SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 May 2026

Generated on 27 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-2026-42901	Origin validation error in Microsoft Entra ID allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-34909	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in UniFi OS devices to access files on the underlying system that could be manipulated to access an underlying account.	10.0	More Details
CVE-2026-47280	Improper authentication in Azure Resource Manager (ARM) allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-41104	Deserialization of untrusted data in Microsoft Planetary Computer Pro allows an unauthorized attacker to disclose information over a network.	10.0	More Details
CVE-2026-40412	Unrestricted upload of file with dangerous type in Azure Orbital Spatio allows an unauthorized attacker to execute code over a network.	10.0	More Details
CVE-2026-23652	Improper neutralization of special elements used in a command ('command injection') in Microsoft Power Pages allows an unauthorized attacker to execute code over a network.	10.0	More Details
CVE-2026-33712	Typebot is a chatbot builder tool. In versions 3.15.2 and prior, the preview chat endpoint (POST /api/v1/typebots/{typebotId}/preview/startChat) allows unauthenticated users to achieve Server-Side Request Forgery (SSRF) by supplying a custom typebot definition with server-side code blocks. The fetch function exposed inside the isolated-vm sandbox calls Node.js native fetch without the SSRF validation (validateHttpReqUrl) that protects the HTTP Request block. This bypasses all SSRF mitigations added after GHSA-8gq9-rw7v-3jpr. Exploitation of this unauthenticated SSRF vulnerability can lead to cloud credential theft, internal network access and data exfiltration for any self-hosted Typebot deployments and hosted services. This issue has been fixed in version 3.16.0.	10.0	More Details
CVE-2026-39821	The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".	10.0	More Details
CVE-2026-46595	Previously, CVE-2024-45337 fixed an authorization bypass for misused ssh server configurations; if any other type of callback is passed other than public key, then the source-address validation would be skipped.	10.0	More Details
CVE-2026-34910	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi OS devices to execute a Command Injection.	10.0	More Details
CVE-2026-34908	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi OS devices to make unauthorized changes to the system.	10.0	More Details
CVE-2026-42960	NLnet Labs Unbound up to and including version 1.25.0 is vulnerable to poisoning via promiscuous records for the authority section. Promiscuous RRSets that complement DNS replies in the authority section can be used to trick Unbound to cache such records. If an adversary is able to attach such records in a reply (i.e., spoofed packet, fragmentation attack) he would be able to poison Unbound's cache. A malicious actor can exploit the possible poisonous effect by injecting RRSets other than NS that are also accompanied by address records in a reply, for example MX. This could be achieved by trying to spoof a reply packet or fragmentation attacks. Unbound would then accept the relative address records in the additional section and cache them if the authority RRSet has enough trust at this point, i.e., in-zone data for the delegation point. Unbound 1.25.1 contains a patch with a fix that disregards address records from the additional section if they are not explicitly relevant only to authority NS records, mitigating the possible poison effect. This is a complement fix to CVE-2025-11411.	10.0	More Details
	A vulnerability in the access validation of internal REST APIs of Cisco Secure Workload could allow an unauthenticated,		

CVE-2026-20223	remote attacker to access site resources with the privileges of the Site Admin role. This vulnerability is due to insufficient validation and authentication when accessing REST API endpoints. An attacker could exploit this vulnerability if they are able to send a crafted API request to an affected endpoint. A successful exploit could allow the attacker to read sensitive information and make configuration changes across tenant boundaries with the privileges of the Site Admin user.	10.0	More Details
CVE-2026-45444	Unrestricted Upload of File with Dangerous Type vulnerability in WP Swings Gift Cards For WooCommerce Pro allows Using Malicious Files. This issue affects Gift Cards For WooCommerce Pro: from n/a through 4.2.6.	10.0	More Details
CVE-2026-40411	Improper input validation in Azure Virtual Network Gateway allows an authorized attacker to execute code over a network.	9.9	More Details
CVE-2026-44450	Lumiverse is a full-featured AI chat application. Prior to 0.9.7, the MCP server creation endpoint validates the command field against an allowlist of binary names but forwards the args array to the child process without any validation. Every binary on the allowlist accepts an inline-code execution flag (-e for node/bun, -c for python3/deno), giving any logged-in user arbitrary OS-level code execution on the Lumiverse server. The route requires only requireAuth (not requireOwner). The server binds on all interfaces (::) and the host-header rebinding check is bypassed trivially by any HTTP client that sends Host: localhost:<port> directly, making this exploitable from any machine with network access to the server port. This vulnerability is fixed in 0.9.7.	9.9	More Details
CVE-2026-44050	A heap-based buffer overflow in the CNID daemon comm_rcv() function in Netatalk 2.0.0 through 4.4.2 allows a remote authenticated attacker to execute arbitrary code with escalated privileges or cause a denial of service.	9.9	More Details
CVE-2026-7374	A flaw was found in KubeVirt's virt-handler component. This vulnerability allows an authenticated OpenShift user with edit permissions in a single namespace to exploit improper symlink validation when connecting to virtual machine console sockets. By replacing the console socket with a symlink to the host's container runtime (CRI-O) socket, an attacker can hijack virt-handler's privileged connection. This enables the attacker to access any Unix socket on the host, potentially leading to full control of the node and the entire cluster.	9.9	More Details
CVE-2026-46624	Twenty is an open source CRM. From 1.7.7 through 1.16.7, a critical Remote Code Execution (RCE) vulnerability exists in Twenty CRM via a chained SQL Injection and PostgreSQL COPY TO PROGRAM attack. If Postgres user is a super user then any authenticated user can execute arbitrary OS commands on the database server by injecting SQL through the unsanitized timeZone parameter in the REST API groupBy endpoint. The timeZone field within the group_by query parameter is directly interpolated into a raw SQL expression using JavaScript template literals without any parameterization, validation, or escaping. This affects engine/api/graphql/graphql-query-runner/group-by/resolvers/utils/get-group-by-expression.util.ts.	9.9	More Details
CVE-2026-9432	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setWiFiAdvancedCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument bgProtection results in os command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-9408	A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. Affected by this issue is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument enable results in os command injection. The attack may be performed from remote. The exploit is now public and may be used.	9.8	More Details
CVE-2026-7251	Eppendorf BioFlo 320 is vulnerable to due to VNC server using a hard-coded password. If a remote attacker knows the network address of any BioFlo 320 model with remote access enabled, they can gain full control of the user interface by using this password. Once connected, the attacker would have full access to all control panel features for the BioFlo 320. VNC traffic is not encrypted.	9.8	More Details
CVE-2026-9407	A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. Affected by this vulnerability is the function setFirewallType of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument firewallType leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-8633	IBM Web Server Plug-ins for WebSphere Application Server and WebSphere Liberty 8.5, 9.0 IBM WebSphere Application Server and WebSphere Application Server Liberty are vulnerable to remote code execution in the Web Server Plug-ins, through a specially crafted request.	9.8	More Details
CVE-2026-44668	FACTION is a PenTesting Report Generation and Collaboration Framework. Prior to 1.8.3, AccessControlInterceptor, the authentication gate for all Struts2 actions, unconditionally calls invocation.invoke() without checking for a valid session. Four action methods in BoilerPlateConfig perform no local session check either, allowing an unauthenticated attacker to read, overwrite, deactivate, and permanently delete any boilerplate template in the system. This vulnerability is fixed in 1.8.3.	9.8	More Details
CVE-2026-9406	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function setRemoteCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument enable can lead to os command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-9434	A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setWiFiWpsCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument wscDisabled leads to os command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-3660	IBM Engineering Lifecycle Management 7.0.3, 7.1.0, and 7.2.0 could allow an unauthenticated remote attacker to update server property files that would allow them to gain unauthorized access to the application.	9.8	More Details
CVE-2026-9405	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This impacts the function setGameSpeedCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument enable results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-48689	FastNetMon Community Edition through 1.2.9 contains an off-by-one heap-based buffer overflow in the dynamic_binary_buffer_t class (src/dynamic_binary_buffer.hpp). Five methods (append_dynamic_buffer, append_data_as_pointer, append_data_as_object_ptr, memcpy_from_ptr, memcpy_from_object_ptr) use an incorrect bounds check of the form 'if (offset + length > maximum_internal_storage_size + 1)' instead of the correct 'if (offset + length > maximum_internal_storage_size)'. This allows writing exactly one byte past the end of the heap-allocated buffer. The class is used pervasively in BGP message encoding/decoding, NetFlow template processing, and Flow Spec NLRI construction. An attacker who can send network traffic (NetFlow, sFlow, IPFIX, or BGP) to a FastNetMon instance can trigger this overflow, potentially achieving arbitrary code	9.8	More Details

	execution by corrupting heap metadata. Notably, the append_byte() method uses the correct bounds check, confirming the inconsistency.		
CVE-2026-9404	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setDdnsCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument provider leads to os command injection. The attack may be launched remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-9388	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setScheduleCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument mode can lead to os command injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-9387	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function setUpgradeFW of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument resetFlags results in os command injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-9433	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setMacFilterRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument enable causes os command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-9436	A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setL2tpServerCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument enable can lead to os command injection. The attack can be executed remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2026-9435	A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function setQosCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument enable results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	9.8	More Details
CVE-2026-48904	An improper access check allows privelege escalation through the com_users group editing webservice endpoint.	9.8	More Details
CVE-2026-48899	An improper access check allows privilege escalation through the com_users batch task.	9.8	More Details
CVE-2026-48898	An improper access check allows privilege escalation through the com_users batch task.	9.8	More Details
CVE-2026-48686	FastNetMon Community Edition through 1.2.9 contains a stack-based buffer overflow in the BGP NLRI (Network Layer Reachability Information) decoder. The function decode_bgp_subnet_encoding_ipv4_raw() in src/bgp_protocol.cpp reads prefix_bit_length directly from the BGP packet (line 99) without validating it is <= 32 for IPv4 prefixes. This value is passed to how_much_bytes_we_need_for_storing_certain_subnet_mask() which computes ceil(prefix_bit_length / 8), returning up to 32 bytes for a prefix_bit_length of 255. The result is used as the length argument to memcpy() (line 106), which copies into a 4-byte uint32_t stack variable (prefix_ipv4). This causes a stack buffer overflow of up to 28 bytes, which can be exploited for arbitrary code execution. Additionally, the unvalidated prefix_bit_length is passed to convert_cidr_to_binary_netmask_local_function_copy() (line 111), where a shift of (32 - cidr) with cidr > 32 causes undefined behavior.	9.8	More Details
CVE-2026-45247	Mirasvit Full Page Cache Warmer for Magento 2 before version 1.11.12 contains a PHP object injection vulnerability that allows unauthenticated attackers to achieve remote code execution by supplying a crafted serialized PHP object in the CacheWarmer cookie. Attackers can exploit the unrestricted call to PHP's native unserialize() function combined with gadget chains available in Magento and its dependencies to execute arbitrary code on the server.	9.8	More Details
CVE-2026-9543	A vulnerability has been found in Totolink N300RH 6.1c.1353_B20190305. Affected is the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument admpass leads to os command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-9478	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setParentalRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument enable can lead to os command injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-9477	A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setAccessDeviceCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument mac 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.	9.8	More Details
CVE-2026-9476	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument admpass leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-9475	A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setIpQosRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument Comment causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-9458	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setWanCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument enabled leads to os command injection. The attack may be performed from remote. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-9457	A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument FileName causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-9385	A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument command causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be	9.8	More Details

	utilized.		
CVE-2026-9456	A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setOpenVpnCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument enabled results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-9455	A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function UploadOpenVpnCert of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument FileName leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-9454	A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setOpenVpnCertGenerationCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument servername can lead to os command injection. The attack may be launched remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2026-9386	A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument lang leads to os command injection. The attack may be performed from remote. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-6555	The ProSolution WP Client plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to, and including, 2.0.0. This is due to an array validation mismatch where only the first file in the upload array undergoes extension and MIME type validation, while all files are processed and uploaded to a web-accessible directory. This makes it possible for unauthenticated attackers to upload malicious PHP files and achieve remote code execution by sending a valid first file followed by a malicious file.	9.8	More Details
CVE-2026-9384	A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument ip results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-6960	The BookingPress Pro plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'bookingpress_validate_submitted_booking_form_func' function in all versions up to, and including, 5.6. 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 signature custom field is added to the booking form.	9.8	More Details
CVE-2026-24207	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause an authentication bypass. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, or information disclosure.	9.8	More Details
CVE-2026-7637	The Boost plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 2.0.3 via deserialization of untrusted input in the STYXKEY-BOOST_USER_LOCATION cookie. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	9.8	More Details
CVE-2026-33278	NLnet Labs Unbound 1.19.1 up to and including version 1.25.0 has a vulnerability in the DNSSEC validator that enables denial of service and possible remote code execution as a result of deep copying a data structure and erroneously overwriting a destination pointer. An adversary can exploit the vulnerability by controlling a malicious signed zone and querying a vulnerable Unbound. When DS sub-queries need to suspend validation due to NSEC3 computational budget exhaustion (introduced in Unbound 1.19.1), Unbound deep-copies response messages to preserve them across memory region teardown. A struct-assignment bug overwrites the destination's pointer with the source's pointer. After the sub-query region is freed, the resumed validator dereferences this dangling pointer, triggering a crash or potentially enabling arbitrary code execution. Unbound 1.25.1 contains a patch with a fix to preserve the correct pointer when deep copying the data structure.	9.8	More Details
CVE-2026-9082	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Drupal core allows SQL Injection. This issue affects Drupal core: from 8.9.0 before 10.4.10, from 10.5.0 before 10.5.10, from 10.6.0 before 10.6.9, from 11.0.0 before 11.1.10, from 11.2.0 before 11.2.12, from 11.3.0 before 11.3.10.	9.8	More Details
CVE-2026-9139	Taiko AG1000-01A SMS Alert Gateway Rev 7.3 and Rev 8 contains a hard-coded credential vulnerability in the embedded web configuration interface where authentication is implemented entirely in client-side JavaScript in login.zhtml, exposing static plaintext credentials in the page source. Unauthenticated attackers with network access can recover administrative credentials directly from the client-side validate() function to obtain full administrative access to the device.	9.8	More Details
CVE-2026-9141	Taiko AG1000-01A SMS Alert Gateway Rev 7.3 and Rev 8 contains an authentication bypass vulnerability in the embedded web configuration interface that allows unauthenticated attackers to access internal application pages without any session management or server-side authentication checks. Attackers with network access can directly request internal resources such as index.zhtml, point.zhtml, and log.shtml to gain full administrative read and write access, enabling unauthorized modification of alarm routing, device configuration, and disruption of monitoring and control functions.	9.8	More Details
CVE-2026-8631	A potential security vulnerability has been identified in the HP Linux Imaging and Printing Software. This potential vulnerability may allow escalation of privileges and/or arbitrary code execution via an integer overflow in the hpcups processing path when handling crafted print data.	9.8	More Details
CVE-2026-48172	LiteSpeed User-End cPanel Plugin before 2.4.5 allows privilege escalation (possibly to root), as exploited in the wild in May 2026. Detection is best done via a command line of grep -rE "cpanel_jsonapi_func=redisAble" /var/cpanel/logs /usr/local/cpanel/logs/ 2>/dev/null in Bash. If you get no output, you have not been hit with exploitation of the vulnerability. If there is output, we recommend you examine the IP addresses in the list, determine if they are valid IP addresses, and if not, block them. To determine damage done, examine the system logs for use by the detected IP addresses. The issue is related to mishandling of Redis enable/disable features. The recommended minimum version is 2.4.7.	9.8	More Details
CVE-2026-6279	The Avada Builder (fusion-builder) plugin for WordPress is vulnerable to Unauthenticated Remote Code Execution via PHP Function Injection in versions up to and including 3.15.2. This is due to the `wp_conditional_tags` case in `Fusion_Builder_Conditional_Render_Helper::get_value()` passing attacker-controlled values from a base64-decoded JSON blob directly to `call_user_func()` without any allowlist validation. This is exploitable by unauthenticated attackers through the `fusion_get_widget_markup` AJAX endpoint, which is registered for non-privileged (unauthenticated) users via `wp_ajax_nopriv_fusion_get_widget_markup`. The endpoint is protected only by a nonce (`fusion_load_nonce`), but this nonce	9.8	More Details

	is generated for user ID 0 and is deterministically exposed in the JavaScript output of any public-facing page containing a Post Cards (`[fusion_post_cards]`) or Table of Contents (`[fusion_table_of_contents]`) element. This makes it possible for unauthenticated attackers to execute arbitrary code on affected sites.		
CVE-2026-5118	The Divi Form Builder plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.1.2. This is due to the plugin accepting a user-controlled 'role' parameter from POST data during user registration without validating it against the form's configured default_user_role setting. This makes it possible for unauthenticated attackers to create administrator accounts by tampering with the role parameter during registration.	9.8	More Details
CVE-2018-25357	Dolibarr ERP CRM 7.0.3 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary code by injecting PHP code through the db_name parameter. Attackers can send a POST request to install/step1.php with malicious PHP code in the db_name parameter, then execute commands via the check.php endpoint using the cmd GET parameter.	9.8	More Details
CVE-2025-71211	A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations. This vulnerability is similar in scope to CVE-2025-71210 but affects a different executable. Please note: although this vulnerability carries a technical critical CVSS rating, this was reported via responsible disclosure via a researcher through the Zero Day Initiative. The SaaS versions of the product have already been mitigated and no customer action required. For this particular vulnerability, an attacker must have access to the Trend Micro Apex One Management Console, so customers that have their console's IP address exposed externally should consider mitigating factors such as source restrictions if not already applied.	9.8	More Details
CVE-2026-48207	Deserialization of untrusted data in Apache Fory PyFory. PyFory's ReduceSerializer could bypass documented DeserializationPolicy validation hooks during reduce-state restoration and global-name resolution. An application is vulnerable if it deserializes attacker-controlled data using PyFory Python-native mode with strict mode disabled and relies on DeserializationPolicy to restrict unsafe classes, functions, or module attributes. This issue affects Apache Fory: from before 1.0.0. Mitigation: Users of Apache Fory are recommended to upgrade to version 1.0.0 or later, which enforces DeserializationPolicy validation for the affected ReduceSerializer paths and thus fixes this issue.	9.8	More Details
CVE-2025-71210	A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations. Please note: although this vulnerability carries a technical critical CVSS rating, this was reported via responsible disclosure via a researcher through the Zero Day Initiative. The SaaS versions of the product have already been mitigated and no customer action required. For this particular vulnerability, an attacker must have access to the Trend Micro Apex One Management Console, so customers that have their console's IP address exposed externally should consider mitigating factors such as source restrictions if not already applied.	9.8	More Details
CVE-2026-9642	There is a mitigation bypass / (incomplete fix) for CVE-2025-62582 (Unauthenticated Remote Database Access) An unauthenticated remote attacker can access configured databases in a DIAView project.	9.8	More Details
CVE-2026-32253	Sunshine is a self-hosted game stream host for Moonlight. In versions prior to 2026.516.143833, the client-certificate authentication can be bypassed because of how OpenSSL verification results are handled. In src/crypto.cpp, the custom verify callback treats X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY, X509_V_ERR_CERT_NOT_YET_VALID, and X509_V_ERR_CERT_HAS_EXPIRED as success. This can allow an untrusted certificate to pass authentication and access protected HTTPS endpoints. This issue has been fixed in version 2026.516.143833.	9.8	More Details
CVE-2018-25350	userSpice 4.3.24 contains a username enumeration vulnerability that allows unauthenticated attackers to discover valid usernames by sending POST requests to the existingUsernameCheck.php endpoint. Attackers can submit usernames and analyze response text for the 'taken' string to identify existing accounts in the system.	9.8	More Details
CVE-2026-7284	The Easy Elements for Elementor – Addons & Website Templates plugin for WordPress is vulnerable to privilege escalation via user registration in all versions up to, and including, 1.4.4. This is due to the 'easyel_handle_register' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2026-44930	An LDAP injection vulnerability in the LDAP Certificate repository of the XKMS server in Apache CXF may allow an attacker to retrieve arbitrary certificates from the repository. Users are recommended to upgrade to versions 4.2.1, 4.1.6 or 3.6.11, which fix this issue.	9.8	More Details
CVE-2026-8670	Insufficient session expiration vulnerability in syslink software AG Avantra on Linux, Windows allows Reusing Session IDs (aka Session Replay). This issue affects Avantra: before 25.3.1.	9.6	More Details
CVE-2026-44451	Lumiverse is a full-featured AI chat application. Prior to 0.9.7, the component override system transpiles user-supplied TSX via Sucrase and evaluates it with new Function, shadowing dangerous globals (fetch, window, eval, etc.) with undefined. A static source validator (validateComponentOverrideSource) additionally blocks these identifiers by word-boundary regex. Both controls are bypassed. String-split bypass of the static validator: any blocked identifier can be reconstructed at runtime from string fragments ('ownerDoc' + 'ument'). DOM ref escape from the sandbox: useRef and useEffect are provided in scope. A ref attached to a rendered element gives a live DOM node. From any real DOM node, node['ownerDoc'+'ument']['def'+'aultView'] yields the real window, bypassing all identifier shadows. Theme packs (.lumitheme / .lumiverse-theme) are the shareable delivery mechanism. A malicious pack is an exploit path: the victim imports the file, enables one component override in the Theme Editor, and the payload fires in their authenticated session.This vulnerability is fixed in 0.9.7.	9.3	More Details
CVE-2026-39531	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wp Directory Kit WP Directory Kit allows Blind SQL Injection. This issue affects WP Directory Kit: from n/a through 1.5.0.	9.3	More Details
CVE-2026-42773	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in eMagicOne eMagicOne Store Manager allows Blind SQL Injection. This issue affects eMagicOne Store Manager: from n/a through 1.3.2.	9.3	More Details
CVE-2026-42774	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crocoblock JetEngine allows SQL Injection. This issue affects JetEngine: from n/a through 3.8.8.1.	9.3	More Details
CVE-2026-41090	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to perform tampering over a network.	9.3	More Details
CVE-2026-9264	A cross-site scripting (XSS) vulnerability in SketchUp 2026's Dynamic Components feature allows remote code execution and local file exfiltration through maliciously crafted SKP files. The vulnerability stems from improper input sanitization in the component options window, enabling attackers to execute arbitrary system commands and read local files without user interaction by exploiting an embedded Internet Explorer 11 browser.	9.3	More Details

