external site. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42236	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, the MCP OAuth client registration endpoint accepted unauthenticated requests and stored client data without adequate resource controls. An unauthenticated remote attacker could exhaust server memory resources by sending large registration payloads, rendering the n8n instance unavailable. The MCP enable/disable toggle gates MCP access but did not restrict client registrations, meaning the endpoint is reachable regardless of whether MCP access is enabled on the instance. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details

CVE-2026-42235	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, an unauthenticated attacker could register a malicious MCP OAuth client with a crafted client_name. If a victim user authorized the OAuth consent dialog and a second user subsequently revoked that access, a toast notification would render the injected script. Clicking the link would execute arbitrary JavaScript in the victim's authenticated n8n browser session, enabling credential and session token theft, workflow manipulation, or privilege escalation. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42234	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, an authenticated user with permission to create or modify workflows containing a Python Code Node could escape the sandbox and achieve arbitrary code execution on the task runner container. This issue only affects instances where the Python Task Runner is enabled. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42233	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, a flaw in the Oracle Database node's select operation allowed user-controlled input passed into the Limit field via expressions to be interpolated directly into the SQL query without sanitization or parameterization. In workflows where external input is passed into the Limit field (e.g., from a webhook), an attacker could inject arbitrary SQL and exfiltrate data from the connected Oracle database. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42232	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, an authenticated user with permission to create or modify workflows could achieve global prototype pollution via the XML Node leading to RCE when combined with other nodes exploiting the prototype pollution. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-42231	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, a flaw in the xml2js library used to parse XML request bodies in n8n's webhook handler allowed prototype pollution via a crafted XML payload. An authenticated user with permission to create or modify workflows could exploit this to pollute the JavaScript object prototype and, by chaining the pollution with the Git node's SSH operations, achieve remote code execution on the n8n host. This issue has been patched in versions 1.123.32, 2.17.4, and 2.18.1.	N/A	More Details
CVE-2026-31692	In the Linux kernel, the following vulnerability has been resolved: rtnetlink: add missing netlink_ns_capable() check for peer netns rtnl_newlink() lacks a CAP_NET_ADMIN capability check on the peer network namespace when creating paired devices (veth, vxcan, netkit). This allows an unprivileged user with a user namespace to create interfaces in arbitrary network namespaces, including init_net. Add a netlink_ns_capable() check for CAP_NET_ADMIN in the peer namespace before allowing device creation to proceed.	N/A	More Details
CVE-2024-13971	Unauthenticated attackers can exploit a weakness in the XML parser functionality of Lobster_pro prior to version 4.12.6-GA. This allows them to obtain read access to files on the application server and adjacent network shares, and perform HTTP GET requests to arbitrary services.	N/A	More Details
CVE-2026-43024	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: reject immediate NF_QUEUE verdict nft_queue is always used from userspace nftables to deliver the NF_QUEUE verdict. Immediately emitting an NF_QUEUE verdict is never used by the userspace nft tools, so reject immediate NF_QUEUE verdicts. The arp family does not provide queue support, but such an immediate verdict is still reachable. Globally reject NF_QUEUE immediate verdicts to address this issue.	N/A	More Details