CVE-2026-44449	Lumiverse is a full-featured AI chat application. Prior to 0.9.7, when the primary toSmbPath(fullPath) call throws, the method falls back to a dirname/basename split and only validates the directory prefix. The basename is concatenated directly into the smbclient -c script without validation. smbclient interprets ; as a subcommand separator and !cmd as a local-shell escape that runs cmd on the host. A path whose directory component is clean but whose basename contains "; !<cmd>; echo " achieves arbitrary command execution on the Lumiverse server. This vulnerability is fixed in 0.9.7.	9.1	More Details
CVE-2026-44444	Lumiverse is a full-featured AI chat application. Prior to 0.9.7, the Spindle extension build pipeline calls bun install without the --ignore-scripts flag before running the static backend safety scan (assertSafeBackendBundle). A malicious extension that ships a package.json with a preinstall, postinstall, or prepare lifecycle script achieves host-level code execution the moment an admin presses Install before any dist file is inspected. This vulnerability is fixed in 0.9.7.	9.1	More Details
CVE-2026-8598	An undocumented configuration export port is accessible on some models of ZKTeco CCTV cameras. This port does not require authentication and exposes critical information about the camera such as open services and camera account credentials.	9.1	More Details
CVE-2026-33843	Authentication bypass using an alternate path or channel in Microsoft Azure Active Directory B2C allows an unauthorized attacker to elevate privileges over a network.	9.1	More Details
CVE-2026-33000	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi OS devices to execute a Command Injection.	9.1	More Details
CVE-2026-42508	Previously, a revoked 'SignatureKey' belonging to a CA was not correctly checked for revocation. Now, both the 'key' and 'key.SignatureKey' are checked for @revoked.	9.1	More Details
CVE-2026-39834	When writing data larger than 4GB in a single Write call on an SSH channel, an integer overflow in the internal payload size calculation caused the write loop to spin indefinitely, sending empty packets without making progress. The size comparison now uses int64 to prevent truncation.	9.1	More Details
CVE-2026-5433	Honeywell Control Network Module (CNM) contains command injection vulnerability in the web interface. An attacker could exploit this vulnerability via command delimiters, potentially resulting in Remote Code Execution (RCE).	9.1	More Details
CVE-2026-39833	The in-memory keyring returned by NewKeyring() silently accepted keys with the ConfirmBeforeUse constraint but never enforced it. The key would sign without any confirmation prompt, with no indication to the caller that the constraint was not in effect. NewKeyring() now returns an error when unsupported constraints are requested.	9.1	More Details
CVE-2026-39832	When adding a key to a remote agent constraint extensions such as restrict-destination-v00@openssh.com were not serialized in the request. Destination restrictions were silently stripped when forwarding keys, allowing unrestricted use of the key on the remote host. The client now serializes all constraint extensions. Additionally, the in-memory keyring returned by NewKeyring() now rejects keys with unsupported constraint extensions instead of silently ignoring them.	9.1	More Details
CVE-2026-39831	The Verify() method for FIDO/U2F security key types (sk-ecdsa-sha2-nistp256@openssh.com, sk-ssh-ed25519@openssh.com) did not check the User Presence flag. Signatures generated without physical touch were accepted, allowing unattended use of a hardware security key. To restore the previous behavior, return a "no-touch-required" extension in Permissions.Extensions from PublicKeyCallback.	9.1	More Details
CVE-2026-39830	A malicious SSH peer could send unsolicited global request responses to fill an internal buffer, blocking the connection's read loop. The blocked goroutine could not be released by calling Close(), resulting in a resource leak per connection. Unsolicited global responses are now discarded.	9.1	More Details
CVE-2026-47372	Crypt::SaltedHash versions through 0.09 for Perl generate insecure random values for salts. These versions use the built-in rand function, which is predictable and unsuitable for cryptography.	9.1	More Details
CVE-2026-45721	Algernon is a small self-contained pure-Go web server. Prior to 1.17.7, when Algernon is asked for any URL path that resolves to a directory without an index file, DirPage walks upward through parent directories — past the configured server root — looking for a file named handler.lua to execute as the request handler. The loop terminates only after 100 ancestor steps or when filepath.Dir returns ., so on any absolute server-root path the search reaches the filesystem root (/ on Unix, drive letter on Windows). The first handler.lua it finds is loaded into the Lua interpreter with the full Algernon API exposed — including run3(), httpclient, os.execute, io.popen, PQ, MSSQL, raw filesystem access, and the userstate database. Any process that can write handler.lua anywhere in a parent directory of the server root obtains pre-authenticated remote code execution on the next HTTP request. This is reachable without authentication — the lookup happens before the permission check returns a hit (the perm system only gates URL prefixes, not the handler-resolution step), and any URL pointing at a directory without an index triggers the walk. On a fresh stock Algernon install the request GET / is enough. This vulnerability is fixed in 1.17.7.	9.0	More Details
CVE-2026-22314	Improper Control of Generation of Code ('Code Injection') vulnerability in Mesalvo Meona Client Launcher Component, Mesalvo Meona Server Component enables code execution on other users' systems. This issue affects Meona Client Launcher Component: through 19.06.2020 15:11:49; Meona Server Component: through 2025.04 5+323020.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	
CVE-2026-47101	LiteLLM prior to 1.83.14 allows an authenticated internal_user to create API keys with access to routes that their role does not permit. When generating a key, the a access controls that would otherwise block the request, enabling full privilege escalation from internal_user to proxy_admin.
CVE-2026-8421	Concrete CMS 9.5.0 and below contains a CSRF vulnerability in the install_package() method of concrete/controllers/single_page/dashboard/extend/install.php. An protection. Package installation executes the package controller's install() method as the web server user, enabling remote code execution. In order to be vulneral https://github.com/maru1009 for reporting.
CVE-2026-24217	NVIDIA BioNeMo Core for Linux contains a vulnerability where a user could cause a path traversal by loading a malicious file. A successful exploit of this vulnerabili
CVE-2026-9431	A vulnerability was identified in Tenda F1202 1.2.0.20(408). This affects the function fromPptpUserAdd of the file /goform/PptpUserAdd. The manipulation of the ar

CVE-2026-9430	A vulnerability was determined in Tenda F1202 1.2.0.20(408). Affected by this issue is the function formGstDhcpSetSer of the file /goform/GstDhcpSetSerof. Execut
CVE-2026-8409	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/logs/delete. The The Concrete CMS security team ga
CVE-2026-8410	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/logs/bulk/delete. The The Concrete CMS security tea
CVE-2026-9429	A vulnerability was found in Tenda F1202 1.2.0.20(408). Affected by this vulnerability is the function formWrlExtraSet of the file /goform/WrlExtraSet. Performing a
CVE-2026-8411	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/page/bulk/delete. The Concrete CMS security team g
CVE-2026-5200	The AcyMailing – An Ultimate Newsletter Plugin and Marketing Automation Solution for WordPress plugin for WordPress is vulnerable to Missing Authorization in ver privileged AcyMailing configuration, export subscriber secret keys, and chain these actions into administrator account takeover when a target administrator email a
CVE-2026-8412	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/page/bulk/cache. The Concrete CMS security team ga
CVE-2026-8413	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/page/bulk/design. The Concrete CMS security team g
CVE-2026-9462	A vulnerability was detected in Edimax EW-7438RPn 1.31. Affected by this vulnerability is the function formWpsProxyEnable of the file /goform/formWpsProxyEnabl respond in any way.
CVE-2026-9428	A vulnerability has been found in Tenda F1202 1.2.0.20(408). Affected is the function fromPPTPUserSetting of the file /goform/PPTPUserSetting. Such manipulation
CVE-2026-9427	A flaw has been found in Edimax EW-7438RPn 1.31. This impacts the function formWlSiteSurvey of the file /goform/formWlSiteSurvey of the component webs. This disclosure but did not respond in any way.
CVE-2026-9463	A flaw has been found in Edimax EW-7438RPn 1.31. Affected by this issue is the function formLicence of the file /goform/formLicence. This manipulation of the argu
CVE-2026-8414	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/event/duplicate. The Concrete CMS security team ga
CVE-2026-9426	A vulnerability was detected in Edimax EW-7438RPn 1.31. This affects the function formHwSet of the file /goform/formHwSet. The manipulation of the argument Ar The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-8415	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/dialog/express/association/reorder. The Concrete CMS secu
CVE-2026-7522	The Advanced Database Cleaner – Premium plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 4.1.0 via the 'template' paran access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.
CVE-2026-8416	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/backend/file addFavoriteFolder($id). The Concrete CMS secu
CVE-2026-8427	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/backend/file removeFavoriteFolder($id). The Concrete CMS
CVE-2026-8432	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/backend/file star(). The Concrete CMS security team gave th
CVE-2026-9295	A security flaw has been discovered in Edimax BR-6428NS 1.10. This affects the function formWirelessTbl of the file /goform/formWirelessTbl of the component POS early about this disclosure but did not respond in any way.
CVE-2026-6406	The Docker CLI --use-api-socket flag bypasses Enhanced Container Isolation (ECI) restrictions in Docker Desktop. When ECI is enabled, Docker socket mounts from enforcement in the Docker Desktop API proxy only inspected Binds, allowing the mount to pass unchecked. This grants a container full access to the Docker Engine potentially escalate privileges.
CVE-2026-9294	A vulnerability was identified in Edimax BR-6428NS 1.10. The impacted element is the function formWanTcpipSetup of the file /goform/formWanTcpipSetup of the c about this disclosure but did not respond in any way.
CVE-	

2026-9461	A security vulnerability has been detected in Edimax EW-7438RPn 1.31. Affected is the function formRadius of the file /goform/formRadius. The manipulation of the way.
CVE-2026-35430	Authorization bypass through user-controlled key in Azure Privileged Identity Management (PIM) allows an authorized attacker to elevate privileges over a network
CVE-2026-24425	Twig versions 2.16.x and 3.9.0 through 3.25.x contain a sandbox bypass vulnerability when using a SourcePolicyInterface that allows attackers with template rende the sandbox is enabled through a source policy rather than globally.
CVE-2026-8426	Concrete CMS 9.5.0 and below does not validate a CSRF token before processing requests to /dashboard/extend/update/prepare_remote_upgrade/<remoteMPID>. execution as the web server user. In order to be vulnerable, the victim must be passing canInstallPackages, victim site must be connected to the Concrete marke vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N. Thanks https://github.com/maru1009 for reporting.
CVE-2026-8428	Concrete CMS 9.5.0 and below emits a CSRF token in the local_available_update.php view ($token->output('do_update')) but the corresponding do_update() metho discards it without verification, an attacker can craft a cross-site POST that triggers a core CMS update to an attacker-specified version string. In order to be vulne vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N. Thanks https://github.com/maru1009 for reporting.
CVE-2026-8350	Concrete CMS 9.5.0 and below is vulnerable to missing authorization in the bulk_user_assignment.php which can lead to privilege escalation to Administrative Grou with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N. Thanks Vincent55 for reporting.
CVE-2026-8676	An attacker is able to downgrade the security of a Bluetooth LE connection by deleting an existing bond, spoofing the bonded device and creating a new bond.
CVE-2026-45659	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.
CVE-2026-6419	The WishList Member plugin for WordPress is vulnerable to Privilege Escalation via Missing Authorization in versions up to and including 3.30.1. This is due to the m causing the plugin to load and execute the administrative API configuration template without authorization. The rendered HTML, which contains the plugin's plainte role, and register an arbitrary administrator-level user account, resulting in complete site takeover.
CVE-2026-6895	The WishList Member plugin for WordPress is vulnerable to Missing Authorization leading to Sensitive Information Disclosure and Privilege Escalation in versions up authenticate to the WishList Member API, create a new membership level assigned the administrator WordPress role, and register an arbitrary administrator-level u
CVE-2026-9460	A weakness has been identified in Edimax EW-7438RPn 1.31. This impacts the function formAccept of the file /goform/formAccept. Executing a manipulation of the disclosure but did not respond in any way.
CVE-2026-6898	The Wishlist Member plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'WishListMember3_Hooks::ge membership level assigned the administrator WordPress role, and register an arbitrary administrator-level user account, resulting in complete site takeover.
CVE-2026-9459	A security flaw has been discovered in Edimax EW-7438RPn 1.31. This affects the function formConnectionSetting of the file /goform/formConnectionSetting. Perfo contacted early about this disclosure but did not respond in any way.
CVE-2026-41075	RT is an open source, enterprise-grade issue and ticket tracking system. Versions 5.0.0 through 5.0.9 and 6.0.0 through 6.0.2 contain an SQL injection vulnerability developers are unable to upgrade immediately, they can temporarily work around this issue by restricting RT account access to trusted users.
CVE-2026-47102	LiteLLM prior to 1.83.10 allows a user to modify their own user_role via the /user/update endpoint. While the endpoint correctly restricts users to updating only thei history. Users with the org_admin role have legitimate access to this endpoint and can exploit this vulnerability without chaining any additional flaw.
CVE-2026-47114	IINA before 1.4.3 contains a user-assisted command execution vulnerability that allows remote attackers to execute arbitrary commands by supplying malicious m arbitrary command execution as the current macOS user upon approval of the browser protocol prompt without requiring a valid media file.
CVE-2026-9443	A security vulnerability has been detected in Edimax BR-6478AC 1.23. This vulnerability affects the function formL2TPSetup of the file /goform/formL2TPSetup of th early about this disclosure but did not respond in any way.
CVE-2026-44925	Cross-Site Request Forgery (CSRF) vulnerability in InfoScale v.9.1.3 Operations Manager (VIOM) allows an attacker to force the user with an active session into click
CVE-2026-44926	InfoScale CmdServer before 7.4.2 mishandles access control.
CVE-2026-6897	The Wishlist Member plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'WishListMember\Features\Te Key, which can be used to create a new membership level assigned the administrator WordPress role, and register an arbitrary administrator-level user account, re
CVE-2026-9442	A weakness has been identified in Edimax BR-6478AC 1.23. This affects the function formiNICSiteSurvey of the file /goform/formiNICSiteSurvey of the component P contacted early about this disclosure but did not respond in any way.
CVE-2026-9425	A security vulnerability has been detected in Edimax EW-7438RPn 1.31. The impacted element is the function formWlanMP of the file /goform/formWlanMP. The ma ateFunc/ateGain/ateTxCount/ateChan/ateRate/ateMacID/e2pTxPower1/e2pTxPower2/e2pTxPower3/e2pTxPower4/e2pTxPower5/e2pTxPower6/e2pTxPower7/e2pTx2 leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was conta
CVE-	

2026-8433	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/backend/file rescan(). The Concrete CMS security team gav
CVE-2026-9089	The ConnectWise Automate™ Agent does not fully verify the authenticity of components obtained during plugin loading and self-update operations. This issue is ac
CVE-2026-46368	luci-app-https-dns-proxy through 2025.12.29-5 — an optional LuCI web UI add-on for the https-dns-proxy package, distributed through the OpenWrt community pa parameter of a ubus RPC call to luci.https-dns-proxy setInitAction, resulting in arbitrary command execution as root on the underlying device. Core OpenWrt is not
CVE-2026-24187	NVIDIA Display Driver for Linux contains a vulnerability where an attacker could cause a use-after-free. A successful exploit of this vulnerability might lead to denia
CVE-2026-40033	FreeRDP before 3.26.0 contains a heap-buffer-overflow vulnerability in gdi_CacheToSurface that allows remote attackers to write out-of-bounds heap memory. The potentially achieve remote code execution or client crash.
CVE-2026-6456	The Account Switcher plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.2. This is due to the `rememberLogin` REST `asSecret` user meta does not exist, causing `get_user_meta()` to return an empty string. An attacker can send an empty `secret` parameter, which passes the co authenticated attackers, with Subscriber-level access and above, to switch to any user account including Administrator, ultimately granting themselves full adminis
CVE-2026-9018	The Easy Elements for Elementor – Addons & Website Templates plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.4.5 meta via `update_user_meta()` without any key whitelist or blocklist, allowing the `wp_capabilities` user meta key to be overwritten after `wp_insert_user()` has a user registration is enabled on the site and that at least one page exposes the Login/Register widget, which publishes the required `easy_elements_nonce` into the
CVE-2026-9346	A flaw has been found in Edimax EW-7438RPn up to 1.31. This impacts the function formWirelessTbl of the file /goform/formWirelessTbl of the component webs. Ex respond in any way.
CVE-2026-9393	A vulnerability was found in H3C Magic B0 up to 100R002. This affects the function Edit_BasicSSID_5G of the file /goform/aspForm. Performing a manipulation of th
CVE-2026-9389	A security vulnerability has been detected in Tenda F456 1.0.0.5. This affects the function frmL7ImForm of the file /goform/L7Im. The manipulation of the argumen
CVE-2026-9348	A vulnerability was found in Edimax EW-7438RPn up to 1.31. Affected by this vulnerability is an unknown functionality of the file /goform/mp of the component web did not respond in any way.
CVE-2026-9382	A flaw has been found in Edimax BR-6675nD 1.12. Affected by this issue is the function formPPTPSetup of the file /goform/formPPTPSetup of the component POST R disclosure but did not respond in any way.
CVE-2026-9345	A vulnerability was detected in Edimax EW-7438RPn up to 1.31. This affects the function formWizSurvey of the file /goform/formWizSurvey of the component webs this disclosure but did not respond in any way.
CVE-2026-9381	A vulnerability was detected in Edimax BR-6675nD 1.12. Affected by this vulnerability is the function formPPPoESetup of the file /goform/formPPPoESetup of the co this disclosure but did not respond in any way.
CVE-2026-44047	An SQL injection vulnerability in the MySQL CNID backend in Netatalk 3.1.0 through 4.4.2 allows a remote authenticated attacker to obtain unauthorized access to
CVE-2026-45216	Incorrect Privilege Assignment vulnerability in StoreApps Smart Manager allows Privilege Escalation. This issue affects Smart Manager: from n/a through 8.85.0.
CVE-2026-8992	An improper certificate validation vulnerability in Ivanti Secure Access Client before 22.8R6 allows a remote unauthenticated attacker to execute arbitrary code.
CVE-2026-44048	A stack-based buffer overflow via UCS-2 type confusion in convert_charset() in Netatalk 2.0.4 through 4.4.2 allows a remote authenticated attacker to execute arbi
CVE-2026-9380	A security vulnerability has been detected in Edimax BR-6675nD 1.12. Affected is the function formL2TPSetup of the file /goform/formL2TPSetup of the component this disclosure but did not respond in any way.
CVE-2026-9360	A security flaw has been discovered in Edimax EW-7438RPn 1.28a. Affected by this issue is the function formwlencrypt24g of the file /goform/formwlencrypt24g of contacted early about this disclosure but did not respond in any way.
CVE-2026-39461	libcasper(3) communicates with helper processes via UNIX domain sockets, and uses the select(2) system call to wait for data to become available. However, it doe executing a program which is not careful to close them upon startup, may trigger stack corruption. If the target application runs with setuid root privileges, this cou
CVE-2026-7467	The Read More & Accordion plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.5.7. This is due to the 'RadMoreAjax::im the plugin's role settings, to insert arbitrary rows into the 'wp_users' and 'wp_usermeta' tables, including the 'wp_capabilities' field, allowing them to create a new a
CVE-2026-	Concrete CMS 9.5.0 and below does not validate a CSRF token before processing requests to /dashboard/extend/update/do_update/<pkgHandle>. The do_update() GET route with no token enforcement, an attacker can force an authenticated administrator to trigger a package upgrade via a single cross-site navigation.In order

8417	vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N. Thanks https://github.com/maru1009 for reporting.
CVE-2026-9399	A vulnerability was detected in Edimax BR-6675nD 1.12. This vulnerability affects the function formsetPPPoE of the file /goform/formsetPPPoE of the component PO disclosure but did not respond in any way.
CVE-2026-9481	A flaw has been found in Edimax EW-7438RPn 1.31. This affects the function formStats of the file /goform/formStats. This manipulation of the argument submit-url
CVE-2026-8434	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/backend/file rescanMultiple(). The Concrete CMS security te
CVE-2026-9111	Use after free in WebRTC in Google Chrome on Linux prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chrom
CVE-2026-9112	Use after free in GPU in Google Chrome on Windows prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HT
CVE-2026-9114	Use after free in QUIC in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via malicious network tra
CVE-2018-25353	Redaxo CMS Mediapool Addon 5.5.1 and older contains an arbitrary file upload vulnerability that allows authenticated users to bypass file extension blacklist restric
CVE-2026-9118	Use after free in XR in Google Chrome on Windows prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromiu
CVE-2026-9119	Heap buffer overflow in WebRTC in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted H
CVE-2026-9120	Use after free in WebRTC in Google Chrome prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium secu
CVE-2026-9479	A security vulnerability has been detected in Edimax EW-7438RPn 1.31. The affected element is the function formLogout of the file /goform/formLogout. The manip not respond in any way.
CVE-2026-9344	A security vulnerability has been detected in Edimax EW-7438RPn up to 1.31. The impacted element is an unknown function of the file /goform/formWpsStart of the early about this disclosure but did not respond in any way.
CVE-2026-9480	A vulnerability was detected in Edimax EW-7438RPn 1.31. The impacted element is the function formrefresh of the file /goform/formrefresh. The manipulation of th
CVE-2026-9482	A vulnerability has been found in Edimax EW-7438RPn 1.31. This impacts the function formSDHCP of the file /goform/formSDHCP. Such manipulation of the argume
CVE-2026-9121	Out of bounds read in GPU in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2026-9403	A vulnerability was determined in Edimax BR-6675nD 1.12. The impacted element is the function formWlSiteSurvey of the file /goform/formWlSiteSurvey of the cor this disclosure but did not respond in any way.
CVE-2026-9401	A vulnerability has been found in Edimax BR-6675nD 1.12. Impacted is the function formWanTcpipSetup of the file /goform/formWanTcpipSetup of the component this disclosure but did not respond in any way.
CVE-2026-9126	Use after free in DOM in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2026-44832	Snipe-IT is an IT asset/license management system. Prior to 8.4.1, aAn authenticated user with only users.edit permission can escalate their own privileges to admi update users. This vulnerability is fixed in 8.4.1.
CVE-2026-44667	FACTION is a PenTesting Report Generation and Collaboration Framework. Prior to 1.8.3, Faction is vulnerable to stored cross-site scripting (XSS) via attachment fil browser of any user who opens the affected verification/remediation views. Because the payload is stored server-side and rendered to other users, exploitation is p
CVE-2026-44729	Twenty is an open source CRM. In 1.18.0 and earlier, the file serving endpoints in Twenty CRM at /files/* and /file/:fileFolder/:id serve uploaded files using fileStream browser in the context of the Twenty CRM domain when accessed — enabling session hijacking, account takeover, and data theft.
CVE-2026-	authentik is an open-source identity provider. Versions 2025.12.4 and prior, and versions 2026.2.0-rc1 through 2026.2.2 were vulnerable to Authentication Bypass attacker to gain access to other accounts. This issue could be exploited on an authentik instance with a SAML Source, where the attacker had an account on the SA

40165	which effectively truncated the NameID value to the snippet before the comment, and gave the attacker access to any user account. This issue has been fixed in v
CVE-2026-41147	NukeViet CMS is a multi Content Management System. Versions 4.5.07 and prior contain a Stored Cross-Site Scripting (XSS) vulnerability caused by insufficient ser directly (e.g., using Burp Suite). An attacker can inject malicious payloads which are stored server-side and executed in the browser of any user who views the con Contact module used only as a proof of concept. Potential consequences include session hijacking through cookie theft, unauthorized actions performed under the this issue by implementing server-side HTML sanitization in the Request class to strip or encode dangerous tags and attributes (e.g., <iframe>, srcdoc, event hand
CVE-2026-28445	Typebot is a chatbot builder tool. In versions 3.15.2 and prior, the RatingButton component in the embed package renders the user-controlled customIcon.svg field import sanitizer and the builder preview renders bots inline on the builder's own origin (builder.typebot.io) under a CSP permitting 'unsafe-inline', a malicious impo within the builder application. This issue has been fixed in version 3.16.0.
CVE-2026-44669	FACTION is a PenTesting Report Generation and Collaboration Framework. Prior to 1.8.3, Faction is vulnerable to stored cross-site scripting (XSS) via attachment fil who views the affected page. Because the payload is stored server-side and rendered to other users, exploitation is persistent and can impact privileged accounts.
CVE-2026-45298	Dozzle is a realtime log viewer for docker containers. Prior to 10.5.2, in a default dozzle deploy (the documented quickstart, no DOZZLE_AUTH_PROVIDER set), POS the response status code AND up to 1MB of the response body to the caller, when the target replies non-2xx. This vulnerability is fixed in 10.5.2.
CVE-2026-39310	Trilium Notes is a cross-platform, hierarchical note taking application focused on building large personal knowledge bases. In versions 0.102.1 and prior, the Clippe endpoints such as /api/clipper/notes to the network with no password, API token, or CSRF protection. An attacker on a shared network (for example, a corporate LA bypasses authentication, confirms a Trilium instance by returning the application name and protocol version. This facilitates unauthorized data access, phishing, ar
CVE-2026-44706	Chatwoot is a customer engagement suite. From 2.2.0 to before 4.11.2, a SQL injection vulnerability exists in the conversation and contact filter APIs. When filterin authenticated user with access to an account can exploit this to execute arbitrary SQL via time-based blind injection. This affects /api/v1/accounts/{account_id}/co
CVE-2026-4480	A flaw was found in the Samba printing subsystem. Samba passes the client-controlled job description string to the command configured with the "print command" lead to remote code execution on the affected system.
CVE-2026-48837	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Unlimited Elements For Elementor allows Blind SQL Injection
CVE-2018-25376	Socusoft 3GP Photo Slideshow 8.05 contains a buffer overflow vulnerability in the registration dialog that allows local attackers to execute arbitrary code by exploit
CVE-2018-25356	SIPp 3.6 and earlier contains a local buffer overflow vulnerability in command-line argument handling that allows local attackers to crash the application or execute
CVE-2018-25377	Flash Slideshow Maker Professional 5.20 contains a buffer overflow vulnerability in the registration dialog that allows local attackers to execute arbitrary code by e
CVE-2026-9157	Improper input validation, Unrestricted upload of file with dangerous type vulnerability in Gmission Web Fax allows Remote Code Inclusion. This issue affects Web I
CVE-2026-2740	Zohocorp ManageEngine ADSelfService Plus version before 6525, DataSecurity Plus before 6264 and RecoveryManager Plus before 6313 are vulnerable to Authent
CVE-2018-25355	Audiograbber 1.83 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting structured exception handling mechar
CVE-2026-45253	ptrace(PT_SC_REMOTE) failed to properly validate parameters for the syscall(2) and __syscall(2) meta-system calls. As a result, a user with the ability to debug a pr system.
CVE-2018-25375	SocuSoft iPod Photo Slideshow 8.05 contains a buffer overflow vulnerability in the registration dialog that allows local attackers to execute arbitrary code by overw
CVE-2018-25344	10-Strike Network Inventory Explorer 8.54 contains a stack-based buffer overflow vulnerability in the registration key input field that allows local attackers to execu dialog to achieve code execution with application privileges.
CVE-2018-25360	AgataSoft Auto PingMaster 1.5 contains a stack-based buffer overflow vulnerability in the Trace Route host name field that allows local attackers to execute arbitra the application.
CVE-2018-25359	Splinterware System Scheduler Pro 5.12 contains an insecure file permissions vulnerability that allows low-privilege users to escalate privileges by modifying servic
CVE-2018-25366	CuteFTP 5.0 XP contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by injecting malicious payload into the Site Manager la
CVE-2018-25373	SocuSoft DVD Photo Slideshow Professional 8.07 contains a stack-based buffer overflow vulnerability in the registration name field that allows local attackers to ex Registration Name field via Help > Register to trigger code execution.
CVE-	

2018-25345	10-Strike Network Scanner 3.0 contains a local buffer overflow vulnerability in the host name field that allows attackers to bypass SafeSEH protections and execute
CVE-2026-44966	Velocity.js is a JavaScript implementation of the Apache Velocity template engine. In 2.1.5 and earlier, a prototype pollution vulnerability was discovered in velocity Remote Code Execution (RCE) depending on the server environment.
CVE-2026-24188	NVIDIA TensorRT contains a vulnerability where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to data tamper
CVE-2018-25342	Smartshop 1 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code th
CVE-2026-44843	LangChain is a framework for building agents and LLM-powered applications. Prior to 0.3.85 and 1.3.3, LangChain contains older runtime code paths that deserializ any trusted LangChain-serializable object to be revived, which is broader than these runtime paths require. As a result, attacker-supplied LangChain serialized cons
CVE-2018-25341	Smartshop 1 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the i
CVE-2026-8890	code100x contains an authentication bypass vulnerability in the Mobile API that allows unauthenticated attackers to impersonate arbitrary users by supplying a cra the downstream route handler in the mobile courses endpoint accepts as trusted, granting unauthorized access to course data belonging to any enrolled user or ac
CVE-2026-42013	A flaw was found in gnutls. When validating certificates, an oversized Subject Alternative Name (SAN) could cause the validation process to incorrectly fall back to
CVE-2026-5260	A flaw was found in libgnutls. A remote attacker, by sending an extremely short premaster secret during an RSA key exchange to a server using an RSA key backe
CVE-2026-5817	The vllm-metal inference backend in Docker Model Runner on macOS unconditionally sets trust_remote_code=True when loading model tokenizers, and runs witho Docker Desktop user when inference is triggered. Any container on the Docker network can trigger this by calling the model-runner.docker.internal API to pull a ma
CVE-2026-9284	The WooCommerce PayPal Payments plugin for WordPress is vulnerable to unauthorized order manipulation and information disclosure due to missing authorizatio validating order ownership, allowing attackers to create PayPal orders for any WC order and write PayPal metadata to it. The `ppc-get-order` endpoint returns full P sensitive order details (payer information, shipping data) by creating a PayPal order for a victim's WC order and then retrieving the PayPal order data.
CVE-2026-5843	The MLX inference backend in Docker Model Runner on macOS uses the MLX-LM library, which unconditionally imports and executes arbitrary Python files from mo safety check. The MLX backend runs without sandboxing, resulting in arbitrary code execution on the Docker host as the Docker Desktop user. Any container on th
CVE-2018-25340	Smartshop 1 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the i
CVE-2026-48235	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in incs/remotes.inc.php where latitude, longitude, callsign, mph, altitude, and timestamp valu the remote GPS tracker endpoint can inject SQL to manipulate the responder location, tracks, and assignment tables.
CVE-2026-44728	Babel is a compiler for writing next generation JavaScript. From 7.12.0 to before 7.29.4 and 8.0.0-alpha.13, using Babel to compile code that was specifically crafte
CVE-2018-25364	Twitter-Clone 1 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through th
CVE-2018-25348	Joomla! Component Ek Rishta 2.10 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL c
CVE-2026-9057	A broken access control issue has been identified in the Talend Administration Center, that allows a user with “View” permission to modify the Talend Studio updat
CVE-2018-25351	Joomla! Component EkRishta 2.10 contains an error-based SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by inj
CVE-2018-25362	Twitter-Clone 1 contains a SQL injection vulnerability in follow.php that allows attackers to manipulate database queries by injecting SQL code through the userid p
CVE-2018-25372	MedDream PACS Server Premium 6.7.1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting
CVE-2018-25371	mooSocial Store Plugin 2.6 contains a blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries through the product p
CVE-	

2018-25379	Collectric CMU 1.0 contains a boolean-based blind SQL injection vulnerability in the lang parameter that allows unauthenticated attackers to manipulate database c
CVE-2026-48126	Algernon is a small self-contained pure-Go web server. Prior to 1.17.8, when algernon is started with --domain (or --letsencrypt, which silently turns on --domain at level above the document root. Subsequent file resolution then exposes everything in that parent directory — arbitrary file read, full directory listing, and, if any .lu
CVE-2026-44051	An improper link resolution vulnerability in Netatalk 3.0.2 through 4.4.2 allows a remote authenticated attacker to read arbitrary files or overwrite arbitrary files via
CVE-2026-48241	Open ISES Tickets before 3.44.2 contains hardcoded MySQL database credentials in loader.php (a public-facing database utility) that are committed to the source r database if it is reachable from their network.
CVE-2026-9256	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when a rewrite directive uses a regex pat unauthenticated attacker along with conditions beyond their control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer o which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2026-43618	Rsync version 3.4.2 and prior contain an integer overflow vulnerability in the compressed-token decoder where a 32-bit signed counter is not checked for overflow, environment variables, passwords, heap and stack data, and library memory pointers, significantly reducing ASLR effectiveness and facilitating further exploitation
CVE-2026-45574	epa4all-client is the Java Client for epa4all / ePA 3.0 in the Telematik Infrastruktur. Prior to 1.2.2, an attacker on the network path between the ePA service and the exchanges. This vulnerability is fixed in 1.2.2.
CVE-2026-48132	The Security Gateway does not correctly validate a length value in certain IKE packets when NAT-T is used (4500/UDP). As a result, a specially crafted or malforme
CVE-2026-48131	The VPN service may mishandle an unexpected IKE fragment value received on the IKE port 500/UDP during the early stage of a connection attempt. This can caus
CVE-2026-48842	Roundcube Webmail 1.6.x before 1.6.16 and 1.7.x before 1.7.1 has Pre-authentication SQL injection in the virtuser_query plugin via a preg_replace() backslash esc
CVE-2026-43935	e107 is a content management system (CMS). Prior to 2.3.4, a Host Header Injection vulnerability in the password reset page allows attackers to manipulate the Ho user authentication. This vulnerability is fixed in 2.3.4.
CVE-2026-45584	Heap-based buffer overflow in Microsoft Defender allows an unauthorized attacker to execute code over a network.
CVE-2026-46727	An issue was discovered in Ruby 4 before 4.0.5. A race condition leading to a use-after-free in the pthread-based getaddrinfo timeout handler (rb_getaddrinfo in ex exploitation is theoretically possible. The attack could, for example, be carried out through a crafted authoritative DNS server or recursive resolver.
CVE-2026-44900	epa4all-client is the Java Client for epa4all / ePA 3.0 in the Telematik Infrastruktur. Prior to 1.2.1, in SignedPublicKeysTrustValidatorImpl.isTrusted(), the ECDSA sign For any structurally valid signature, it returns true. This vulnerability is fixed in 1.2.1.
CVE-2026-47784	In memcached before 1.6.42, password data for SASL password database authentication has a timing side channel because memcmp is used by sasl_server_userdl
CVE-2026-47783	In memcached before 1.6.42, username data for SASL password database authentication has a timing side channel because a loop exits as soon as a valid usernar
CVE-2026-45361	Apache Airflow providers-google's `ComputeEngineSSHHook` disables SSH host-key verification by default, exposing SSH traffic between an Airflow worker and a C
CVE-2026-9277	shell-quote's `quote()` function did not validate object-token inputs against the operator model used by `parse()`. The `.op` field was backslash-escaped character separator, so any content after it would execute as a second command. The vulnerable code path is reachable in two ways: (1) direct construction of `{ op: '...\n...' `.op` must match the parser's control-operator allowlist; `{ op: 'glob', pattern }` validates `pattern` and forbids line terminators; `{ comment }` validates `comme
CVE-2026-41076	RT is an open source, enterprise-grade issue and ticket tracking system. Versions 5.0.9 and prior in addition to 6.0.0 through 6.0.2 contain an authentication bypas been fixed in versions 5.0.10 and 6.0.3. If developers are unable to upgrade immediately, they can temporarily work around this issue by reviewing their LDAP serv
CVE-2026-8046	The affected products insufficiently verify authorization when deleting user accounts. An authenticated, low-privileged remote user can exploit this vulnerability to
CVE-2026-25193	Insertion of Sensitive Information into Log File (CWE-532) in some Command Centre Service installers could lead to Service Account credentials exposure. Mitigatir change the Service Account password. They can also delete any installer log files, usually found in %programdata%\Gallagher\Command Centre.
CVE-2026-48695	FastNetMon Community Edition through 1.2.9 contains an OS command injection vulnerability in the MikroTik router integration plugin. The _log() function in src/m identical in pattern to the Juniper plugin vulnerability. The $msg variable contains unsanitized attack data from command-line arguments. An attacker who can infl
CVE-	FastNetMon Community Edition through 1.2.9 contains a configuration injection vulnerability in the Juniper router integration plugin. In src/juniper_plugin/fastnetmo

2026-48694	>load_set_configuration("set routing-options static route {$IP_ATTACK} community 65535:666 discard"). Line 90: $conn->load_set_configuration("delete routing-o modify the router's routing table, firewall filters, user accounts, or any other configuration element accessible via NETCONF. The impact is full router compromise.
CVE-2026-48692	FastNetMon Community Edition through 1.2.9 exposes a gRPC API server on port 50052 with no authentication mechanism. The server is initialized with grpc::Insec ExecuteUnBan, GetBanlist, GetTotalTrafficCounters, etc.) perform any credential verification. The ExecuteBan and ExecuteUnBan methods trigger security-critical a traffic), unban active attacks (disabling DDoS mitigation), and trigger script execution. There is also no role-based access control separating read-only monitoring f
CVE-2026-8855	IBM HTTP Server 8.5, and 9.0 is vulnerable to remote code execution and denial of service in configurations with TLS mutual authentication (client authentication).
CVE-2026-9397	A weakness has been identified in Besen BS20 EV Charging Station up to 20260426. Affected by this issue is some unknown functionality of the component OTA Up disclosure mentions, that "[t]hese vulnerabilities have been reported to Besen and we have received their acknowlegement that they are reviewing this as of April
CVE-2026-48242	Open ISES Tickets before 3.44.2 contains hardcoded MySQL database connection credentials (host, username, password, database name) in import_mdb.php. The
CVE-2026-45760	(Externally Controlled Reference to a Resource in Another Sphere), (Authorization Bypass Through User-Controlled Key) vulnerability in Apache Camel K. Authorized before 2.9.2, from 2.10.0 before 2.10.1. Users are recommended to upgrade to version 2.10.1 (or 2.8.1 or 2.9.2), which fixes the issue.
CVE-2026-24218	NVIDIA DGX OS contains a vulnerability in the factory provisioning process, where the cloning of a base image causes identical SSH host keys to be deployed acros tampering, escalation of privileges, information disclosure, and denial of service.
CVE-2026-40172	authentik is an open-source identity provider. In versions prior to 2025.12.5 and 2026.2.0-rc1 through 2026.2.2, the PATCH /api/v3/core/users/{pk}/ API allows a ca permission model enforced in group-management paths and enables delegated user-management permissions to escalate target users to administrator-equivalent 22025.12.5 and 2026.2.3.
CVE-2026-24213	NVIDIA Triton Inference Server contains a vulnerability in the DALI backend where an attacker could cause an out-of-bounds read. A successful exploit of this vulne
CVE-2026-24214	NVIDIA Triton Inference Server contains a vulnerability in the DALI backend where an attacker could cause an integer overflow. A successful exploit of this vulnerab
CVE-2026-4858	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to check integration URL for path traversal which allows an m
CVE-2025-11954	Cross-Site request forgery (CSRF) vulnerability in Sitemio Information Technologies Trade Ltd. Co. WISECP allows Cross Site Request Forgery. This issue affects WIS
CVE-2026-8834	IBM HTTP Server 8.5, and 9.0 contains a buffer overflow vulnerability. A privileged user, authenticated to the Administration Server, could exploit this vulnerability
CVE-2025-71213	An origin validation error vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker
CVE-2026-45206	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-
CVE-2025-71216	A time-of-check time-of-use vulnerability in the Trend Micro Apex One (mac) agent cache mechanism could allow a local attacker to escalate privileges on affected these were addressed already via ActiveUpdate/SaaS updates in mid to late 2025 (SaaS 2507 & 2005 Yearly Release).
CVE-2026-28764	MediaArea MediaInfoLib LXF element parsing heap-based buffer overflow vulnerability
CVE-2026-7452	A maliciously crafted WRL file, when parsed through Autodesk 3ds Max, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerabil
CVE-2026-45208	A time-of-check time-of-use vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. Please note: an atta
CVE-2026-45251	A file descriptor can be closed while a thread is blocked in a poll(2) or select(2) call waiting for that descriptor. Because the blocked thread does not hold a referenc case of some file descriptor types, the kernel failed to unlink blocked threads from the object before freeing it. When the blocked thread is subsequently woken, it a
CVE-2025-71217	An origin validation error vulnerability in the Trend Micro Apex One (mac) agent self-protection mechanism could allow a local attacker to escalate privileges on aff references, as these were addressed already via ActiveUpdate/SaaS updates in mid to late 2025 (SaaS 2507 & 2005 Yearly Release).
CVE-2026-45207	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-
CVE-	The setcred(2) system call is only available to privileged users. However, before the privilege level of the caller is checked, the user-supplied list of supplementary