CVE-2026-43041	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: replace qrtr_tx_flow radix_tree with xarray to fix memory leak __radix_tree_create() allocates and links intermediate nodes into the tree one by one. If a subsequent allocation fails, the already-linked nodes remain in the tree with no corresponding leaf entry. These orphaned internal nodes are never reclaimed because radix_tree_for_each_slot() only visits slots containing leaf values. The radix_tree API is deprecated in favor of xarray. As suggested by Matthew Wilcox, migrate qrtr_tx_flow from radix_tree to xarray instead of fixing the radix_tree itself [1]. xarray properly handles cleanup of internal nodes — xa_destroy() frees all internal xarray nodes when the qrtr_node is released, preventing the leak. [1] https://lore.kernel.org/all/20260225071623.41275-1-jiayuan.chen@linux.dev/T/	N/A	More Details
CVE-2026-43052	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: check tdls flag in ieee80211_tdls_oper When NL80211_TDLS_ENABLE_LINK is called, the code only checks if the station exists but not whether it is actually a TDLS station. This allows the operation to proceed for non-TDLS stations, causing unintended side effects like modifying channel context and HT protection before failing. Add a check for sta->sta.tdls early in the ENABLE_LINK case, before any side effects occur, to ensure the operation is only allowed for actual TDLS peers.	N/A	More Details
CVE-2026-43050	In the Linux kernel, the following vulnerability has been resolved: atm: lec: fix use-after-free in sock_def_readable() A race condition exists between lec_atm_close() setting priv->lecd to NULL and concurrent access to priv->lecd in send_to_lecd(), lec_handle_bridge(), and lec_atm_send(). When the socket is freed via RCU while another thread is still using it, a use-after-free occurs in sock_def_readable() when accessing the socket's wait queue. The root cause is that lec_atm_close() clears priv->lecd without any synchronization, while callers dereference priv->lecd without any protection against concurrent teardown. Fix this by converting priv->lecd to an RCU-protected pointer: - Mark priv->lecd as __rcu in lec.h - Use rcu_assign_pointer() in lec_atm_close() and lecd_attach() for safe pointer assignment - Use rcu_access_pointer() for NULL checks that do not dereference the pointer in lec_start_xmit(), lec_push(), send_to_lecd() and lecd_attach() - Use rcu_read_lock/rcu_dereference/rcu_read_unlock in send_to_lecd(), lec_handle_bridge() and lec_atm_send() to safely access lecd - Use rcu_assign_pointer() followed by synchronize_rcu() in lec_atm_close() to ensure all readers have completed before proceeding. This is safe since lec_atm_close() is called from vcc_release() which holds lock_sock(), a sleeping lock. - Remove the manual sk_receive_queue drain from lec_atm_close() since vcc_destroy_socket() already drains it after lec_atm_close() returns. v2: Switch from spinlock + sock_hold/put approach to RCU to properly fix the race. The v1 spinlock approach had two issues pointed out by Eric Dumazet: 1. priv->lecd was still accessed directly after releasing the lock instead of using a local copy. 2. The spinlock did not prevent packets being queued after lec_atm_close() drains sk_receive_queue since timer and workqueue paths bypass netif_stop_queue(). Note: Syzbot patch testing was attempted but the test VM terminated unexpectedly with "Connection to localhost closed by remote host", likely due to a QEMU AHCI emulation issue unrelated to this fix. Compile testing with "make W=1 net/atm/lec.o" passes cleanly.	N/A	More Details
CVE-2026-43049	In the Linux kernel, the following vulnerability has been resolved: HID: logitech-hidpp: Prevent use-after-free on force feedback initialisation failure Presently, if the force feedback initialisation fails when probing the Logitech G920 Driving Force Racing Wheel for Xbox One, an error number will be returned and propagated before the userspace infrastructure (sysfs and /dev/input) has been torn down. If userspace ignores the errors and continues to use its references to these dangling entities, a UAF will promptly follow. We have 2 options; continue to return the error, but ensure that all of the infrastructure is torn down accordingly or continue to treat this condition as a warning by emitting the message but returning success. It is thought that the original author's intention was to emit the warning but keep the device functional, less the force feedback feature, so let's go with that.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: btrfs: reject root items with drop_progress and zero drop_level [BUG] When recovering relocation at mount time, merge_reloc_root() and btrfs_drop_snapshot() both use BUG_ON(level == 0) to guard against an impossible state: a non-zero drop_progress combined with a zero drop_level in a root_item, which can be triggered: -		