2026-45250	occurs after the kernel stack buffer has already been written, an unprivileged local user may trigger the overflow without holding any special privilege. Successful e
CVE-2026-34927	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker mu
CVE-2026-34930	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-
CVE-2026-48864	A flaw was found in libsolv. This heap buffer overflow occurs during the decompression of attacker-controlled compressed data within `.solv` files due to insufficien execution, or a denial of service.
CVE-2025-71212	A link following vulnerability in the Trend Micro Apex One scan engine could allow a local attacker to escalate privileges on affected installations. Please note: an at
CVE-2026-7451	A maliciously crafted TIF file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerab
CVE-2026-34929	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-
CVE-2025-71214	An origin validation error vulnerability in the Trend Micro Apex One (mac) agent iCore service could allow a local attacker to escalate privileges on affected installat were addressed already via ActiveUpdate/SaaS updates in mid to late 2025 (SaaS 2507 & 2005 Yearly Release).
CVE-2026-34928	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-
CVE-2026-7454	A maliciously crafted WRL file, when parsed through Autodesk 3ds Max, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerabil
CVE-2026-25112	A high-severity vulnerability in the deployment of Genetec RabbitMQ that allows a privilege escalation attack.
CVE-2026-24162	NVIDIA Transformers4Rec for Linux contains a vulnerability where an attacker could cause improper deserialization of untrusted data. A successful exploit of this v
CVE-2026-24194	NVIDIA Display Driver for Linux contains a vulnerability in a kernel mode layer handler, where a user could cause improper permission handling. A successful explo
CVE-2026-44468	The affected product creates a directory with insecure default permissions during administrative installation. This allows a low-privileged local attacker to modify a
CVE-2026-41054	In `src/havegecmd.c`, the `socket_handler` function performs a credential check on the abstract UNIX socket (`\0/sys/entropy/haveged`). However, while it detects privileged commands such as `MAGIC_CHROOT`.
CVE-2026-9255	Missing input source validation in the tool authorization prompt in Kiro CLI before 1.28.0 allows a local attacker to execute arbitrary tools, including shell command
CVE-2026-24216	NVIDIA BioNemo for Linux contains a vulnerability where a user could cause a deserialization of untrusted data. A successful exploit of this vulnerability might lead
CVE-2026-24193	NVIDIA Display Driver for Windows and Linux contains a vulnerability where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerabilit
CVE-2026-25713	MediaArea MediaInfoLib ID3v2 parsing heap buffer overflow vulnerability
CVE-2026-40034	gix-submodule before 0.82.0 incorrectly validates the update field in .gitmodules, allowing attackers to bypass the CommandForbiddenInModulesConfiguration gua previously-initialized submodule, enabling remote code execution.
CVE-2026-24192	NVIDIA Display Driver for Linux contains a vulnerability where an attacker could cause an incorrect conversion between numeric types, leading to a heap buffer ov
CVE-2026-25104	MediaArea MediaInfoLib LXF parsing heap-based buffer overflow vulnerability
CVE-2026-	A potential security vulnerability has been identified in the HP Linux Imaging and Printing Software. This potential vulnerability may allow escalation of privileges a

8632	
CVE-2026-24191	NVIDIA Display Driver for Windows contains a vulnerability where an attacker could cause a time-of-check time-of-use issue. A successful exploit of this vulnerabilit
CVE-2026-24190	NVIDIA Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause improper access to GPU resources. A succ
CVE-2026-44933	`PluginScript` attempts to `chroot` the plugin to the `repoManagerRoot`, this root is frequently `/` (the system root) in standard configurations or when using `--ro
CVE-2026-0856	Improper Access Control vulnerability in Mesalvo Meona Client Launcher Component, Mesalvo Meona Server Component enables a normal user gaining access to th
CVE-2026-41091	Improper link resolution before file access ('link following') in Microsoft Defender allows an authorized attacker to elevate privileges locally.
CVE-2026-22554	MediaArea MediaInfoLib Channel Splitting heap-based buffer overflow vulnerability
CVE-2026-44469	The affected product extracts installation files to a temporary directory with incorrect default permissions during administrative installation. A low-privileged local a
CVE-2026-42834	Improper link resolution before file access ('link following') in Azure Portal Windows Admin Center allows an authorized attacker to elevate privileges locally.
CVE-2026-46300	In the Linux kernel, the following vulnerability has been resolved: net: skbuff: preserve shared-frag marker during coalescing skb_try_coalesce() can attach paged f later in-place writers. In particular, ESP input checks skb_has_shared_frag() before deciding whether an uncloned nonlinear skb can skip skb_cow_data(). If TCP rece frags. The tailroom copy path does not need the marker because it copies bytes into @to's linear data rather than transferring frag descriptors.
CVE-2026-8856	IBM HTTP Server 8.5, and 9.0 is vulnerable to denial of service in configurations where an attacker has write access to parts of the server configuration.
CVE-2026-26147	Improper input validation in Azure Compute Gallery allows an authorized attacker to disclose information over a network.
CVE-2026-39965	TypeBot is a chatbot builder tool. Versions 3.15.2 and prior contain an SSRF via Open Redirect Bypass as the HTTP Request block and Code block validate the initia block to an attacker-controlled server that responds with a redirect to an internal IP, causing the Typebot server to reach internal services. An authenticated Typeb 3.16.0.
CVE-2026-34911	A malicious actor with access to the network and low privileges could exploit a Path Traversal vulnerability found in UniFi OS devices to access files on the underlyi
CVE-2026-9133	Active debug code exists in the ARN resolver of amazon-mq rabbitmq-aws before version 0.2.1. A debug ARN scheme (arn:aws-debug:file) accepted by the PUT /ap aws. If RabbitMQ is configured to use TLS for connections, we also recommend rotating any associated private certificate keys.
CVE-2026-45082	Karakeep is a elf-hostable bookmark-everything app. A Server-Side Request Forgery (SSRF) protection bypass vulnerability was identified in versions prior to 0.32.0 redirect chains. By leveraging attacker-controlled redirects, an authenticated user could cause vulnerable application components to initiate requests toward intern patch.
CVE-2026-44680	MikroORM is a TypeScript ORM for Node.js based on Data Mapper, Unit of Work and Identity Map patterns. Prior to @mikro-orm/knex 6.6.14 and @mikro-orm/sql 7.(identifier or string-literal context they emit into. When application code passes attacker-influenced strings to public ORM APIs that expect an identifier or a JSON-pr
CVE-2026-44068	Incomplete sanitization of extended attribute (EA) path components in Netatalk 2.1.0 through 4.4.2 allows a remote authenticated attacker to write to files outside
CVE-2026-42383	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Blind SQL
CVE-2026-9047	Improper handling of factor key state in the multi-factor authentication management feature in Devolutions Server allows an attacker with knowledge of a user's pa
CVE-2026-34207	TypeBot is a chatbot builder tool. In versions prior to 3.16.0, SSRF protection for Webhook / HTTP Request blocks validates only the URL string, blocked hostname li fetched by the backend HTTP client. This enables server-side request forgery to loopback, cloud metadata, and private network targets. This issue has been resolv
CVE-2026-9144	Taiko AG1000-01A SMS Alert Gateway Rev 7.3 and Rev 8 contains a stored cross-site scripting vulnerability in the embedded web configuration interface that allow concatenate executable script fragments that are rendered in administrative dashboard views such as index.zhtml, resulting in persistent script execution within a
CVE-2026-	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Beyaz Computer Software Design Industry and Trade Ltd. Co. Cit

5783	
CVE-2026-9011	The Ditty – Responsive News Tickers, Sliders, and Lists plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.1.65. This is disabled entries — by enumerating integer post IDs against the ditty_init AJAX endpoint. Unlike the non-AJAX init() counterpart, init_ajax() does not verify that the r
CVE-2026-45728	Algernon is a small self-contained pure-Go web server. Prior to 1.17.7, when Algernon is invoked with a single file path instead of a directory, singleFileMode is set parser error text. This response is served with HTTP 200 OK to whoever sent the request that triggered the error. Any client able to reach the server and able to pr
CVE-2026-8679	The AudioIgniter plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 2.0.2. This is due to the handle_playlist_en authentication, capability, or post_status check — only the post_type is validated. This makes it possible for unauthenticated attackers to view track metadata (title
CVE-2026-23663	Improper privilege management in Azure Entra ID allows an unauthorized attacker to elevate privileges over a network.
CVE-2026-44417	The fix for CVE-2025-48913: Apache CXF: Untrusted JMS configuration can lead to RCE was not complete, meaning that another path in the code might lead to cod
CVE-2026-42001	Insufficient Validation of Autoprimary SOA Queries
CVE-2026-48688	FastNetMon Community Edition through 1.2.9 contains multiple out-of-bounds reads in the BGP MP_REACH_NLRI IPv6 attribute decoder. The function decode_mp_r verifying sufficient data exists (line 158), uses the attacker-controlled length_of_next_hop field to determine memcpy size (line 181), and computes prefix_length b 202) with no check against remaining buffer size.
CVE-2026-45255	When bsdinstall or bsdconfig are prompted to scan for nearby Wi-Fi networks, they build up a list of network names and use bsddialog(1) to prompt the user to sel subshell. The problem can be exploited to execute code as root on the system running bsdinstall or bsdconfig. The attacker would need to create an access point w
CVE-2026-24212	NVIDIA Isaac Launchable for Linux contains a vulnerability where sensitive information is transmitted in clear text. A successful exploit of this vulnerability might le
CVE-2026-46473	Authen::TOTP versions before 0.1.1 for Perl generate secrets using rand. Secrets were generated using Perl's built-in rand function, which is predictable and unsuit
CVE-2026-8850	IBM HTTP Server 8.5, and 9.0 is vulnerable to denial of service via the optional module mod_ibm_upload.
CVE-2018-25358	D-Link DIR601 2.02NA contains a credential disclosure vulnerability that allows unauthenticated attackers to retrieve sensitive configuration data by manipulating clear text.
CVE-2026-5740	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to properly validate msgpack-encoded WebSocket frames bef Advisory ID: MMSA-2026-00647
CVE-2026-4834	The WP ERP Pro plugin for WordPress is vulnerable to SQL Injection via the 'search_key' parameter in all versions up to, and including, 1.5.1. This is due to insufficie to extract sensitive information from the database.
CVE-2025-45145	Directory traversal in Follett Software's Destiny Library Manager 22_0_2_rc1 and fixed in v.22.5 AU1 allows remote attackers to read arbitrary system and applicati
CVE-2025-13479	Authorization bypass through User-Controlled key vulnerability in PosCube Hardware Software and Consulting Ltd. QR Menu allows Exploitation of Trusted Identifie
CVE-2026-46597	An incorrectly placed cast from bytes to int allowed for server-side panic in the AES-GCM packet decoder for well-crafted inputs.
CVE-2026-48829	In GNU SASL before 2.2.3, DIGEST-MD5 has a NULL pointer dereference affecting both clients and servers, via a known token with no accompanying = character. T
CVE-2026-39829	The RSA and DSA public key parsers did not enforce size limits on key parameters. A crafted public key with an excessively large modulus or DSA parameter could FIPS 186-2.
CVE-2025-32750	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Exposure of Information Through Directory Listing vulnerability. An unauthenticated attacker with remot
CVE-2026-9064	A flaw was found in 389-ds-base. The get_ldapmessage_controls_ext() function in the LDAP server does not enforce an upper bound on the number of controls per consumption and heap allocation on the server. Under concurrent exploitation, this leads to significant latency degradation, worker thread starvation, or out-of-me
CVE-2018-	Nord VPN 6.14.31 contains a denial of service vulnerability that allows unauthenticated attackers to crash the application by submitting an excessively long string

25368	
CVE-2026-3039	BIND servers that are configured to use TKEY-based authentication via GSS-API tokens are vulnerable to excessive memory consumption when receiving and proce through 9.18.48, 9.20.0 through 9.20.22, 9.21.0 through 9.21.21, 9.9.3-S1 through 9.16.50-S1, 9.18.11-S1 through 9.18.48-S1, and 9.20.9-S1 through 9.20.22-S1.
CVE-2018-25365	PCViewer vt1000 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by submitting relative path sequences in G
CVE-2026-5946	Multiple flaws have been identified in `named` related to the handling of DNS messages whose CLASS is not Internet (`IN`) — for example, `CHAOS` or `HESIOD`, processing of `IN`-specific record types in non-`IN` data — can cause assertion failures in `named`. This issue affects BIND 9 versions 9.11.0 through 9.16.50, 9.18
CVE-2026-5947	Undefined behavior may result due to a race condition leading to a use-after-free violation. If BIND receives an incoming DNS message signed with SIG(0), it begins validation may attempt to read the now-discarded DNS message. This issue affects BIND 9 versions 9.20.0 through 9.20.22, 9.21.0 through 9.21.21, and 9.20.9-S1
CVE-2026-39047	Buffer Overflow vulnerability in EPSON L14150 FL27PB allows a remote attacker to execute arbitrary code via the RAW Printing Service (JetDirect) on TCP port 9100
CVE-2026-8047	The affected products perform improper length checking when parsing incoming HTTP requests, resulting in a size-limited out-of-bounds write. An unauthenticated
CVE-2026-44847	MaxKB is an open-source AI assistant for enterprise. Prior to 2.9.0, MaxKB's webhook trigger endpoint (/api/trigger/v1/webhook/{trigger_id}) is accessible without a requirements, any unauthenticated attacker who knows a valid trigger ID can invoke webhook triggers to execute their bound tasks. This vulnerability is fixed in 2.
CVE-2026-20239	In Splunk Enterprise versions below 10.2.2 and 10.0.5, and Splunk Cloud Platform versions below 10.3.2512.8, 10.2.2510.11, 10.1.2507.21, and 10.0.2503.13, a us
CVE-2026-39661	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Magentech SW Core allows PHP Local File
CVE-2025-11482	An Allocation of Resources Without Limits or Throttling vulnerability in the OPC-UA Server used in PPT30 Operating System versions before 1.8.0 may be used by a
CVE-2026-48133	When the Identity Awareness blade is enabled with Browser-Based Authentication, an unauthenticated user may be able to read certain internal files on the Securi
CVE-2026-44209	Banks generates meaningful LLM prompts using a template language that makes sense. Prior to 2.4.2, banks uses jinja2.Environment() (unsandboxed) to render pr vulnerability is fixed in 2.4.2.
CVE-2026-9117	Type Confusion in GFX in Google Chrome on Linux, ChromeOS prior to 148.0.7778.179 allowed a remote attacker who had compromised the renderer process to p
CVE-2026-9123	Heap buffer overflow in Chromecast in Google Chrome on Android, Linux, ChromeOS prior to 148.0.7778.179 allowed a local attacker to execute arbitrary code insi
CVE-2018-25374	Softneta MedDream PACS Server Premium 6.7.1.1 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by manip
CVE-2026-42959	NLnet Labs Unbound up to and including version 1.25.0 has a denial of service vulnerability in the DNSSEC validator that can lead to a crash given malicious upstre authority filtering could decrease the AUTHORITY section count and create an uninitialized array slot. Combining these two, the validator later dereferences this un AUTHORITY records alongside signed ADDITIONAL glue records. Unbound 1.25.1 contains a patch with a fix to use the proper counters to calculate the write offsets
CVE-2026-40092	nimiq-blockchain provides persistent block storage for Nimiq's Rust implementation. In versions 1.3.0 and below, a malicious network peer can crash any Nimiq full victim node's DHT verifier calls TaggedSigned::verify, execution reaches Ed25519Signature::from_bytes(sig).unwrap() in the TaggedPublicKey implementation for E implementation panics. This issue has been fixed in version 1.4.0.
CVE-2026-42944	NLnet Labs Unbound 1.14.0 up to and including version 1.25.0 has a vulnerability that results in heap overflow when encoding multiple NSID and/or DNS Cookie ED vulnerability by attaching multiple NSID and/or DNS Cookie EDNS and/or EDNS Padding options to the query. A flaw in the size calculation of the EDNS field truncat to de-duplicate the EDNS options and a fix to prevent truncation of the EDNS field size calculation.
CVE-2026-3985	The Creative Mail – Easier WordPress & WooCommerce Email Marketing plugin for WordPress is vulnerable to SQL Injection via the 'checkout_uuid' parameter in all unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2026-45209	Missing Authorization vulnerability in edward_plainview MyCryptoCheckout allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affect
CVE-2026-45438	Missing Authorization vulnerability in WebToffee Smart Coupons for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This iss
CVE-2026-	Roundcube Webmail 1.6.x before 1.6.16 and 1.7.x before 1.7.1 has insecure code evaluation logic in LDAP the autovalues option that could lead to code injection. (

48844	
CVE-2026-44905	Vanetza is an open-source implementation of the ETSI C-ITS protocol suite. In 26.02 and earlier, a denial-of-service vulnerability was identified in the cryptographic are only strictly enforced during OER re-encoding. Specifically, if a crafted packet contains a certificate where the Psid (Provider Service Identifier) sub-type violate verification, it must re-encode the signing certificate. The underlying ASN.1 wrapper (asn1c_wrapper.cpp) detects the semantic violation during encoding and raise e1a2e2709210d309458c3d77f98d50dec26c0df0.
CVE-2025-33255	NVIDIA TRT-LLM for any platform contains a vulnerability in MPI server, where an attacker could cause an unsafe deserialization. A successful exploit of this vulnera
CVE-2026-24163	NVIDIA TRT-LLM for any platform contains a vulnerability in RPC testing, where an attacker could cause an unsafe deserialization. A successful exploit of this vulner
CVE-2026-24209	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a path traversal issue. A successful exploit of this vulnerability might lead to
CVE-2026-24210	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause an integer overflow. A successful exploit of this vulnerability might lead to de
CVE-2026-9003	E-LAN Hybrid Recording System developed by TONNET has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commar
CVE-2026-9010	The Boost plugin for WordPress is vulnerable to time-based SQL Injection via the 'current_url' and 'user_name' parameters in versions up to, and including, 2.0.3 du that can be used to extract sensitive information from the database.
CVE-2026-43988	Vanetza is an open-source implementation of the ETSI C-ITS protocol suite. In 26.02 and earlier, a denial-of-service vulnerability was identified in the ASN.1/OER pa std::runtime_error. This exception is not caught at the parsing boundary and propagates to std::terminate, resulting in process termination. This vulnerability is fixe
CVE-2026-9496	Versions of the package pacote from 11.2.7 are vulnerable to Denial of Service (DoS) via the addGitSha function. An attacker can exploit this vulnerability by suppl
CVE-2026-40622	NLnet Labs Unbound 1.16.2 up to and including version 1.25.0 has a vulnerability of the 'ghost domain names' family of attacks that could extend the ghost domai overwrite the cached expired parent-side referral NS rrset with the child-side apex NS rrset and essentially extend the ghost domain window by up to one cached T with a fix that does not allow extension of TTLs for (parent) NS records regardless of their trust.
CVE-2026-41292	NLnet Labs Unbound up to and including version 1.25.0 is vulnerable to a degradation of service attack related to parsing long lists of incoming EDNS options. An a Unbound 1.25.1 contains a patch with a fix to limit acceptable incoming EDNS options (100).
CVE-2026-47373	Crypt::SaltedHash versions through 0.09 for Perl is susceptible to timing attacks. These versions use Perl's built-in eq comparison. Discrepencies in timing could be
CVE-2026-8671	Insertion of sensitive information into log file vulnerability in syslink software AG Avantra on Linux, Windows allows Resource Leak Exposure. This issue affects Ava
CVE-2026-9170	IBM Web Server Plug-ins for WebSphere Application Server and WebSphere Liberty 8.5, 9.0 IBM WebSphere Application Server and WebSphere Application Server L
CVE-2026-8854	IBM HTTP Server 8.5, and 9.0 is vulnerable to denial of service via the optional module mod_mem_cache.
CVE-2026-44062	A missing output length bounds check in pull_charset_flags() in Netatalk 2.0.4 through 4.4.2 allows a remote authenticated attacker to execute arbitrary code or ca
CVE-2026-44055	A logic error involving bitwise OR operations in Netatalk 3.1.4 through 4.4.2 allows a remote authenticated attacker to inject OS commands and execute arbitrary c
CVE-2026-44049	An out-of-bounds write due to improper null termination in convert_charset() in Netatalk 2.0.4 through 4.4.2 allows a remote authenticated attacker to execute arb
CVE-2026-44052	Netatalk 2.1.0 through 4.4.2 inserts LDAP simple-bind passwords into log output in cleartext, which allows an attacker with access to the log files to obtain LDAP cr
CVE-2026-44060	An integer underflow in dsi_writeinit() in Netatalk 1.5.0 through 4.4.2 allows a remote unauthenticated attacker to cause a denial of service via a crafted DSI write
CVE-2026-8620	IBM Web Server Plug-ins for WebSphere Application Server and WebSphere Liberty 8.5, 9.0 IBM WebSphere Application Server and WebSphere Application Server L
CVE-	

2026-3593	A use-after-free vulnerability exists within the DNS-over-HTTPS implementation. This issue affects BIND 9 versions 9.20.0 through 9.20.22, 9.21.0 through 9.21.21,
CVE-2026-39850	Yii 2 is a PHP application framework. Versions 2.0.54 and prior contain flawed logic in the core view rendering method View::renderPhpFile() that leads to Local File file to include, potentially enabling RCE if an attacker can write PHP files through a separate primitive, as well as information disclosure. This issue has been fixed i
CVE-2026-44053	Netatalk 1.5.0 through 4.2.2 uses a broken cryptographic algorithm in the DHCAST128 UAM, which allows a remote attacker to obtain authentication credentials or
CVE-2026-45575	epa4all-client is the Java Client for epa4all / ePA 3.0 in the Telematik Infrastruktur. Prior to 1.2.2, an attacker who can MITM the TLS connection between the client response to the attacker's encryption key and POSTs it to the attacker's auth endpoint. This captures the signed authentication material. This vulnerability is fixed
CVE-2026-48697	FastNetMon Community Edition through 1.2.9 does not verify TLS certificates on outbound HTTPS connections. The execute_web_request_secure() function in src/fa handshake without validating the server's certificate chain, making all HTTPS connections vulnerable to man-in-the-middle attacks. This function is used for teleme malicious server.
CVE-2026-9367	A vulnerability was determined in NousResearch hermes-agent up to 5157f5427f19488b31c6fdebbacd15d798ce7f63. This affects the function detect_dangerous_c was contacted early about this disclosure but did not respond in any way.
CVE-2026-9517	A vulnerability was determined in hemant6488 CodeIgniter-StudentManagementSystem. The affected element is an unknown function of the file /index.php/studen product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was inform
CVE-2026-9353	A security vulnerability has been detected in NousResearch hermes-agent up to 2026.4.23. Impacted is an unknown function of the file agent/skills_guard.py of the vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9521	A security vulnerability has been detected in fraillt bitsery up to 5.2.4. Affected is the function loadFromSharedState in the library include/bitsery/ext/std_smart_ptr name of the patch is 66d16516e24893bebc1c8af52bf2fe9ad0735061. Upgrading the affected component is advised.
CVE-2026-9356	A vulnerability has been found in SourceCodester Hospitals Patient Records Management System 1.0. This affects an unknown function of the file /admin/patients/r
CVE-2026-9551	A vulnerability was identified in Das Parking Management System 停车场管理系统 6.2.0. This affects the function xp_cmdshell of the file ParkingRecord/ExportParkin this disclosure but did not respond in any way.
CVE-2026-9580	A vulnerability was determined in JeecgBoot up to 3.9.1. The affected element is the function LoginController.selectDepart of the file /sys/selectDepart. This manipu affected component.
CVE-2026-9453	A vulnerability was detected in FoundDream miniclawd up to 2d65665046e2222eeea76cafc8570ed546a8c125. This affects the function which of the file /src/applic 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 wa
CVE-2026-9523	A vulnerability was detected in Acrel Electrical EEMS Enterprise Power Operation and Maintenance Cloud Platform 3000WEBV2. Affected by this vulnerability is an u be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9368	A vulnerability was identified in NousResearch hermes-agent up to 2026.4.16. This impacts the function execute_code of the file tools/code_execution_tool.py of th but did not respond in any way.
CVE-2026-9584	A security vulnerability has been detected in code-projects Project Management System 1.0. Affected is an unknown function of the file chk.php of the component
CVE-2026-9465	A vulnerability was found in Tiandy Easy7 Integrated Management Platform 7.17.0. This vulnerability affects unknown code of the file /Easy7/apps/WebService/GetI disclosure but did not respond in any way.
CVE-2026-36228	Buffer Overflow vulnerability in Easy Chat Server 3.1 allows a remote attacker to obtain sensitive information and execute arbitrary code via the chat message fun
CVE-2026-37470	An issue in ClipBucket v5 v.5.5.2 allows an attacker to execute arbitrary code via the Authentication interface, login page endpoint and HTTP response security hea
CVE-2026-9495	Versions of the package @koa/router from 14.0.0 and before 15.0.0 are vulnerable to Access Control Bypass due to the middleware being silently dropped from the sanitization.
CVE-2026-9528	A vulnerability was identified in itsourcecode Electronic Judging System 1.0. Impacted is an unknown function of the file /admin/delete_judge.php. Such manipulatio
CVE-2026-9372	A flaw has been found in ItzCrazyKns Vane up to 1.12.1. This vulnerability affects unknown code of the file src/app/api/providers/route.ts of the component Model P through an issue report but has not responded yet.
CVE-2026-	A vulnerability was found in itsourcecode Electronic Judging System 1.0. This vulnerability affects unknown code of the file /admin/edit_team.php. The manipulation

9526	
CVE-2026-9469	A weakness has been identified in yashpokharna2555 StudentManagementSystem cb2f558ddf8d19396de0f92abf2d224d46a0a203. The impacted element is an ur product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was inforr
CVE-2026-9350	A vulnerability was identified in NousResearch hermes-agent up to 2026.4.16. This affects the function check_all_command_guards of the file tools/approval.py of t respond in any way.
CVE-2026-9470	A security vulnerability has been detected in yashpokharna2555 StudentManagementSystem cb2f558ddf8d19396de0f92abf2d224d46a0a203. This affects the func used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not availab
CVE-2026-9366	A vulnerability was found in NousResearch hermes-agent 2026.4.23. The impacted element is the function _scan_context_content of the file agent/prompt_builder.
CVE-2026-24206	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause an authentication bypass. A successful exploit of this vulnerability might lead
CVE-2026-44983	smallbitvec is a growable bit-vector for Rust, optimized for size. From 1.0.1 to 2.6.0, an integer overflow in the internal capacity calculation of smallbitvec can lead
CVE-2026-8835	IBM HTTP Server 8.5, and 9.0 is vulnerable to invalid pointer dereference. A privileged user, authenticated to the Administration Server, could exploit this vulnerabi
CVE-2026-9525	A vulnerability has been found in itsourcecode Electronic Judging System 1.0. This affects an unknown part of the file /admin/edit_judge.php. The manipulation of th
CVE-2026-9474	A vulnerability was found in yashpokharna2555 StudentManagementSystem up to cb2f558ddf8d19396de0f92abf2d224d46a0a203. Affected by this issue is the fur release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the pro
CVE-2026-9562	A vulnerability has been found in sambitraj STUDENT-MANAGEMENT-SYSTEM up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. The affected element is an un release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. Multiple endpoints are affected. The
CVE-2026-9364	A flaw has been found in projectworlds Online Art Gallery Shop 1.0. Impacted is an unknown function of the file /admin/adminHome.php. Executing a manipulation
CVE-2026-9452	A security vulnerability has been detected in FoundDream miniclawd up to 2d65665046e2222eeea76cafc8570ed546a8c125. Affected by this issue is the function E why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not respon
CVE-2026-9575	A vulnerability has been found in itsourcecode Student Transcript Processing System 1.0. This issue affects some unknown processing of the file /admin/modules/cl
CVE-2026-9447	A vulnerability was found in SourceCodester Simple POS and Inventory System 1.0. The impacted element is an unknown function of the file /user/search.php. Perf
CVE-2026-9421	A vulnerability was determined in KLiK SocialMediaWebsite 1.0. This vulnerability affects the function uniqid of the file upload.inc.php of the component File Handle
CVE-2026-9422	A vulnerability was identified in KLiK SocialMediaWebsite 1.0. This issue affects some unknown processing of the component HTTP POST Request Parameter Handle
CVE-2026-9550	A vulnerability was determined in Acrel Electrical EEMS Enterprise Power Operation and Maintenance Cloud Platform 1.3.0. Affected by this issue is some unknown utilized. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9544	A vulnerability was found in Shenzhen Sixun Software Sixun Shanghui Group Business Management System 10. Affected by this vulnerability is an unknown functio contacted early about this disclosure but did not respond in any way.
CVE-2026-9355	A flaw has been found in SourceCodester Hospitals Patient Records Management System 1.0. The impacted element is an unknown function of the file /classes/Mas
CVE-2026-9574	A flaw has been found in itsourcecode Student Transcript Processing System 1.0. This vulnerability affects unknown code of the file /admin/modules/student/trans.p
CVE-2026-9573	A vulnerability was detected in itsourcecode Student Transcript Processing System 1.0. This affects an unknown part of the file /admin/modules/student/index.php?
CVE-2026-	A vulnerability has been found in itsourcecode Electronic Judging System 1.0. This affects an unknown part of the file /intrams/admin/login.php. The manipulation o

9383	
CVE-2026-9552	A security flaw has been discovered in Das Parking Management System 停车场管理系统 6.2.0. This vulnerability affects unknown code of the component Search API disclosure but did not respond in any way.
CVE-2026-48843	Roundcube Webmail 1.6.x between 1.6.14 and 1.6.16,and 1.7.x before 1.7.1 has Insufficient Cascading Style Sheets (CSS) sanitization in HTML e-mail messages m
CVE-2026-4051	IBM Engineering Lifecycle Management 7.0.3, 7.1.0, and 7.2.0 could allow an attacker with administrative privileges to execute remote code due to exposed metho
CVE-2026-44058	An authentication bypass vulnerability in Netatalk 2.2.2 through 4.4.2 allows a remote privileged user to authenticate as an arbitrary user via the admin auth user
CVE-2026-44730	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 6.9.7, an organization admin can escalate their pri
CVE-2026-48848	Roundcube Webmail 1.6.x before 1.6.16 and 1.7.x before 1.7 has insufficient HTML sanitization that could lead to Cascading Style Sheets (CSS) injection via an SVG
CVE-2026-42785	OpenKM 6.3.12 contains a remote code execution vulnerability that allows authenticated administrators to execute arbitrary Java/BeanShell code through the /adm
CVE-2026-22315	Incorrect Privilege Assignment vulnerability in Mesalvo Meona Client Launcher Component, Mesalvo Meona Server Component enables the export of user data, inc
CVE-2026-42425	OpenKM 6.3.12 contains an unrestricted SQL execution vulnerability that allows authenticated administrative users to execute arbitrary SQL statements against th from the OKM_USER table, modify permissions, or delete database records.
CVE-2026-7613	The Cost of Goods by PixelYourSite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'csvdata[0][cost_of_goods_value]' parameter in version page.
CVE-2026-8134	Concrete CMS 9.5.0 and below fails to sanitize path traversal sequences in the ptComposerFormLayoutSetControlCustomTemplate field when saving page type cor code in files saved with image extensions like .png), this can result in authenticated remote code execution. The Concrete CMS security team gave this vulnerabilit
CVE-2026-8135	Concrete CMS 9.5.0 and below is vulnerable to Remote Code Execution due to insecure deserialization occurring in the ExpressEntryList block controller. An rogue Because the REST API parses requests using json_decode(), the string "true" is evaluated as a strict PHP Boolean(true). This bypass allows the attacker to inject a CMS security team gave this vulnerability a CVSS v.4.0 score of 8.9 with a vector of CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H. Thanks Ng
CVE-2026-24937	Improper Control of Generation of Code ('Code Injection') vulnerability in VideoWhisper.Com Broadcast Live Video allows Code Injection. This issue affects Broadcas
CVE-2026-48232	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in ajax/fullsit_incidents.php where the offset GET parameter is concatenated into the LIMIT cl
CVE-2018-25347	WordPress Contact Form Maker Plugin 1.12.20 contains SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries through the
CVE-2026-48231	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in tables.php where the multiple POST parameters (tablename, indexname, sortby) are conca contents.
CVE-2026-48240	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in ajax/statistics.php where the tick_id and f_tick_id POST parameters are concatenated into
CVE-2026-39436	Cross-Site Request Forgery (CSRF) vulnerability in bgermann CformsII allows Cross Site Request Forgery. This issue affects CformsII: from n/a through 15.1.3.
CVE-2018-25346	WordPress Form Maker Plugin 1.12.24 and below contains SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries by injecti WordPress database.
CVE-2026-7325	Improper authorization in the Active Directory browsing feature in Devolutions Server allows a low-privileged authenticated user to obtain authentication material a
CVE-2025-14361	Missing Authorization vulnerability in AA-Team Woocommerce Envato Affiliates allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects
CVE-2026-39968	TypeBot is a chatbot builder tool. In versions 3.15.2 and prior, the fix for GHSA-4xc5-wfwc-jw47 ("Credential Theft via Client-Side Script Execution and API Authoriza preview chat endpoint. The bot-engine's getCredentials() utility function uses a falsy check (if (workspaceId && ...)) for workspace ownership validation. Since the p exfiltration, external service abuse, financial damage and a data breach.

CVE-2026-42012	A flaw was found in gnutls. A remote attacker could exploit this vulnerability by presenting a specially crafted certificate that contains Uniform Resource Identifier (legitimate services or intercept sensitive information.
CVE-2026-48690	FastNetMon Community Edition through 1.2.9 contains an integer overflow vulnerability in the packet capture buffer allocation. In src/packet_storage.hpp, the alloc max_captured_packet_size=1500 and sizeof(fastnetmon_pcap_pkthdr_t)=16, each packet requires approximately 1516 bytes. If buffer_size_in_packets exceeds ap derived from the ban_details_records_count configuration parameter, which is parsed using atoi() with no overflow checking.
CVE-2018-25352	WordPress Ultimate Form Builder Lite plugin version 1.3.7 and below contains an SQL injection vulnerability that allows authenticated attackers to manipulate data WordPress database.
CVE-2026-3603	IBM Engineering Lifecycle Management 7.0.3, 7.1.0, and 7.2.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. An authent
CVE-2026-24196	NVIDIA Display Driver for Linux contains a vulnerability where a user could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to den
CVE-2026-48233	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in ajax/sit_incidents.php where the offset GET parameter is concatenated into the LIMIT claus
CVE-2026-48234	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in portal/ajax/list_requests.php where the sort and dir GET parameters are concatenated into
CVE-2026-41074	RT is an open source, enterprise-grade issue and ticket tracking system. Versions 6.0.0 through 6.0.2 contain a Cross-Site Request Forgery (CSRF) vulnerability. An
CVE-2025-13477	Exposure of private personal information to an unauthorized actor, Insufficiently Protected Credentials vulnerability in Digital Operations Services Inc. WifiBurada a
CVE-2026-48238	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in ajax/mobile_main.php where the id GET parameter is concatenated into the WHERE clause
CVE-2026-48237	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in message.php where the frm_ticket_id and frm_resp_id POST parameters are concatenated
CVE-2026-48236	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in db_loader.php where the multiple POST parameters (ticketsdb, ticketshost, ticketsuser, tic modify, or destroy database contents.
CVE-2026-44066	Multiple heap out-of-bounds reads in the Spotlight RPC unmarshalling code in Netatalk 3.1.0 through 4.4.2 allow a remote authenticated attacker to obtain sensitiv
CVE-2018-25380	Joomla Component eXtroForms 2.1.5 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL commands through the fil
CVE-2026-9291	Insecure deserialization in the job results processing component in Amazon Braket SDK before 1.117.0 might allow a remote authenticated user with S3 write acce
CVE-2018-25381	Joomla Responsive Portfolio 1.6.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL commands through multiple f
CVE-2026-44064	An out-of-bounds read in ASP session ID handling in Netatalk 1.3 through 4.4.2 allows an adjacent network attacker to obtain limited information or cause a denial
CVE-2026-48239	Open ISES Tickets before 3.44.2 contains a SQL injection vulnerability in ajax/reports.php where the tick_id POST parameter is concatenated into the WHERE clause
CVE-2026-24195	NVIDIA Display Driver for Linux contains a vulnerability in UVM, where a user could cause improper input validation. A successful exploit of this vulnerability might
CVE-2025-71215	A time-of-check time-of-use vulnerability in the Trend Micro Apex One (mac) agent iCore service signature verification could allow a local attacker to escalate privil references, as these were addressed already via ActiveUpdate/SaaS updates in mid to late 2025 (SaaS 2507 & 2005 Yearly Release).
CVE-2026-29518	Rsync versions before 3.4.3 contain a time-of-check to time-of-use (TOCTOU) race condition in daemon file handling that allows attackers to redirect file writes outs files and achieving privilege escalation when the daemon runs with elevated privileges. This vulnerability can only be triggered if the chroot setting is false.
CVE-2026-24200	NVIDIA vGPU software contains a vulnerability in the virtual GPU manager, where an attacker could cause a use-after-free for stack memory. A successful exploit o
	Microsoft is aware of a security feature bypass vulnerability in Windows publicly referred to as "YellowKey". The proof of concept for this vulnerability ha

CVE-2026-45585	Mitigation FAQs Should I leverage the temporary mitigation? Microsoft recommends that you consider implementing these mitigations if you are concerned your de implementing the mitigations? Implementing these mitigations will not impact service availability or management operations. Do customers need to revert the cha am I at risk of this vulnerability being exploited No, if you are using TPM+PIN the vulnerability is not exploitable.
CVE-2026-35593	Trilium Notes is an open-source, cross-platform hierarchical note taking application for building large personal knowledge bases. Versions 0.102.1 and prior are vul /api/attachments/{attachmentId}/upload-modified-file, replaces the content of the attachment with the content from another file (whose path is provided in filePat remote code execution and compromise of co-hosted applications. This issue has been fixed in version 0.102.2.
CVE-2026-42000	Insufficient Validation of Names During AXFR
CVE-2026-20171	A vulnerability in the Border Gateway Protocol (BGP) enforce-first-as feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switch could exploit this vulnerability by sending a crafted BGP update through an established BGP peer session. If the update propagates to an affected device, it could c
CVE-2026-39311	Trilium Notes is a cross-platform, hierarchical note taking application focused on building large personal knowledge bases. Versions 0.102.1 and prior contain a crit from an insecure-by-design architecture: Trilium serves SVG attachments with the image/svg+xml MIME type without any sanitization, and it explicitly disables Hel document body. With that token, it can send a signed request to /api/script/exec to execute arbitrary Node.js code on the server. An attacker can compromise the
CVE-2026-44707	Chatwoot is a customer engagement suite. From 2.14.0 to before 4.13.0, a Pre-Account Takeover (Pre-ATO) vulnerability existed in Chatwoot's authentication flow. Google OAuth (or another OmniAuth provider), the OAuth flow silently confirmed the existing account without invalidating the attacker's pre-set credentials. The at 4.13.0.
CVE-2018-25361	Soroush IM Desktop App 0.17.0 contains an authentication bypass vulnerability that allows local attackers to remove passcodes by injecting pre-encrypted databas
CVE-2026-44076	Insufficient sanitization of volume paths in Netatalk 3.1.0 through 4.4.2 allows a local privileged user to inject OS commands and execute arbitrary code via a craft
CVE-2021-21508	Dell VxRail versions before 7.0.200 contain a Plain-text Password Storage Vulnerability in VxRail Manager. A sys-admin user may exploit this vulnerability, leading t
CVE-2026-34926	A directory traversal vulnerability in the Apex One (on-premise) server could allow a pre-authenticated local attacker to modify a key table on the server to inject m credentials to the server via some other method to exploit this vulnerability.
CVE-2026-27768	SQL Injection affecting the Access Manager role.
CVE-2026-27427	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dylan Kuhn Geo Mashup allows Stored XSS. This issue affects
CVE-2022-34363	Dell Unisphere for PowerMax vApp version prior to 10.0.0.2, contains an authorization bypass vulnerability in the Unisphere for VMAX application running in vApp
CVE-2026-45435	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Melapress WP Activity Log allows DOM-Based XSS. This issue a
CVE-2026-45217	Authentication Bypass Using an Alternate Path or Channel vulnerability in ThemeHigh Stripe Payment Gateway for WooCommerce allows Password Recovery Explo
CVE-2026-39966	TypeBot is a chatbot builder tool. In versions 3.15.2, the getLinkedTypebots API endpoint returns full bot definitions to any authenticated user who references a tar access control predicate is never actually evaluated. Any authenticated Typebot user can read the full definition of any other workspace's private bots, including: a
CVE-2026-4915	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to filter nil elements from outgoing webhook attachment payl
CVE-2025-62745	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Team Showcase allows Stored XSS. This issue affec
CVE-2026-41863	Spring AI's support for Anthropic's Skills API used LLM-influenced filenames unsanitized in Path.resolve before writing files to disk. This could allow a malicious user
CVE-2026-46620	e107 is a content management system (CMS). Prior to 2.3.5, e107 CMS does not properly enforce CSRF token validation on comment moderation actions. The prob entirely. This vulnerability is fixed in 2.3.5.
CVE-2026-43934	e107 is a content management system (CMS). Prior to 2.3.4, a Broken Access Control vulnerability exists in the application, allowing an unauthorized authenticated confirming the requesting user’s ownership of the comment. This vulnerability is fixed in 2.3.4.
CVE-2026-48683	FastNetMon Community Edition through 1.2.9 contains an out-of-bounds read vulnerability in the NetFlow v9 data flowset processor. In src/netflow_plugin/netflow_ checks 'if (pkt + offset + field_template->total_length > packet_end)' before each iteration. The Data branch omits this check entirely. Since template definitions a