CVE-2026-43046	----------[cut here]---------- kernel BUG at fs/btrfs/relocation.c:1545! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 1 UID: 0 PID: 283 ... Tainted: 6.18.0+ #16 PREEMPT(voluntary) Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU Ubuntu 24.04 PC v2, BIOS 1.16.3-debian-1.16.3-2 RIP: 0010:merge_reloc_root+0x1266/0x1650 fs/btrfs/relocation.c:1545 Code: ffff0000 00004589 d7e9acfa ffffe8a1 79bafebe 02000000 Call Trace: merge_reloc_roots+0x295/0x890 fs/btrfs/relocation.c:1861 btrfs_recover_relocation+0xd6e/0x11d0 fs/btrfs/relocation.c:4195 btrfs_start_pre_rw_mount+0xa4d/0x1810 fs/btrfs/disk-io.c:3130 open_ctree+0x5824/0x5fe0 fs/btrfs/disk-io.c:3640 btrfs_fill_super fs/btrfs/super.c:987 [inline] btrfs_get_tree_super fs/btrfs/super.c:1951 [inline] btrfs_get_tree_subvol fs/btrfs/super.c:2094 [inline] btrfs_get_tree+0x111c/0x2190 fs/btrfs/super.c:2128 vfs_get_tree+0x9a/0x370 fs/super.c:1758 fc_mount fs/namespace.c:1199 [inline] do_new_mount_fc fs/namespace.c:3642 [inline] do_new_mount fs/namespace.c:3718 [inline] path_mount+0x5b8/0x1ea0 fs/namespace.c:4028 do_mount fs/namespace.c:4041 [inline] __do_sys_mount fs/namespace.c:4229 [inline] __se_sys_mount fs/namespace.c:4206 [inline] __x64_sys_mount+0x282/0x320 fs/namespace.c:4206 ... RIP: 0033:0x7f969c9a8fde Code: 0f1f4000 48c7c2b0 ffffffff d8648902 b8ffffff ffc3660f ---[end trace 0000000000000000]--- The bug is reproducible on 7.0.0-rc2-next-20260310 with our dynamic metadata fuzzing tool that corrupts btrfs metadata at runtime. [CAUSE] A non-zero drop_progress.objectid means an interrupted btrfs_drop_snapshot() left a resume point on disk, and in that case drop_level must be greater than 0 because the checkpoint is only saved at internal node levels. Although this invariant is enforced when the kernel writes the root item, it is not validated when the root item is read back from disk. That allows on-disk corruption to provide an invalid state with drop_progress.objectid != 0 and drop_level == 0. When relocation recovery later processes such a root item, merge_reloc_root() reads drop_level and hits BUG_ON(level == 0). The same invalid metadata can also trigger the corresponding BUG_ON() in btrfs_drop_snapshot(). [FIX] Fix this by validating the root_item invariant in tree-checker when reading root items from disk: if drop_progress.objectid is non-zero, drop_level must also be non-zero. Reject such malformed metadata with -EUCLEAN before it reaches merge_reloc_root() or btrfs_drop_snapshot() and triggers the BUG_ON. After the fix, the same corruption is correctly rejected by tree-checker and the BUG_ON is no longer triggered.	N/A	More Details
CVE-2026-43045	In the Linux kernel, the following vulnerability has been resolved: mshv: Fix error handling in mshv_region_pin The current error handling has two issues: First, pin_user_pages_fast() can return a short pin count (less than requested but greater than zero) when it cannot pin all requested pages. This is treated as success, leading to partially pinned regions being used, which causes memory corruption. Second, when an error occurs mid-loop, already pinned pages from the current batch are not properly accounted for before calling mshv_region_invalidate_pages(), causing a page reference leak. Treat short pins as errors and fix partial batch accounting before cleanup.	N/A	More Details
CVE-2026-43043	In the Linux kernel, the following vulnerability has been resolved: crypto: af-alg - fix NULL pointer dereference in scatterwalk The AF_ALG interface fails to unmark the end of a Scatter/Gather List (SGL) when chaining a new af_alg_tsgl structure. If a sendmsg() fills an SGL exactly to MAX_SGL_ENTS, the last entry is marked as the end. A subsequent sendmsg() allocates a new SGL and chains it, but fails to clear the end marker on the previous SGL's last data entry. This causes the crypto scatterwalk to hit a premature end, returning NULL on sg_next() and leading to a kernel panic during dereference. Fix this by explicitly unmarking the end of the previous SGL when performing sg_chain() in af_alg_alloc_tsgl().	N/A	More Details
CVE-2026-43040	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: ndisc: fix ndisc_ra_useropt to initialize nduseropt_padX fields to zero to prevent an info-leak When processing Router Advertisements with user options the kernel builds an RTM_NEWNDUSEROPT netlink message. The nduseroptmsg struct has three padding fields that are never zeroed and can leak kernel data The fix is simple, just zeroes the padding fields.	N/A	More Details