CVE-2026-42827	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to disclose information over
CVE-2026-25680	Parsing arbitrary HTML can consume excessive CPU time, possibly leading to denial of service.
CVE-2026-9354	A vulnerability was detected in NousResearch hermes-agent up to 2026.4.16. The affected element is an unknown function of the component Slack Agent/Matterm not respond in any way.
CVE-2026-48684	FastNetMon Community Edition through 1.2.9 contains an out-of-bounds read in the NetFlow v9 options template parser. In process_netflow_v9_options_template() step. No bounds check validates that (zone_address + scopes_offset + sizeof(record)) stays within the flowset. The same issue affects the options field loop (lines 2 packet buffer.
CVE-2026-4795	A missing authorization vulnerability in Zyxel GS1200-5v3 firmware versions through 1.00(ACPS.2)C0, GS1200-8v3 firmware versions through 1.00(ACPT.2)C0, GS1 the system configuration from a log file via a crafted HTTP request.
CVE-2026-24574	Cross-Site Request Forgery (CSRF) vulnerability in Recorp Export WP Page to Static HTML/CSS allows Cross Site Request Forgery. This issue affects Export WP Page
CVE-2026-48685	FastNetMon Community Edition through 1.2.9 has out-of-bounds memory access because it incorrectly parses BGP path attributes with the extended length flag se (attribute_value_length = value[2] at line 173). Per RFC 4271 Section 4.3, when the Extended Length bit is set, the Attribute Length field is two octets and the valu remaining 256 bytes are then misinterpreted as subsequent attributes, causing cascading parse failures and potential out-of-bounds memory access.
CVE-2026-28444	Typebot is a chatbot builder tool. In versions 3.15.2 and prior, the getResultLogs API endpoint authorizes the caller against the provided typebotId but fetches logs leaking sensitive data including HTTP response bodies, AI model outputs, and webhook payloads. Every other result-scoped endpoint in the same router properly v
CVE-2026-41401	libyang before 5.2.6 contains a heap use-after-free write vulnerability in lyd_parser_set_data_flags that incorrectly updates metadata list pointers when freeing non execution.
CVE-2026-48846	In Roundcube Webmail 1.6.x before 1.6.16 and 1.7.x before 1.7.1, the remote image blocking feature can be bypassed via a crafted CSS var() value in an e-mail m
CVE-2026-36227	Directory Traversal vulnerability in Easy Chat Server 3.1 allows a remote attacker to obtain sensitive information and execute arbitrary code via the UserName par
CVE-2026-48845	In Roundcube Webmail 1.6.x between 1.6.14 and 1.6.16 and 1.7.x before 1.7.1, remote image blocking was not honored for URLs pointing to local/private destinati
CVE-2026-39969	TypeBot is a chatbot builder tool. In versions 3.16.0 and prior, the WhatsApp Cloud API webhook endpoint (POST /v1/workspaces/{workspaceId}/whatsapp/{creden access logs, visible in Meta's webhook configuration dashboard, and potentially shared when configuring integrations. This allows any unauthenticated attacker to
CVE-2026-9351	A security flaw has been discovered in NousResearch hermes-agent up to 2026.4.16. This vulnerability affects the function _is_blocked_device of the file tools/file_t about this disclosure but did not respond in any way.
CVE-2026-41069	libheif is a HEIF and AVIF file format decoder and encoder. In versions 1.21.2 and prior, a malformed HEIF sequence file can trigger an out-of-bounds read in core se constructor still enters its loop. This leads to an out-of-bounds dereference on the empty chunks[0] in chunked mode.
CVE-2026-42763	Missing Authorization vulnerability in SePay team SePay Gateway allows Retrieve Embedded Sensitive Data. This issue affects SePay Gateway: from n/a through 1.
CVE-2026-24197	NVIDIA Display Driver for Linux contains a vulnerability in the Multi-Instance GPU (MIG) partition management, where an insecure default initialization of memory s
CVE-2026-39827	An authenticated SSH client that repeatedly opened channels which were rejected by the server caused unbounded memory growth, eventually crashing the serve
CVE-2026-20238	In Splunk AI Toolkit versions below 5.7.3, a low-privileged user that does not hold the 'admin' or 'power' roles could access confidential data that was restricted thr with the `OR` SPL operator, the injected filter overrides more restrictive filters on child roles.
CVE-2026-20240	In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.11, and 9.3.12, and Splunk Cloud Platform versions below 10.4.2603.1, 10.3.2512.9, 10.2.2510.11, 10.1.250 Splunk directories, making the instance non-functional. The Denial of Service is possible because of missing input validation in the `coldToFrozen.sh` scri
CVE-2026-8140	Concrete CMS 9.5.0 and below does not validate a CSRF token before processing requests to /dashboard/extend/install/download/<remoteId>. The download() met endpoint is a state-changing GET route with no token enforcement, an attacker who can cause an authenticated administrator to visit a crafted page can force an a vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N. Thanks https://github.com/maru1009 for re
CVE-2026-44054	Netatalk 2.0.0 through 4.4.2 generates AFP session tokens derived from predictable process IDs, which allows a remote authenticated attacker to cause a denial of

CVE-2026-8435	Concrete CMS 9 before 9.5.0 is vulnerable to Cross Site Request Forgery (CSRF) at concrete/controllers/backend/file approveVersion(). The Concrete CMS security t
CVE-2026-43620	Rsync version 3.4.2 and prior contain a receiver-side out-of-bounds array read vulnerability in recv_files() in receiver.c that allows a malicious rsync server to crash record with ndx=0 and an iflag word without ITEM_TRANSFER, causing the receiver to read 8 bytes before the allocated pointer array and dereference an invalid po
CVE-2026-9603	A security vulnerability has been detected in SourceCodester eDoc Doctor Appointment System 1.0. This affects an unknown part of the file /admin/delete-session.
CVE-2026-9122	Out of bounds read in GPU in Google Chrome on Mac prior to 148.0.7778.179 allowed a remote attacker to obtain potentially sensitive information from process me
CVE-2026-6072	The Oliver POS – A WooCommerce Point of Sale (POS) plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to 'OliverAuth' header value against the 'oliver_pos_authorization_token' option. On fresh installations where the admin has not yet completed the connection flow, th to all POS API endpoints, enabling attackers to read user data (including administrator details), update user profiles (including email addresses), and delete non-ad
CVE-2026-24182	NVIDIA Display Driver for Windows and Linux contains a vulnerability where an attacker could leak held driver locks. A successful exploit of this vulnerability might
CVE-2026-44836	view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. From 3.0.0 to 4.9.0, the preview route derives ViewComponent::Preview are route-reachable. The most important one is render_with_template, which accepts template: and locals:. Those values can come from
CVE-2026-5072	A bitwise shift vulnerability in Zephyr's PTP subsystem allows a remote attacker to cause undefined behavior and potential system crashes. An attacker sends a cra timeout as NSEC_PER_SEC >> -log_seconds; if the attacker-supplied value is sufficiently negative (e.g., -127), the shift amount exceeds the 64-bit integer width, tr
CVE-2026-9150	A flaw was found in libsolv. This stack-based buffer overflow vulnerability occurs in libsolv's Debian metadata parser when processing specially crafted Debian repo
CVE-2026-27405	Missing Authorization vulnerability in Magepeople inc. WpBookingly allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WpBo
CVE-2026-44213	The OpenTelemetry.Exporter.Instana exports telemetry to Instana backend. Prior to 1.1.0, the OpenTelemetry.Exporter.Instana NuGet package does not validate H connection, all OpenTelemetry telemetry data and the Instana API key are exposed to the attacker. This vulnerability is fixed in 1.1.0.
CVE-2026-24573	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Visualizer allows Stored XSS. This issue affects Visua
CVE-2026-45254	In the case of the cap_net service, when a key present in the old limit was omitted from the new limit, the missing key was treated as "allow any" instead of being
CVE-2026-21836	The HCL DominoIQ RAG feature is affected by a Broken Access Control vulnerability. Under certain circumstances, document level access restrictions will be ignore
CVE-2026-8487	Incorrect default permissions vulnerability in Progress Software MOVEit Automation allows Retrieve Embedded Sensitive Data. This issue affects MOVEit Automatio
CVE-2026-39593	Missing Authorization vulnerability in VillaTheme HAPPY allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HAPPY: from n/a
CVE-2026-48710	Starlette is a lightweight ASGI framework/toolkit. Prior to version 1.0.1, the HTTP `Host` request header was not validated before being used to reconstruct `reques endpoints that apply security restrictions based on `request.url` (rather than the raw `scope` path) could therefore be bypassed. Users should upgrade to a versio
CVE-2026-4635	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to archive the channel before removing persistent notificatio 00637
CVE-2026-47672	epa4all-client is the Java Client for epa4all / ePA 3.0 in the Telematik Infrastruktur. In 1.2.4 and earlier, any network-reachable caller can write arbitrary documents credentials.
CVE-2026-9149	A flaw was found in libsolv. This heap buffer overflow vulnerability occurs when a victim processes a specially crafted `.solv` file containing negative size values in
CVE-2026-44923	SQL injection in InfoScale VIOM before v9.1.3 allows remote attackers to escalate privileges.
CVE-2026-40102	Plane is an open-source project management tool. In versions 1.3.0 and below, SavedAnalyticEndpoint passes the user-controlled segment query parameter direct /api/workspaces/<slug>/saved-analytic-view/<analytic_id>/ with a crafted segment value that is forwarded into build_graph_plot() and traverses foreign-key relati tokens, and related users' email addresses, making it a stronger primitive than the related order_by injection where values are only leaked through ordering. This i
CVE-	

2026-5755	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.2, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to validate the TIFF IFD offset in the image ID: MMSA-2026-00648
CVE-2026-8685	The Infility Global plugin for WordPress is vulnerable to SQL Injection via the 'orderby' and 'order' parameters in all versions up to, and including, 2.15.16. This is du capability. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queri
CVE-2025-36126	IBM Cognos Analytics 11.2.0, 12.0, and 12.1.0 and IBM Cognos Transformer 12.0, 11.2.4, and 12.1.0 is vulnerable to stored cross-site scripting (XSS) in Cognos Adr
CVE-2026-35070	Dell SmartFabric Storage Software, versions prior to 1.4.5, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vuln
CVE-2026-7887	For Concrete CMS 9.5.0 and below, OAuth 2.0 Authorization-Code Handler Bypasses Account Status. A user with uIsActive=0 (suspended, banned, terminated emp Thanks 0x4c616e for reporting.
CVE-2026-7890	In Concrete CMS 9.5.0 and below, the RSS Displayer block accepts a feed URL from any page editor and fetches it server-side without validation enabling redirect-t
CVE-2026-44056	A stack-based buffer overflow in desktop.c in Netatalk 1.3 through 4.2.2 allows a remote authenticated attacker to cause a denial of service, obtain limited informa
CVE-2026-6397	The Sticky plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `cvmh-sticky` shortcode `readmoretext` attribute in versions up to and includin without any escaping function such as `esc_html()`. This makes it possible for authenticated attackers with Contributor-level access and above to inject arbitrary w
CVE-2026-8038	The Faces of Users plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'default' shortcode attribute in the 'facesofusers' shortcode in all versio whenever a user accesses an injected page.
CVE-2026-1543	The Avada (Fusion) Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple shortcodes in all versions up to, and including, 3.15.2 due administrator) accesses a page displaying dynamic user data (such as via the Dynamic Data feature pulling user biographical information).
CVE-2026-6549	The Logo Manager For Enamad plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' attribute of the `vc_enamad_namad`, `vc_enamad_sh contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2026-9104	The Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Draft Post Title in all versions up to, and including, 2.6.3 due to insufficient input injection path is triggered specifically when the viewing user lacks edit capabilities, meaning payloads embedded in draft post titles via attribute-breakout techniqu
CVE-2026-7509	The KIA Subtitle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `the-subtitle` shortcode `before` and `after` attributes in all versi scripts in pages that will execute whenever a user accesses an injected page.
CVE-2026-5293	The 診断ジェネレータ作成プラグイン (Diagnosis Generator) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'js' parameter in versions up to ar allowing any authenticated user (including subscribers) to save malicious JavaScript to theme files. Additionally, the save() function uses stripslashes() which remo containing the diagnosis form shortcode.
CVE-2026-9087	A flaw was found in Keycloak. The cross-session verification proof is keyed only by (local userId, idpAlias) and is not bound to the upstream identity that was actual
CVE-2026-2955	The AI Chatbot & Workflow Automation by AIWU plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'X-Forwarded-For' header in versions up to NOTE: Practical exploitation is constrained due to a 20-character storage limit.
CVE-2026-9531	A weakness has been identified in Totolink CA750-PoE 6.2c.510. Impacted is the function setUpgradeUboot of the file /cgi-bin/cstecgi.cgi of the component Setting
CVE-2026-9362	A security vulnerability has been detected in Edimax EW-7438RPn 1.12. This vulnerability affects the function formConnectionSetting of the file /goform/formConne vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9361	A weakness has been identified in Edimax EW-7438RPn 1.12. This affects the function formAccept of the file /goform/formAccep of the component POST Request H this disclosure but did not respond in any way.
CVE-2026-9359	A vulnerability was identified in Edimax EW-7438RPn 1.28a. Affected by this vulnerability is the function formHwSet of the file /goform/formHwSet of the componer The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9484	A vulnerability was determined in SourceCodester Student Grades Management System 1.0. Affected by this vulnerability is the function getClassroomStudents/rer utilized.
CVE-2026-9363	A vulnerability was detected in Edimax EW-7438RPn 1.12. This issue affects the function formEZCHNwlanSetup of the file /goform/formEZCHNwlanSetu of the comp about this disclosure but did not respond in any way.
CVE-	

2026-9472	A flaw has been found in dazeb markdown-downloader up to 3d4394b34b6c99d81af817623af55e3384df5a6a. Affected is the function download_markdown/list_do 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
CVE-2026-9473	A vulnerability has been found in c-rick jimeng-mcp 1.10.0. Affected by this vulnerability is the function getFileContent/uploadCoverFile/generateImage/generateVi through an issue report but has not responded yet.
CVE-2026-9497	A flaw has been found in changmingxie tcc-transaction up to 2.1.0. This issue affects the function Fastjson.parseObject of the component Fastjson AutoType REST /
CVE-2026-24142	NVIDIA TRT-LLM for any platform contains a deserialization vulnerability and unsafe serialized handle. A successful exploit of this vulnerability might lead to code e
CVE-2026-1816	Improper restriction of excessive authentication attempts vulnerability in Turkiye Electricity Transmission Corporation (TEİAŞ) Mobile Application allows Brute Force
CVE-2026-9347	A vulnerability has been found in Edimax EW-7438RPn up to 1.31. Affected is the function formWizSurvey of the file /goform/formWizSurvey of the component web disclosure but did not respond in any way.
CVE-2026-9524	A flaw has been found in xianrendzw EasyReport up to 2.0.17.0522_Beta. Affected by this issue is the function execute of the component REST Endpoint. Executing
CVE-2026-9305	A weakness has been identified in QuantumNous new-api up to 0.12.1. The impacted element is the function SearchUserTopUps/SearchAllTopUps of the file model/ this disclosure but did not respond in any way.
CVE-2026-9299	A flaw has been found in omec-project amf up to 2.1.1. Affected by this issue is the function PDUSessionResourceModifyIndication of the file /go/src/amf/ngap/hand
CVE-2026-9468	A security flaw has been discovered in dazeb cline-mcp-memory-bank up to 55c81b9cf6c16700983c84dc4cdea3cafa19a75f. The affected element is the function h attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. Th
CVE-2026-9379	A weakness has been identified in Edimax BR-6675nD 1.12. This impacts the function formWpsStart of the file /goform/formWpsStart of the component POST Requ about this disclosure but did not respond in any way.
CVE-2026-9378	A security flaw has been discovered in Edimax BR-6675nD 1.12. This affects the function formHwSet of the file /goform/formHwSet of the component POST Reques may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9302	A vulnerability was determined in 546669204 vps-inventory-monitoring up to 98c00b370668c96ae75e91c15548d9ea113652d9. This issue affects the function eva and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not c
CVE-2026-9301	A vulnerability was found in omec-project amf up to 2.1.1. This vulnerability affects unknown code of the component NGReset Message Handler. Performing a mani
CVE-2026-9376	A vulnerability was determined in JPress up to 1.0.3. The affected element is an unknown function of the file /ucenter/article/doWriteSave of the component UCente was informed of the problem early through an issue report but has not responded yet.
CVE-2026-9374	A vulnerability was found in yangzongzhuan RuoYi-Vue up to 3.9.2. Impacted is the function FileUploadUtils.upload of the file /common/upload of the component Co
CVE-2026-9300	A vulnerability has been found in omec-project amf up to 2.1.1. This affects an unknown part of the component NGSetupRequest Handler. Such manipulation leads
CVE-2026-9296	A weakness has been identified in Edimax BR-6428NS 1.10. This impacts the function system of the file /goform/formWlanM of the component POST Request Handl ateFunc/ateGain/ateTxCount/ateChan/ateRate/ateMacID/e2pTxPower1/e2pTxPower2/e2pTxPower3/e2pTxPower4/e2pTxPower5/e2pTxPower6/e2pTxPower7/e2pTx2 can lead to command injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor
CVE-2026-9483	A vulnerability was found in SourceCodester Student Grades Management System 1.0. Affected is an unknown function of the file grades.php. Performing a manipu
CVE-2026-9297	A security vulnerability has been detected in Edimax BR-6428NS 1.10. Affected is the function formWlbasic of the file /goform/formWlbasic of the component POST disclosure but did not respond in any way.
CVE-2026-9298	A vulnerability was detected in omec-project amf up to 2.1.1. Affected by this vulnerability is an unknown functionality of the component PathSwitchRequest Handl
CVE-2026-27331	Missing Authorization vulnerability in Magepeople inc. WpTravelly allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WpTrav
CVE-	

2026-9343	A weakness has been identified in Edimax EW-7438RPn up to 1.31. The affected element is the function formWpsStart of the file /goform/formWpsStart of the comp contacted early about this disclosure but did not respond in any way.
CVE-2026-9498	A vulnerability has been found in Dromara lamp-cloud up to 5.6.2. Impacted is the function GroovyClassLoader.parseClass of the component Message Template Ha and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9441	A security flaw has been discovered in Edimax BR-6478AC 1.23. Affected by this issue is the function formiNICbasic of the file /goform/formiNICbasic of the compor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9440	A vulnerability was identified in Edimax BR-6478AC 1.23. Affected by this vulnerability is the function formAccept of the file /goform/formAccept of the component disclosure but did not respond in any way.
CVE-2026-9445	A flaw has been found in SourceCodester Simple POS and Inventory System 1.0. Impacted is an unknown function of the file /admin/addproduct.php of the compon
CVE-2026-9439	A vulnerability was determined in Edimax BR-6675nD 1.12. Affected is the function stainfo of the file /goform/stainfo. This manipulation of the argument interface c
CVE-2026-9437	A vulnerability has been found in DTStack Taier 1.4.0. This affects the function Runtime.exec of the component REST API. The manipulation of the argument sqlTex
CVE-2026-9579	A vulnerability was found in JeecgBoot up to 3.9.1. Impacted is the function user.getUsername of the file /sys/user/login/setting/userEdit of the component SysUser issue. The affected component should be upgraded.
CVE-2026-43619	Rsync version 3.4.2 and prior contain symlink race condition vulnerabilities in path-based system calls including chmod, lchown, utimes, rename, unlink, mkdir, syr execution by swapping symlinks to apply sender-supplied permissions, ownership, timestamps, or filenames to arbitrary files outside the intended module boundar
CVE-2026-9511	A vulnerability was identified in Totolink CA750-PoE 6.2c.510. This affects the function setWebWlanIdx of the file /cgi-bin/cstecgi.cgi of the component Setting Hanc
CVE-2026-9581	A vulnerability was identified in JeecgBoot up to 3.9.1. The impacted element is an unknown function of the file /sys/comment/add. Such manipulation leads to imp
CVE-2026-9532	A security vulnerability has been detected in Totolink CA750-PoE 6.2c.510. The affected element is the function setUploadUserData of the file /cgi-bin/cstecgi.cgi of
CVE-2026-9449	A vulnerability was identified in code-projects Employee Management System 1.0. This impacts an unknown function of the file /changepassemp.php. The manipula
CVE-2026-9424	A weakness has been identified in Edimax EW-7438RPn 1.31. The affected element is the function formWlanMP of the file /goform/formWlanMP of the component C ateFunc/ateGain/ateTxCount/ateChan/ateRate/ateMacID/e2pTxPower1/e2pTxPower2/e2pTxPower3/e2pTxPower4/e2pTxPower5/e2pTxPower6/e2pTxPower7/e2pTx2 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 ver
CVE-2026-9450	A security flaw has been discovered in code-projects Employee Management System 1.0. Affected is an unknown function of the file /psubmit.php. The manipulatio
CVE-2026-9420	A vulnerability was found in KLiK SocialMediaWebsite 1.0. This affects an unknown part of the component HTTP GET Request Parameter Handler. The manipulation
CVE-2026-9451	A weakness has been identified in code-projects Employee Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /process/a
CVE-2026-42776	Missing Authorization vulnerability in WP Sunshine Sunshine Photo Cart allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects S
CVE-2026-39828	When an SSH server authentication callback returned PartialSuccessError with non-nil Permissions, those permissions were silently discarded, potentially dropping
CVE-2026-9542	A weakness has been identified in CodeAstro Leave Management System 1.0. The affected element is an unknown function of the file /admin/add_staff.php. Execut
CVE-2026-9412	A vulnerability was determined in SourceCodester Indian Invoicing System 1.0. Impacted is an unknown function of the component Backend Endpoint. Executing a
CVE-2026-9512	A security flaw has been discovered in Totolink CA750-PoE 6.2c.510. This vulnerability affects the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the com
CVE-	