CVE-2026-43054	In the Linux kernel, the following vulnerability has been resolved: scsi: target: tcm_loop: Drain commands in target_reset handler tcm_loop_target_reset() violates the SCSI EH contract: it returns SUCCESS without draining any in-flight commands. The SCSI EH documentation (scsi_eh.rst) requires that when a reset handler returns SUCCESS the driver has made lower layers "forget about timed out scmds" and is ready for new commands. Every other SCSI LLD (virtio_scsi, mpt3sas, ipr, scsi_debug, mpi3mr) enforces this by draining or completing outstanding commands before returning SUCCESS. Because tcm_loop_target_reset() doesn't drain, the SCSI EH reuses in-flight scsi_cmnd structures for recovery commands (e.g. TUR) while the target core still has async completion work queued for the old se_cmd. The memset in queuecommand zeroes se_lun and lun_ref_active, causing transport_lun_remove_cmd() to skip its percpu_ref_put(). The leaked LUN reference prevents transport_clear_lun_ref() from completing, hanging configfs LUN unlink forever in D-state: INFO: task rm:264 blocked for more than 122 seconds. rm D 0 264 258 0x00004000 Call Trace: __schedule+0x3d0/0x8e0 schedule+0x36/0xf0 transport_clear_lun_ref+0x78/0x90 [target_core_mod] core_tpg_remove_lun+0x28/0xb0 [target_core_mod] target_fabric_port_unlink+0x50/0x60 [target_core_mod] configfs_unlink+0x156/0x1f0 [configfs] vfs_unlink+0x109/0x290 do_unlinkat+0x1d5/0x2d0 Fix this by making tcm_loop_target_reset() actually drain commands: 1. Issue TMR_LUN_RESET via tcm_loop_issue_tmr() to drain all commands that the target core knows about (those not yet CMD_T_COMPLETE). 2. Use blk_mq_tagset_busy_iter() to iterate all started requests and flush_work() on each se_cmd — this drains any deferred completion work for commands that already had CMD_T_COMPLETE set before the TMR (which the TMR skips via __target_check_io_state()). This is the same pattern used by mpi3mr, scsi_debug, and libsas to drain outstanding commands during reset.	N/A	More Details
CVE-2026-43036	In the Linux kernel, the following vulnerability has been resolved: net: use skb_header_pointer() for TCPv4 GSO frag_off check Syzbot reported a KMSAN uninit-value warning in gso_features_check() called from netif_skb_features() [1]. gso_features_check() reads iph->frag_off to decide whether to clear mangleid_features. Accessing the IPv4 header via ip_hdr()/inner_ip_hdr() can rely on skb header offsets that are not always safe for direct dereference on packets injected from PF_PACKET paths. Use skb_header_pointer() for the TCPv4 frag_off check so the header read is robust whether data is already linear or needs copying. [1] https://syzkaller.appspot.com/bug?extid=1543a7d954d9c6d00407	N/A	More Details
CVE-2026-43035	In the Linux kernel, the following vulnerability has been resolved: net: sched: cls_api: fix tc_chain_fill_node to initialize tcm_info to zero to prevent an info-leak When building netlink messages, tc_chain_fill_node() never initializes the tcm_info field of struct tcmsg. Since the allocation is not zeroed, kernel heap memory is leaked to userspace through this 4-byte field. The fix simply zeroes tcm_info alongside the other fields that are already initialized.	N/A	More Details
CVE-2026-43034	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: set backing store type from query type bnxt_hwrm_func_backing_store_qcaps_v2() stores resp->type from the firmware response in ctxm->type and later uses that value to index fixed backing-store metadata arrays such as ctx_arr[] and bnxt_bstore_to_trace[]. ctxm->type is fixed by the current backing-store query type and matches the array index of ctx->ctx_arr. Set ctxm->type from the current loop variable instead of depending on resp->type. Also update the loop to advance type from next_valid_type in the for statement, which keeps the control flow simpler for non-valid and unchanged entries.	N/A	More Details
CVE-2026-43032	In the Linux kernel, the following vulnerability has been resolved: NFC: pn533: bound the UART receive buffer pn532_receive_buf() appends every incoming byte to dev->recv_skb and only resets the buffer after pn532_uart_rx_is_frame() recognizes a complete frame. A continuous stream of bytes without a valid PN532 frame header therefore keeps growing the skb until skb_put_u8() hits the tail limit. Drop the accumulated partial frame once the fixed receive buffer is full so malformed UART traffic cannot grow the skb past	N/A	More Details

	PN532_UART_SKB_BUFF_LEN.		
CVE-2026-43027	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_helper: pass helper to expect cleanup nf_conntrack_helper_unregister() calls nf_ct_expect_iterate_destroy() to remove expectations belonging to the helper being unregistered. However, it passes NULL instead of the helper pointer as the data argument, so expect_iter_me() never matches any expectation and all of them survive the cleanup. After unregister returns, nfnl_cthelper_del() frees the helper object immediately. Subsequent expectation dumps or packet-driven init_conntrack() calls then dereference the freed exp->helper, causing a use-after-free. Pass the actual helper pointer so expectations referencing it are properly destroyed before the helper object is freed. BUG: KASAN: slab-use-after-free in string+0x38f/0x430 Read of size 1 at addr ffff888003b14d20 by task poc/103 Call Trace: string+0x38f/0x430 vsnprintf+0x3cc/0x1170 seq_printf+0x17a/0x240 exp_seq_show+0x2e5/0x560 seq_read_iter+0x419/0x1280 proc_reg_read+0x1ac/0x270 vfs_read+0x179/0x930 ksys_read+0xef/0x1c0 Freed by task 103: The buggy address is located 32 bytes inside of freed 192-byte region [ffff888003b14d00, ffff888003b14dc0)	N/A	More Details
CVE-2026-43026	In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: zero expect NAT fields when CTA_EXPECT_NAT absent ctnetlink_alloc_expect() allocates expectations from a non-zeroing slab cache via nf_ct_expect_alloc(). When CTA_EXPECT_NAT is not present in the netlink message, saved_addr and saved_proto are never initialized. Stale data from a previous slab occupant can then be dumped to userspace by ctnetlink_exp_dump_expect(), which checks these fields to decide whether to emit CTA_EXPECT_NAT. The safe sibling nf_ct_expect_init(), used by the packet path, explicitly zeroes these fields. Zero saved_addr, saved_proto and dir in the else branch, guarded by IS_ENABLED(CONFIG_NF_NAT) since these fields only exist when NAT is enabled. Confirmed by priming the expect slab with NAT-bearing expectations, freeing them, creating a new expectation without CTA_EXPECT_NAT, and observing that the ctnetlink dump emits a spurious CTA_EXPECT_NAT containing stale data from the prior allocation.	N/A	More Details
CVE-2026-43053	In the Linux kernel, the following vulnerability has been resolved: xfs: close crash window in attr dabtree inactivation When inactivating an inode with node-format extended attributes, xfs_attr3_node_inactive() invalidates all child leaf/node blocks via xfs_trans_binval(), but intentionally does not remove the corresponding entries from their parent node blocks. The implicit assumption is that xfs_attr_inactive() will truncate the entire attr fork to zero extents afterwards, so log recovery will never reach the root node and follow those stale pointers. However, if a log shutdown occurs after the leaf/node block cancellations commit but before the attr bmap truncation commits, this assumption breaks. Recovery replays the attr bmap intact (the inode still has attr fork extents), but suppresses replay of all cancelled leaf/node blocks, maybe leaving them as stale data on disk. On the next mount, xlog_recover_process_iunlinks() retries inactivation and attempts to read the root node via the attr bmap. If the root node was not replayed, reading the unreplayed root block triggers a metadata verification failure immediately; if it was replayed, following its child pointers to unreplayed child blocks triggers the same failure: XFS (pmem0): Metadata corruption detected at xfs_da3_node_read_verify+0x53/0x220, xfs_da3_node block 0x78 XFS (pmem0): Unmount and run xfs_repair XFS (pmem0): First 128 bytes of corrupted metadata buffer: 00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... XFS (pmem0): metadata I/O error in "xfs_da_read_buf+0x104/0x190" at daddr 0x78 len 8 error 117 Fix this in two places: In xfs_attr3_node_inactive(), after calling xfs_trans_binval() on a child block, immediately remove the entry that references it from the parent node in the same transaction. This eliminates the window where the parent holds a pointer to a cancelled block. Once all children are removed, the now-empty root node is converted to a leaf block within the same transaction. This node-to-leaf conversion is necessary for crash safety. If the system shutdown after the empty node is written