2026-9513	A weakness has been identified in Totolink CA750-PoE 6.2c.510. This issue affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi of the component Se
CVE-2026-9514	A security vulnerability has been detected in Totolink CA750-PoE 6.2c.510. Impacted is the function setNetworkDiag of the file /cgi-bin/cstecgi.cgi of the componen NetDiagHost/NetDiagPingNum/NetDiagPingSize/NetDiagPingTimeOut/NetDiagTracertHop leads to os command injection. The attack may be initiated remotely. The
CVE-2026-20206	A vulnerability in the BrowserBot component of Cisco ThousandEyes Enterprise Agent could have allowed an authenticated, remote attacker to execute arbitrary co insufficient input validation of command arguments that are supplied by the user. Prior to this vulnerability being addressed, an attacker could have exploited this the node user. To exploit this vulnerability, the attacker must have valid user credentials for the ThousandEyes SaaS and the ability to manage transaction tests.
CVE-2026-9515	A vulnerability was detected in Totolink CA750-PoE 6.2c.510. The affected element is the function setUnloadUserData of the file /cgi-bin/cstecgi.cgi of the compone
CVE-2026-9411	A vulnerability was found in SourceCodester Indian Invoicing System 1.0. This issue affects some unknown processing of the file /Invoicing/IGST_Invoice.php of the
CVE-2026-9342	A security flaw has been discovered in SourceCodester Hospitals Patient Records Management System 1.0. Impacted is an unknown function of the file /admin/pati
CVE-2026-9534	A flaw has been found in Totolink CA750-PoE 6.2c.510. This affects the function setWiFiWpsConfig of the file /cgi-bin/cstecgi.cgi of the component Setting Handler.
CVE-2026-9402	A vulnerability was found in Edimax BR-6675nD 1.12. The affected element is the function formWlanMP of the file /goform/formWlanMP of the component POST Rec ateFunc/ateGain/ateRate/ateChan/ateTxCount/e2pTx2Power1/e2pTx2Power2/e2pTx2Power3/e2pTx2Power4/e2pTx2Power5/e2pTx2Power6/e2pTx2Power7/e2pTxPo results in command injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about th
CVE-2026-9533	A vulnerability was detected in Totolink CA750-PoE 6.2c.510. The impacted element is the function recvUpgradeNewFw of the file /cgi-bin/cstecgi.cgi of the compor
CVE-2026-9400	A flaw has been found in Edimax BR-6675nD 1.12. This issue affects the function formUSBStorage of the file /goform/formUSBStorage of the component POST Requ disclosure but did not respond in any way.
CVE-2026-9565	A vulnerability was determined in haojing8312 WorkClaw up to 0.6.4. This affects the function is_dangerous of the file apps/runtime/src-tauri/src/agent/tools/bash.r early through an issue report but has not responded yet.
CVE-2026-36189	Buffer Overflow vulnerability in Uncrustify Project Affected v.Uncrustify_d-0.82.0-132-bcc41cbdc and Fixed in commit 68e67b9a1435a1bb173b106fedb4a4f510972
CVE-2018-25367	NASA openVSP 3.16.1 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the geo
CVE-2026-8852	IBM HTTP Server 8.5, and 9.0 is vulnerable to denial of service via the optional module mod_fastcgi module.
CVE-2018-25369	Visual Ping 0.8.0.0 contains a buffer overflow vulnerability in input field handling that allows local attackers to crash the application by supplying oversized data. At
CVE-2018-25378	Notebook Pro 2.0 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the noteboo
CVE-2026-42627	In Arm ArmNN through 2026-03-27, an integer overflow in TensorShape::GetNumElements() in armnn/Tensor.cpp allows a crafted TFLite model file to bypass buffe an understated allocation size. During Optimize()->InferOutputShapes(), the BatchToSpaceNdLayer reads beyond the allocated buffer.
CVE-2026-44897	Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.2.1, HTMLRenderer.heading() builds the opening <hN> tag by string-concatenating the attributes (event handlers, src=, href=, etc.) into the heading element. This vulnerability is fixed in 3.2.1.
CVE-2026-22880	Mattermost Mobile Apps versions <=2.37 11.4 2.0.37 11.0.4 11.1.3 11.3.2 10.11.11.0 fail to properly validate the SSO authentication callback origin which allows a
CVE-2026-30691	Cross-Site Scripting (XSS) vulnerability in @cyntler/react-doc-viewer v1.17.1 allows remote attackers to execute arbitrary JavaScript via a crafted .txt file. The TXTR
CVE-2026-45249	A cross-site scripting (XSS) vulnerability exists in Apache ECharts in the Lines series tooltip rendering logic. This issue affects Apache ECharts: from before 6.1.0. In tooltip content. Although tooltip is allowed to accept user-provided raw HTML via a custom tooltip.formatter, the built-in tooltip formatters conventionally perform H fixes the issue.
CVE-2026-26028	CryptPad is an end-to-end encrypted collaborative office suite. In versions prior to 2026.2.0, the HTML sanitizer in Diffmarked.js can be bypassed due to incomplete completely defeating CryptPad's intended bounce sandboxing and enabling link injection or other interactive content within user-controlled documents. The root ca pairing a benign blob: src with a malicious srcdoc results in unrestricted rendering. This issue has been fixed in version 2026.2.0.
CVE-	

2026-44708	Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.2.1, the mistune math plugin renders inline math ($...$) and block math ($$...$$) by co sanitised before reaching the DOM. This vulnerability is fixed in 3.2.1.
CVE-2026-5776	The Email Encoder WordPress plugin before 2.4.7 does not escape email addresses retrieved via user input, allowing unauthenticated attackers to perform Stored
CVE-2026-47099	TeleJSON prior to 6.0.0 contains a DOM-based cross-site scripting vulnerability in the parse() function that allows attackers to execute arbitrary JavaScript by delive to inject arbitrary JavaScript through vectors such as postMessage in cross-frame communication contexts to achieve script execution within the application.
CVE-2026-44898	Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.2.1, render_toc_ul() builds a table-of-contents tree from a list of (level, id, text) tu from user-supplied heading text (the standard use-case for readable slug anchors), an attacker can craft a heading whose text breaks out of the href="#..." attribu
CVE-2026-27136	Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications t
CVE-2026-40295	Devise is an authentication solution for Rails based on Warden. In versions 5.0.3 and below, when the Timeoutable module is enabled in Devise, the FailureApp#re cross-origin form can cause a victim with an expired Devise session to be redirected to an arbitrary external URL. This contrasts with the GET timeout path (which session users can be silently redirected from the trusted app domain to attacker-controlled URLs, enabling phishing and malware delivery while bypassing browser config.action_controller.action_on_open_redirect = :raise (and the older raise_on_open_redirects setting) do not reach it. This issue has been fixed in version 5.0.4.
CVE-2026-8627	The Correct Prices plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the $_SERVER['PHP_SELF'] variable in versions up to and including 1.0. T path-info appended to the script URL, an attacker can break out of the attribute and inject arbitrary markup. This makes it possible for unauthenticated attackers t
CVE-2026-8626	The SponsorMe plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PHP_SELF Parameter in all versions up to, and including, 0.5.2 due to insuffi The PHP_SELF value is reflected in two separate locations within the vulnerable function — a form action attribute and an anchor href attribute — both of which car
CVE-2026-42506	Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications t
CVE-2026-25681	Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications t
CVE-2026-6864	The CBX 5 Star Rating & Review plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 1. such as clicking on a link.
CVE-2026-36226	Cross Site Scripting vulnerability in Advantech WebAccess/SCADA 8.0-2015.08.16 allows a remote attacker to obtain sensitive information via the decryption field i
CVE-2026-8624	The LJ comments import: reloaded plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PHP_SELF Parameter in all versions up to, and including, as clicking on a link. The vulnerability arises specifically because PHP_SELF includes attacker-controllable PATH_INFO appended to the script name, and there are t
CVE-2026-48903	Inadequate content filtering within the checkAttribute methods leads to XSS vulnerabilities in various components.
CVE-2026-48905	Lack of input filtering leads to an XSS vector in the HTML filter code.
CVE-2026-8420	The BLOGCHAT Chat System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.6.3. This is due to missing or such as clicking on a link.
CVE-2018-25349	userSpice 4.3.24 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through the X-Forwarded-For HTTP header. Attackers c
CVE-2026-3481	The WP Blockade plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shortcode' parameter in all versions up to and including 0.9.14. This i directly via echo do_shortcode($shortcode) on line 393. When the input is not a valid WordPress shortcode (e.g., an HTML tag with JavaScript event handlers), do_s account. There is no nonce verification or additional capability check. This makes it possible for authenticated attackers, with Subscriber-level access and above, t
CVE-2025-26483	Dell PowerFlex Manager, versions 4.6.2 and prior, contains an Open Redirect Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability,
CVE-2026-7462	The VatanSMS WP SMS plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `page` parameter in all versions up to, and including, 1.01. This such as clicking on a link.
CVE-2026-6395	The Word 2 Cash plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Stored Cross-Site Scripting in versions up to and including 0.9.2. This w2c-definitions POST parameter is saved raw via update_option() and later echoed without escaping inside a <textarea> element. This makes it possible for unaut
CVE-2026-6391	The Sentence To SEO (keywords, description and tags) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. Th trick a site administrator into performing an action such as clicking on a link.

CVE-2026-42502	Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications t
CVE-2026-0857	Cleartext Storage of Sensitive Information in Memory vulnerability in Mesalvo Meona Client Launcher Component, Mesalvo Meona Server Component. This issue aft
CVE-2026-48249	Open ISES Tickets before 3.44.2 disables TLS certificate verification in rm/incs/mobile_login.inc.php by setting CURLOPT_SSL_VERIFYPEER to false (and not setting C to intercept, monitor, or modify the request and response, including any API keys or session-bearing data in transit.
CVE-2026-48248	Open ISES Tickets before 3.44.2 disables TLS certificate verification in incs/login.inc.php by setting CURLOPT_SSL_VERIFYPEER to false (and not setting CURLOPT_S monitor, or modify the request and response, including any API keys or session-bearing data in transit.
CVE-2026-48247	Open ISES Tickets before 3.44.2 disables TLS certificate verification in incs/functions.inc.php by setting CURLOPT_SSL_VERIFYPEER to false (and not setting CURLOP can present a forged certificate to intercept, monitor, or modify the request and response, including any API keys or session-bearing data in transit.
CVE-2026-48246	Open ISES Tickets before 3.44.2 disables TLS certificate verification in ajax/reports.php by setting CURLOPT_SSL_VERIFYPEER to false (and not setting CURLOPT_SS forged certificate to intercept, monitor, or modify the request and response, including any API keys or session-bearing data in transit.
CVE-2026-44061	Netatalk 1.5.0 through 4.4.2 uses DES-ECB for authentication with a timing side channel, which allows a remote attacker to recover authentication credentials via t
CVE-2026-44837	view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. From 3.0.0 to 4.9.0, the system test entrypoi vulnerability is fixed in 4.9.0.
CVE-2026-44788	SharpCompress is a fully managed C# library to deal with many compression types and formats. In 0.47.4 and earlier, a path traversal vulnerability in IArchive.Wri filesystem subject to the permissions of the running process.
CVE-2026-8673	Unprotected transport of credentials vulnerability in syslink software AG Avantra on Linux, Windows allows Sniffing Attacks. This issue affects Avantra: before 25.3.
CVE-2026-9100	The MongoDB C Driver's legacy GridFS API accepts malformed file metadata from the database without adequate validation. Crafted documents in a GridFS collecti
CVE-2026-5434	Honeywell Control Network Module (CNM) contains insertion of sensitive information into an unintended directory. An attacker could exploit this vulnerability throu
CVE-2022-31231	Dell ECS, versions 3.5 and 3.6, contain an Improper Access Control in the Identity and Access Management (IAM) module. A remote unauthenticated attacker may
CVE-2026-42626	HP ENVY 5000 series printers VERBASPP1N003.2237A.00 do not properly manage concurrent TCP connections to port 9100 (JetDirect/RAW printing). An unauthenti and concurrent session limits, resulting in a persistent Denial of Service (DoS) that renders the printer unresponsive to all user commands and print jobs. Physical i
CVE-2026-42002	Concurrency and locking defects in GSS-TSIG
CVE-2026-44833	Snipe-IT is an IT asset/license management system. Prior to 8.4.1, an open redirect vulnerability in Snipe-IT allows attackers to redirect users to malicious sites via
CVE-2026-3473	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to validate file ownership and access control, which allows an
CVE-2026-44608	NLnet Labs Unbound 1.14.0 up to and including version 1.25.0 has a locking inconsistency vulnerability that when certain conditions are met (multi-threaded, RPZ zone with 'rpz-nsip'/'rpz-nsdname' triggers and an ongoing XFR for that RPZ zone. Local RPZ files do not trigger the vulnerability. If the timing is right and an XFR h 1.25.1 contains a patch with a fix to the locking code.
CVE-2026-8485	Uncontrolled Memory Allocation vulnerability in Progress Software MOVEit Automation allows Excessive Allocation. This issue affects MOVEit Automation: before 20
CVE-2026-7385	The Decent Comments WordPress plugin before 3.0.2 does not restrict access to comment author email addresses and post author email addresses via its REST AP
CVE-2026-44214	eventsource-encoder encodes events as well-formed EventSource/Server Sent Event (SSE) messages. Prior to 1.0.2, eventsource-encoder does not sanitize the eve stream. This vulnerability is fixed in 1.0.2.
CVE-2026-24201	NVIDIA vGPU software contains a vulnerability in the virtual GPU manager, where an attacker could cause an out-of-bound access. A successful exploit of this vulne

CVE-2026-44409	There is an an information disclosure vulnerability in ZTE MU5250. Due to improper configuration of the access control mechanism, attackers can obtain informatio
CVE-2026-1815	Insufficient session expiration vulnerability in Turkiye Electricity Transmission Corporation (TEİAŞ) Mobile Application allows Session Hijacking. This issue affects Mo
CVE-2026-8174	Zohocorp Zoho Mail wordpress plugin is vulnerable to Cross-Site request forgery (CSRF). This issue affects Zoho Mail wordpress plugin versions before 1.6.2.
CVE-2026-24215	NVIDIA Triton Inference Server contains a vulnerability in the DALI backend, where an attacker could cause uncontrolled resource consumption. A successful exploi
CVE-2026-24198	NVIDIA GPU Display Driver for Linux contains a vulnerability where an advanced attacker could use a race condition to leak sensitive memory, which might cause li
CVE-2026-9371	A security vulnerability has been detected in ItzCrazyKns Vane up to 1.12.1. Affected by this issue is some unknown functionality of the file route.ts of the compone appears that basic authentication is planned.
CVE-2026-48134	When the DLP is active, the UserCheck Web Portal contains an input-handling issue in the UserChoice flow. Under specific conditions, an attacker who can access t resource impact if the issue is abused repeatedly. Exposure is reduced if the UserCheck Portal is not accessible from untrusted networks.
CVE-2026-9365	A vulnerability has been found in Ettercap up to 0.8.3. The affected element is the function FUNC_DECODER of the file src/dissectors/ec_gg.c of the component GG been disclosed to the public and may be used. Upgrading to version 0.8.4 is sufficient to fix this issue. The identifier of the patch is feeae6fa366e01a3dd9f1857ec6
CVE-2025-13755	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) stores potentially sensitive information in lo
CVE-2026-39309	Trilium Notes is a cross-platform, hierarchical note taking application focused on building large personal knowledge bases. In versions 0.102.1 and prior, the Electro RunAsNode fuse allows launching the app in a special Node.js mode using -e to execute arbitrary system commands with Trilium Notes's permissions and identity. Trilium rather than the attacker's code, because macOS treats the subprocess as part of the parent application. Exploitation allows access to TCC-protected resour
CVE-2025-32751	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Insecure Storage of Sensitive Information vulnerability. A low privileged attacker with local access could
CVE-2026-24160	NVIDIA TRT-LLM for any platform contains a vulnerability where an attacker could cause an unchecked return value to a null pointer dereference. A successful expl
CVE-2026-40610	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. In versions 1.4.38 and prior, the build packaging workflo place a symlink such as loot.txt -> /tmp/outside-marker.txt or a link to a more sensitive local file. When bentoml build runs, BentoML dereferences the symlink and secrets such as cloud credentials, SSH keys, API tokens, environment files, or other sensitive local configurations. Because Bento artifacts are commonly exported,
CVE-2026-48693	FastNetMon Community Edition through 1.2.9 is vulnerable to a local symlink attack via predictable file paths in /tmp. The statistics file path defaults to '/tmp/fastn chmod() call on line 2190 always operates on cli_stats_file_path regardless of which file_path parameter was passed (a bug that applies wrong permissions), and th
CVE-2026-45252	When a fusefs file system implements extended attributes, the kernel may send a FUSE_LISTXATTR message to the userspace daemon to retrieve the list of extend terminated. If a malicious daemon sends a non-NUL-terminated list, the fusefs kernel module may read beyond the end of one heap-allocated buffer and potentially
CVE-2026-44924	InfoScale VIOM 9.1.3 allows XSS.
CVE-2026-39964	TypeBot is a chatbot builder tool. In versions prior to 3.16.0, the Typebot viewer (packages/embeds/js) renders anchor tags from rich text bubble content without fi runs in the host page's origin and can exfiltrate cookies and session tokens. This can result in any authenticated Typebot user (including those on the free tier) bei
CVE-2026-32389	Missing Authorization vulnerability in Linethemes NanoCare allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects NanoCare: fro
CVE-2026-7798	The FluentCRM – Email Newsletter, Automation, Email Marketing, Email Campaigns, Optins, Leads, and CRM Solution plugin for WordPress is vulnerable to Blind Se and can be used to query and modify information from internal services. Exploitation requires that the SES bounce handling key ('_fc_bounce_key') has never been and reject unauthenticated requests.
CVE-2026-9251	Missing authorization in the entry status management feature in Devolutions Server allows a non-administrator authenticated user to bypass the administrator-enf
CVE-2026-9438	A vulnerability was found in yashpokharna2555 StudentManagementSystem cb2f558ddf8d19396de0f92abf2d224d46a0a203. This impacts an unknown function of release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem
CVE-2026-24586	Missing Authorization vulnerability in Themeansar Newses allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Newses: from

CVE-2026-28735	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to validate the OAuth token scope on the callback which allow
CVE-2026-8381	A broken access control vulnerability exists in the TeamViewer DEX Platform (On-Premises) prior version 9.2. Certain backend API endpoints do not correctly enforc access to administrative or sensitive functionality.
CVE-2026-48214	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in add_nm.php that allows authenticated attackers to inject arbitrary JavaScri executes in the victim's browser when the response is rendered.
CVE-2025-14290	IBM webMethods Integration (on prem) -Integration Server 10.15 through IS_10.15_Core_Fix2611.1 to IS_11.1_Core_Fix10 IBM webMethods Integration is vulnerabl
CVE-2026-6394	The Nexa Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Server-Side Request Forgery (SSRF) in versions or private network destinations. The nexa_blocks_nonce required for the AJAX action is publicly exposed in the HTML source of any frontend page where the plugin server-side HTTP requests to arbitrary internal or external destinations, potentially exposing internal services, cloud metadata endpoints such as the AWS instance a second wp_remote_get() call, allowing chained exploitation through a crafted JSON payload.
CVE-2026-48224	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ics214.php that allows authenticated attackers to inject arbitrary JavaScript browser when the response is rendered.
CVE-2026-48230	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ticketsmdb_import.php that allows authenticated attackers to inject arbitra input value attributes. Attackers can craft a malicious request containing a JavaScript payload that executes in the victim's browser when the response is rendered
CVE-2026-9056	A stored cross-site scripting vulnerability has been found in the Talend Administration Center. An attacker with permission to manage servers can store a XSS payl
CVE-2026-48229	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in routes_i.php that allows authenticated attackers to inject arbitrary JavaScri when the response is rendered.
CVE-2026-48228	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in patient_w.php that allows authenticated attackers to inject arbitrary JavaSc the response is rendered.
CVE-2026-48227	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in patient.php that allows authenticated attackers to inject arbitrary JavaScrip response is rendered.
CVE-2026-48226	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in os_watch.php that allows authenticated attackers to inject arbitrary JavaSc victim's browser when the response is rendered.
CVE-2026-48225	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in landb.php that allows authenticated attackers to inject arbitrary JavaScript the response is rendered.
CVE-2026-48223	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ics213rr.php that allows authenticated attackers to inject arbitrary JavaScri browser when the response is rendered.
CVE-2026-9078	Firefox for iOS displayed specially crafted right-to-left (RTL) and internationalized domain names (IDNs) incorrectly in link preview UI surfaces. A crafted RTL hostna
CVE-2026-48222	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ics213.php that allows authenticated attackers to inject arbitrary JavaScript browser when the response is rendered.
CVE-2026-48221	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ics205a.php that allows authenticated attackers to inject arbitrary JavaScrip browser when the response is rendered.
CVE-2026-48220	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ics205.php that allows authenticated attackers to inject arbitrary JavaScript browser when the response is rendered.
CVE-2026-48219	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in ics202.php that allows authenticated attackers to inject arbitrary JavaScript browser when the response is rendered.
CVE-2026-48213	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in add.php that allows authenticated attackers to inject arbitrary JavaScript by response is rendered.
CVE-2026-48218	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in icons/buttons/landb.php that allows authenticated attackers to inject arbitra executes in the victim's browser when the response is rendered.
CVE-2026-48216	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in db_loader.php that allows authenticated attackers to inject arbitrary JavaSc request containing a JavaScript payload that executes in the victim's browser when the response is rendered.