to the log but before the second-phase bmap truncation commits, log recovery will attempt to verify the root block on disk. xfs_da3_node_verify() does not permit a node block with count == 0; such a block will fail verification and trigger a metadata corruption shutdown. on the other hand, leaf blocks are allowed to have this transient state. In xfs_attr_inactive(), split the attr fork truncation into two explicit phases. First, truncate all extents beyond the root block (the child extents whose parent references have already been removed above). Second, invalidate the root block and truncate the attr bmap to zero in a single transaction. The two operations in the second phase must be atomic: as long as the attr bmap has any non-zero length, recovery can follow it to the root block, so the root block invalidation must commit together with the bmap-to-zero truncation.	N/A	More Details
CVE-2025-8903	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-2052. Reason: This candidate is a reservation duplicate of CVE-2026-2052 Notes: All CVE users should reference CVE-2026-2052 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-43058	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: fix pass-by-value structs causing MSAN warnings vidtv_ts_null_write_into() and vidtv_ts_pcr_write_into() take their argument structs by value, causing MSAN to report uninit-value warnings. While only vidtv_ts_null_write_into() has triggered a report so far, both functions share the same issue. Fix by passing both structs by const pointer instead, avoiding the stack copy of the struct along with its MSAN shadow and origin metadata. The functions do not modify the structs, which is enforced by the const qualifier.	N/A	More Details
CVE-2026-34996	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-13890	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-12494. Reason: This candidate is a reservation duplicate of CVE-2025-12494. Notes: All CVE users should reference CVE-2025-12494 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-51847	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-51849	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-51850	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-34994	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE-2026-34995	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-34997	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-12993	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-67968. Reason: This candidate is a reservation duplicate of CVE-2025-67968. Notes: All CVE users should reference CVE-2025-67968 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-34998	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-42788	Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated memory exhaustion via oversized HTTP/2 frames. 'Elixir.Bandit.HTTP2.Frame':deserialize/2 in lib/bandit/http2/frame.ex checks the SETTINGS_MAX_FRAME_SIZE limit only after pattern-matching payload::binary-size(length), which requires the entire frame body to be present in memory before either the accept or reject clause can fire. A peer that announces a frame length up to the 24-bit maximum (~16 MiB) causes the server to buffer that entire body before the size guard is evaluated, regardless of the max_frame_size negotiated during the HTTP/2 handshake (default 16 KiB per RFC 9113). An unauthenticated attacker holding many concurrent connections can force the server to buffer far more memory than the negotiated frame size limit should permit, leading to memory pressure and potential denial of service. This issue affects bandit: from 0.3.6 before 1.11.0.	N/A	More Details
CVE-2026-42786	Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated remote denial of service via memory exhaustion. The fragment reassembly path in 'Elixir.Bandit.WebSocket.Connection':handle_frame/3 in lib/bandit/websocket/connection.ex appends every incoming Continuation{fin: false} frame's payload to a per-connection iolist with no cumulative size cap. The existing max_frame_size option only bounds individual frames; a peer that streams an unbounded number of continuation frames without ever setting fin=1 grows BEAM heap linearly until the OS or a supervisor kills the process. Because the accumulation happens before WebSock.handle_in/2 is called, the application has no opportunity to interpose a size check. Phoenix Channels and LiveView both run over WebSock on Bandit, so a stock Phoenix application exposes this surface as soon as it accepts socket connections. This issue affects bandit: from 0.5.0 before 1.11.0.	N/A	More Details
CVE-2026-39807	Reliance on Untrusted Inputs in a Security Decision vulnerability in mtrudel bandit allows unauthenticated transport-state spoofing on plaintext HTTP connections. 'Elixir.Bandit.Pipeline':determine_scheme/2 in lib/bandit/pipeline.ex returns the client-supplied URI scheme verbatim, ignoring the transport's secure? flag. HTTP/1.1 absolute-form request targets (e.g. GET https://victim/path HTTP/1.1) and the HTTP/2 :scheme pseudo-header are both attacker-controlled strings that flow through this function. Over a plaintext TCP connection, a client can declare https and Bandit will set conn.scheme = :https even though no TLS was negotiated. Downstream Plug consumers that branch on conn.scheme are silently misled: Plug.SSL's already-secure branch skips its HTTP→HTTPS redirect, cookies emitted with secure: true are sent over plaintext, audit logs record requests as having arrived over HTTPS, and CSRF/SameSite gating may make incorrect decisions. This issue affects bandit: from 1.0.0 before 1.11.0.	N/A	More Details
CVE-2026-39805	Inconsistent Interpretation of HTTP Requests vulnerability in mtrudel bandit allows HTTP request smuggling via duplicate Content-Length headers. 'Elixir.Bandit.Headers':get_content_length/1 in lib/bandit/headers.ex uses List.keyfind/3, which returns only the first matching header. When a request contains two Content-Length headers with different values, Bandit silently accepts it, uses the first value to read the body, and dispatches the remaining bytes as a second pipelined request on the same keep-alive connection. RFC 9112 §6.3 requires recipients to treat this as an unrecoverable framing error. When Bandit sits behind a proxy that picks the last Content-Length value and forwards the request rather than rejecting it, an unauthenticated attacker can smuggle requests past edge WAF rules, path-based ACLs, rate limiting, and audit logging. This issue affects bandit: before 1.11.0.	N/A	More Details
CVE-2026-39804	Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated remote denial of service via memory exhaustion when WebSocket permessage-deflate compression is enabled. 'Elixir.Bandit.WebSocket.PerMessageDeflate':inflate/2 in lib/bandit/websocket/permessage_deflate.ex calls :zlib.inflate/2 with no output-size cap, then materializes the entire decompressed payload as a single binary via IO.iodata_to_binary/1. The websocket_options.max_frame_size option only bounds the on-the-wire (compressed) frame size, not the decompressed output. A high-ratio compressed frame (e.g. uniform data at ~1024:1 ratio) can stay well under any wire-size limit while forcing GiB-scale heap allocations in the connection process before any application code runs. An unauthenticated attacker who can open a WebSocket connection can send a single such frame to exhaust the BEAM node's memory and trigger an OOM kill. This vulnerability requires both Bandit's server-level websocket_options.compress and the per-upgrade compress: true option passed to WebSockAdapter.upgrade/4 to be enabled. Stock Phoenix and LiveView applications are not affected as they default to compress: false. This issue affects bandit: from 0.5.9 before 1.11.0.	N/A	More Details
CVE-2026-40934	Jupyter Server is the backend for Jupyter web applications. In versions 2.17.0 and earlier, the secret used to sign authentication cookies is persisted to a static file at ~/.local/share/jupyter/runtime/jupyter_cookie_secret and is never rotated when a user changes their password. After a password reset and server restart, any previously issued authentication cookie remains cryptographically valid because the signing key has not changed. An attacker who has captured a session cookie through any means retains full authenticated access to the server regardless of subsequent password changes. This affects deployments using password-based authentication, particularly shared or public-facing servers where credential rotation is expected to revoke existing sessions. This issue has been fixed in version 2.18.0.	N/A	More Details