CVE-2026-8203	Concrete CMS 9.5.0 and below has Stored XSS on the height parameter. The controller does not validate or sanitize $height. Any user with editor privileges can inje of 7.3 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N. Thanks Alfin Joseph for reporting.
CVE-2026-48217	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in delete_module.php that allows authenticated attackers to inject arbitrary Ja JavaScript payload that executes in the victim's browser when the response is rendered.
CVE-2026-48215	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in circle.php that allows authenticated attackers to inject arbitrary JavaScript response is rendered.
CVE-2026-40864	JupyterHub is software that allows users to create a multi-user server for Jupyter notebooks. In versions 4.1.0 through 5.4.4, XSRF protection (updated in 4.1.0) inap trigger server spawn (but not access the server) and if the attacker is a JupyterHub user permitted to share access to their server, cause a user to accept a share a if they are using a reverse proxy.
CVE-2025-36148	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4.0 through 3.2.4.15 IBM Financial Transaction Manager SWIFT is vulnerable to cross-s
CVE-2026-22678	Webmin before 2.641 contains a stored cross-site scripting vulnerability in the email template description field of the System and Server Status module that allows
CVE-2026-39960	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and below contain flawed logic that causes improper escaping of a textarea custom takeover, full project data access. In order to exploit this issue, a textarea-type custom field must be configured for the project, the attack must be carried out by a around the issue by using the default Content-Security Policy, which blocks script execution.
CVE-2026-8139	Concrete CMS 9.5.0 and below is vulnerable to Stored XSS via external-link page cvName because updateCollectionAliasExternal bypasses being sanitized. The Cor
CVE-2026-8245	Concrete CMS 9.5.0 and below is vulnerable to Reflected XSS in Legacy Pagination via HTML attribute injection. Concrete\Core\Legacy\Pagination builds pagination Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.0 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks
CVE-2025-36145	IBM watsonx.data 2.2 through 2.3.1 IBM Lakehouse does not properly restrict inbound and outbound connections which could allow an attacker to transfer or modif
CVE-2026-27398	Missing Authorization vulnerability in WP Chill RSVP and Event Management allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affec
CVE-2026-44390	NLnet Labs Unbound up to and including version 1.25.0 has a vulnerability when handling replies with very large RRsets that Unbound needs to perform name com degraded performance and eventually denial of service in well orchestrated attacks. An adversary can exploit the vulnerability by querying Unbound for the specia compression limit was introduced in 1.21.1 for this but it didn't account for the case where records would not share any suffix above the root. That causes Unbound counter regardless of the compression tree lookup. This is a complement fix to CVE-2024-8508.
CVE-2026-42923	NLnet Labs Unbound up to and including version 1.25.0 has a vulnerability in the DNSSEC validator where the code path to consult the negative cache for DS recor with acceptably high iterations for child delegations and querying a vulnerable Unbound. Unbound will keep performing the allowed hash calculations on the NSEC3 Coordinated attacks could raise the vulnerability to denial of service. Unbound 1.25.1 contains a patch with a fix to bound the vulnerable code path with the existin
CVE-2026-9502	A vulnerability was identified in GNU LibreDWG up to 0.14. This affects the function decompress_R2004_section of the file src/decode.c of the component Dwgread this issue, it is recommended to deploy a patch.
CVE-2026-9500	A vulnerability was found in GNU LibreDWG up to 0.14. The affected element is the function read_2004_compressed_section of the file src/decode.c of the compone through an issue report but has not responded yet.
CVE-2025-15369	The Xpro Addons — 140+ Widgets for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the g
CVE-2026-39655	Missing Authorization vulnerability in TeconceTheme Mayosis Core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Mayos
CVE-2026-8486	Allocation of resources without limits or throttling vulnerability in Progress Software MOVEit Automation allows Flooding. This issue affects MOVEit Automation: befo
CVE-2026-4293	The affected Kieback & Peter DDC building controllers are vulnerable to cross-site scripting, enabling JavaScript to be executed by the victim's browser, which allov
CVE-2026-3592	BIND resolvers are vulnerable to an amplified resource consumption/exhaustion attack. If a victim resolver makes a query to a specially crafted zone, the resolver 9.20.9-S1 through 9.20.22-S1.
CVE-2026-6728	The Slider Revolution plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 7.0.9 via the 'get_stream_data()' functio
CVE-2026-24208	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a path traversal issue. A successful exploit of this vulnerability might lead to

CVE-2018-25370	Admidio 3.3.5 contains a cross-site request forgery vulnerability that allows low-privilege users to increase their permissions by exploiting improper origin checking
CVE-2026-32792	NLnet Labs Unbound 1.6.2 up to and including version 1.25.0 has a denial of service vulnerability when compiled with DNSCrypt support ('--enable-dnscrypt'). A ba entirely of '0x00' bytes and does not contain the expected '0x80' marker. Unbound would then start reading more bytes than necessary until it finds a non-'0x00' b memory layout. If the heap overflow does not happen, Unbound's later packet checks will deny the packet. Unbound 1.25.1 contains a patch with a fix to bound rea
CVE-2026-5950	An unbounded resend loop vulnerability exists in the BIND 9 resolver state machine during bad-server handling, enabling a remote unauthenticated attacker to cau 9.20.9-S1 through 9.20.22-S1.
CVE-2026-27357	Missing Authorization vulnerability in Cornel Raiu WP Search Analytics allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP
CVE-2026-9466	A vulnerability was determined in Tiandy Easy7 Integrated Management Platform 7.17.0. This issue affects some unknown processing of the file /rest/user/updateU early about this disclosure but did not respond in any way.
CVE-2026-42534	NLnet Labs Unbound up to and including version 1.25.0 has a vulnerability in the jostle logic that could defeat its purpose and degrade resolution performance. Ret who can control a domain name server that replies slowly and/or maliciously to Unbound's queries can exploit the vulnerability and degrade the resolution perform then happens because duplicate queries that need resolution would skew the aging result by using the timestamp of the latest duplicate query instead of the origin non-updatable start time for incoming queries that allow the jostle logic to work as intended.
CVE-2026-42015	A flaw was found in gnutls. An off-by-one error exists in the PKCS#12 bag element bounds check. This vulnerability allows an remote attacker to write past the inte
CVE-2026-24546	Missing Authorization vulnerability in Ruben Garcia GamiPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects GamiPress
CVE-2026-24592	Missing Authorization vulnerability in Lucian Apostol Auto Affiliate Links allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects A
CVE-2025-32747	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially
CVE-2026-9352	A weakness has been identified in NousResearch hermes-agent up to 2026.4.23. This issue affects the function _make_run_env of the file tools/environments/local. vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-8239	Concrete CMS 9.5.0 and below is vulnerable to IDOR. The '/ccm/frontend/conversations/get_rating' endpoint confirms existence and returns rating score for any me
CVE-2026-8237	Concrete CMS 9.5.0 and below is vulnerable to IDOR. The `/ccm/frontend/conversations/message_detail` endpoint returns the full content of any conversation mess Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with Vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thank
CVE-2026-48135	A Check Point HTTP-based service can incorrectly handle malformed HTTP requests. The issue is related to HTTP request parsing and validation.
CVE-2026-9540	A vulnerability was identified in vllm-project vllm 0.19.0. This issue affects some unknown processing of the component OpenAI-compatible Serving Path. Such mar
CVE-2026-9124	Insufficient validation of untrusted input in Input in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker who had compromised the renderer proce
CVE-2025-32749	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Exposure of Information Through Directory Listing vulnerability. An unauthenticated attacker with remot
CVE-2026-7879	In Concrete CMS 9.5.0 and below, the submit_password() method in concrete/controllers/single_page/download_file.php allows unauthorized file access since down permission to access the file. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:
CVE-2026-25426	Missing Authorization vulnerability in Magepeople inc. Taxi Booking Manager for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Le
CVE-2026-8205	Concrete CMS 9.5.0 and below is vulnerable to authorization bypass in the Calendar Block since action_get_events does not check canView on the calendar which r reporting.
CVE-2026-8204	Concrete CMS 9.5.0 and below is vulnerable to authorization Bypass in the Calendar Event Frontend Dialog which can allow cross-calendar data disclosure. A public Thanks Winston Crooker for reporting.
CVE-2026-9369	A security flaw has been discovered in NousResearch hermes-agent 2026.4.23. Affected is the function _discover_dashboard_plugins of the file hermes_cli/web_ser 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.

CVE-2026-6826	Concrete CMS 9.5.0 and below is vulnerable to unauthenticated file usage disclosure via missing permission check in the usage controller. Any unauthenticated vi permissions.The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.9 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/
CVE-2026-27393	Missing Authorization vulnerability in Tobias CF7 WOW Styler allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CF7 WOW S
CVE-2026-7453	A maliciously crafted WRL file, when parsed through Autodesk 3ds Max, can cause a Stack Exhaustion vulnerability, leading to a denial-of-service condition.
CVE-2026-48245	Open ISES Tickets before 3.44.2 embeds a hardcoded Google Maps API key in tables.php that is committed to the public source repository. The key can be extracte
CVE-2026-48244	Open ISES Tickets before 3.44.2 embeds a hardcoded Google Maps API key in settings.inc.php that is committed to the public source repository. The key can be ex
CVE-2026-7450	A maliciously crafted PAR file, when parsed through Autodesk 3ds Max, can force a NULL Pointer Dereference vulnerability. Successful exploitation may cause the a
CVE-2026-48243	Open ISES Tickets before 3.44.2 embeds a hardcoded WhitePages reverse-phone API key in wp1.php that is committed to the public source repository. Any actor w
CVE-2026-8238	Concrete CMS 9.5.0 and below is vulnerable to IDOR. The '/ccm/frontend/conversations/message_page' endpoint returns the full content of any conversation messa CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with Vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Tristan
CVE-2026-9541	A security flaw has been discovered in Squirrel up to 3.2. Impacted is the function ReadObject of the file squirrel/sqobject.cpp of the component Cnut File Handler. an issue report but has not responded yet.
CVE-2026-8240	Concrete CMS 9.5.0 and below is vulnerable to unauthenticated page metadata disclosure across every page with a configured summary template, revealing the e vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting.
CVE-2026-8684	The MotoPress Hotel Booking plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.0.1. This is due to the plugin not prop ID. The nonce for this action is output in the HTML source of every public page through wp_localize_script (MPHB._data.nonces), so any unauthenticated visitor can
CVE-2026-24590	Missing Authorization vulnerability in VideoWhisper.Com Paid Videochat Turnkey Site allows Exploiting Incorrectly Configured Access Control Security Levels. This is
CVE-2026-46745	Apache Airflow FAB Auth Manager contains an LDAP filter injection vulnerability (CWE-90) that allows unauthenticated attackers to exfiltrate directory data or bypa
CVE-2026-44618	Insecure XML parser configuration in Apache CXF's WS-Transfer module may allow attackers to perform XXE attacks. Users are recommended to upgrade to versio
CVE-2026-39642	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in SpabRice Nyla allows Code Injection. This issue affects Nyla: from n
CVE-2026-2812	ArcGIS Server contains an improper authentication vulnerability in an undocumented administrative endpoint. An unauthenticated attacker could exploit this issue
CVE-2025-36221	IBM Cloud Pak for Data System - Cyclops 11.3.0.2 through Interim Fix 002 IBM Cloud Pak for Data System uses default passwords default passwords from the manu
CVE-2026-9349	A vulnerability was determined in calcom cal.diy up to 4.9.4. Affected by this issue is the function getServerSideProps of the file apps/web/modules/bookings/views publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-8337	Concrete CMS 9.5.0 and below is vulnerable to IDOR in surveys. To be vulnerable, a site would have to be configured in such a way that both public and private sur score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Zer0daySec https://github.com/Zee99y for reporting
CVE-2026-39835	SSH servers which use CertChecker as a public key callback without setting IsUserAuthority or IsHostAuthority could be caused to panic by a client presenting a ce
CVE-2026-46598	For certain crafted inputs, a 'ed25519.PrivateKey' was created by casting malformed wire bytes, leading to a panic when used.
CVE-2026-5091	Catalyst::Plugin::Authentication versions through 0.10024 for Perl is susceptible to timing attacks. These versions use Perl's built-in eq comparison. Discrepencies i

CVE-2026-8672	Use of default password vulnerability in syslink software AG Avantra on Linux, Windows allows Try Common or Default Usernames and Passwords. This issue affect
CVE-2026-9304	A security flaw has been discovered in calcom cal.diy up to 4.9.4. The affected element is the function validateUrlForSSRF of the file apps/web/app/api/logo/route.ts 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.
CVE-2026-9245	Improper input validation in the external authentication provider flow in Devolutions Server allows an unauthenticated remote attacker to redirect victims to an att
CVE-2026-44723	Vowpal Wabbit is a machine learning system. The workflow .github/workflows/python_checks.yml embeds ${{ github.event.pull_request.title }} directly inside dou attacker to break out of the quotes and execute arbitrary commands on the runner. The pull_request trigger fires on PRs targeting any branch (branches: ['*']), wit
CVE-2026-9568	A weakness has been identified in ThingsBoard up to 4.3.1.1. Affected by this vulnerability is the function getGatewayDockerComposeFile of the file /api/v1/provisi problem early through a pull request but has not reacted yet.
CVE-2026-44073	Authentication modules in Netatalk 1.5.0 through 4.4.2 fail to check the return value of seteuid(), which may allow a remote authenticated attacker to retain elevat
CVE-2026-45443	Missing Authorization vulnerability in ADD-ONS.ORG PDF for Elementor Forms + Drag And Drop Template Builder allows Exploiting Incorrectly Configured Access C
CVE-2026-42797	Exposure of Sensitive Information Through Data Queries vulnerability in Apache Syncope. An administrator with adequate entitlements for Derived Schemas can cr 4.1.0. Users are recommended to upgrade to version 4.0.6 / 4.1.1, which fix this issue by further restricting the JEXL expression definition.
CVE-2026-42396	Insufficient Validation of Member Zone Data May Cause Catalog Zone Transfer to Fail
CVE-2026-5308	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to enforce request body size limits on plugin HTTP endpoints
CVE-2026-41917	OpenKM 6.3.12 contains a local file inclusion vulnerability in the administrative scripting interface at /admin/Scripting that allows authenticated administrators to re credentials, and JVM keystores accessible to the OpenKM process.
CVE-2026-7472	The Read More & Accordion plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'orderby' parameter in all versions up to, and including, 3.5 value is only processed through esc_attr() (an HTML-escaping function) before being passed to these database functions, where esc_sql() is applied but the value is context), an attacker can inject arbitrary SQL expressions such as (SELECT SLEEP(5)) or conditional subqueries to perform time-based blind data extraction. This m administrator credential hashes.
CVE-2026-4811	The WPB Floating Menu & Categories for WordPress – Sticky Side Menu with Icons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Icon CSS in pages that will execute whenever a user accesses an injected page.
CVE-2026-27346	Missing Authorization vulnerability in Kings Plugins B2BKing allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects B2BKing: fror
CVE-2026-8197	Concrete CMS 9.5.0 and below is vulnerable to Stored XSS via OAuth integration name. The OAuth authorize template renders the integration name (admin-control could potentially snoop on login submissions.The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.3 with vector CVSS:4.0/AV:N/AC:L/AT:
CVE-2026-44443	Lumiverse is a full-featured AI chat application. Prior to 0.9.7, consumeNonce() only checks that the module-level variable is set and unexpired. It does not validate set but never consumed. Any POST /api/auth/sign-up/email request that arrives during the remaining window registers successfully regardless of who sent it. An at
CVE-2026-41999	Incorrect Behaviour of Views with TCP PROXY Requests
CVE-2026-8353	Concrete CMS version 9.0 to 9.5.0 is vulnerable to Stored XSS via page name in the Atomik theme. A rogue editor can inject arbitrary JavaScript that executes in th team gave this vulnerability a CVSS v.4.0 score of 2.1 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Yonatan Drori (Tenzai
CVE-2026-43617	Rsync version 3.4.2 and prior contain an authorization bypass vulnerability in the rsync daemon's hostname-based access control list enforcement when configure defaults to UNKNOWN.
CVE-2026-44831	Snipe-IT is an IT asset/license management system. Prior to 8.4.1, users with component view access could be impacted by an unescaped notes column, resulting i
CVE-2026-24199	NVIDIA Display Driver for Linux contains a vulnerability in a kernel module, where a user could cause a race condition by reordering compiler or processor memory
CVE-2026-44899	Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.2.1, the Image directive plugin validates the :width: and :height: options with a regex c prefix-only regex, any CSS after the leading digits reaches the style= attribute verbatim and without escaping. This vulnerability is fixed in 3.2.1.

CVE-2026-20199	A vulnerability in the SSL certificate handling of Cisco ThousandEyes Virtual Appliance could allow an authenticated, remote attacker to execute commands on the successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit this vulnerability, the attacker
CVE-2026-9446	A vulnerability has been found in SourceCodester Simple POS and Inventory System 1.0. The affected element is an unknown function of the file /admin/edit_custo
CVE-2026-9464	A vulnerability has been found in YunaiV yudao-cloud 2026.03. This affects the function IotDataSinkHttpConfig of the file /admin-api/iot/data-sink/create of the com disclosure but did not respond in any way.
CVE-2026-9423	A security flaw has been discovered in Edimax BR-6675nD 1.12. Impacted is the function mp of the file /goform/mp of the component POST Request Handler. Perfo disclosure but did not respond in any way.
CVE-2026-9444	A vulnerability was detected in SourceCodester Simple POS and Inventory System 1.0. This issue affects the function delete of the file /admin/deleteproduct.php of
CVE-2026-2813	ArcGIS Server contains an input validation weakness in the login redirection workflow. An Authenticated attacker could exploit this issue by sending a specially craf the client side navigation logic during authentication and remains confined to the same security boundary. No server side compromise or cross component impact
CVE-2026-35013	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in street_view.php that allows authenticated attackers to inject arbitrary JavaS victim's browser when the URL is visited.
CVE-2026-35011	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in opena.php that allows authenticated attackers to inject arbitrary JavaScript URL is visited.
CVE-2026-35010	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in patient_JF.php that allows authenticated attackers to inject arbitrary JavaSc victim's browser when the URL is visited.
CVE-2026-35012	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in add_facnote.php that allows authenticated attackers to inject arbitrary Java the victim's browser when the URL is visited.
CVE-2026-35009	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in add_note.php that allows authenticated attackers to inject arbitrary JavaScr victim's browser when the URL is visited.
CVE-2026-35014	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in routes_nm.php that allows authenticated attackers to inject arbitrary JavaS victim's browser when the URL is visited.
CVE-2026-35015	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in do_unit_mail.php that allows authenticated attackers to inject arbitrary Java the victim's browser when the URL is visited.
CVE-2026-35008	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in single.php that allows authenticated attackers to inject arbitrary JavaScript URL is visited.
CVE-2026-35007	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in single_unit.php that allows authenticated attackers to inject arbitrary JavaS URL is visited.
CVE-2026-41073	RT is an open source, enterprise-grade issue and ticket tracking system. Versions prior to 5.0.10 and 6.0.0 through 6.0.2 contain a spreadsheet (CSV/formula) injec issue has been fixed in versions 5.0.10 and 6.0.3. If developers are unable to upgrade immediately, they can temporarily work around this issue by avoiding openi
CVE-2026-35016	Open ISES Tickets before 3.44.2 contains a reflected cross-site scripting vulnerability in search.php that allows authenticated attackers to inject arbitrary JavaScrip in the victim's browser when submitted.
CVE-2026-3314	Missing password field masking vulnerability in Hitachi Ops Center Analyzer (Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe modules), viewpoint: from 10.8.1-00 before 11.0.8-00; Hitachi Infrastructure Analytics Advisor: from 3.2.0-00 before 11.0.8-00.
CVE-2026-44059	A race condition in the privilege toggle mechanism in Netatalk 2.2.5 through 4.4.2 allows a local attacker to obtain limited information, modify limited data, or caus
CVE-2026-6399	The General Options plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 1.1.0. This is due to the use of sanitize_text_fi double-quoted HTML attribute (value="..."), an attacker-supplied double-quote character breaks out of the attribute context. Even with WordPress's wp_magic_quo This makes it possible for authenticated attackers with Administrator-level access and above to inject arbitrary web scripts in the admin settings page that will exe
CVE-2026-6404	The Anomify AI – Anomaly Detection and Alerting plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'anomify_api_key' parameter in versions tags without encoding double-quote characters, and the value is then echoed directly into an HTML attribute context (value="...") without esc_attr(). This makes it
CVE-2026-48849	In Roundcube Webmail 1.6.x before 1.6.16 and 1.7.x before 1.7.1, an unsanitized subject field in the draft restored value could lead to stored XSS/HTML/CSS injecti

CVE-2026-41164	nuts-node is the reference implementation of the Nuts specification. Prior to 6.2.3 and 5.4.31, the v1 access token introspection endpoint (/auth/v1/introspect_acce active: true introspection response. This vulnerability is fixed in 6.2.3 and 5.4.31.
CVE-2026-25602	Insufficient Verification of Data Authenticity vulnerability in Mesalvo Meona Client Launcher Component, Mesalvo Meona Server Component makes it possible to se
CVE-2025-33221	NVIDIA Display Driver for Windows and Linux contains a vulnerability in the kernel driver, where a user could cause an incorrect permission assignment for a critica
CVE-2026-47728	Bugsink is a self-hosted error tracking tool. Prior to 2.2.0, Bugsink resolved sourcemaps and debug files by debug ID without scoping that lookup to the project that debug ID was referenced. This vulnerability is fixed in 2.2.0.
CVE-2026-46431	Algernon is a small self-contained pure-Go web server. Prior to 1.17.7, the SSE event server's Access-Control-Allow-Origin response header was hardcoded to the w read the live filename stream from JavaScript. This vulnerability is fixed in 1.17.7.
CVE-2026-24638	Missing Authorization vulnerability in Webful Creations RepairBuddy allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Repa
CVE-2026-46430	Algernon is a small self-contained pure-Go web server. Prior to 1.17.7, the SSE event server bound to 0.0.0.0:5553 on Linux/macOS by default because the platform
CVE-2026-48900	An improper access check allowed low privileged users to edit the task types of existing scheduler tasks.
CVE-2026-43936	e107 is a content management system (CMS). Prior to 2.3.4, you can access the local environment by specifying the URL of the local environment from "Image/File
CVE-2026-44502	Bugsink is a self-hosted error tracking tool. Prior to 2.1.3, Bugsink's webhook URL validation could be (partially) bypassed because of a mismatch in URL parsing. Tl ends and which hostname is the real target. A URL may therefore appear to target an allowlisted public hostname during validation, while the HTTP client actually
CVE-2026-9582	A security flaw has been discovered in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This affects an unknown function. Performi
CVE-2026-9583	A weakness has been identified in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This impacts an unknown function of the file /in for attacks.
CVE-2025-36220	IBM Cloud Pak for Data System - Cyclops 11.3.0.2 through Interim Fix 002 IBM Cloud Pak for Data System is vulnerable to SQL injection. A remote attacker could se
CVE-2026-44749	The SAP Gateway allows attackers to inject content into error messages, potentially leading to disclosure of request artefacts (e.g., regex patterns) and revealing u
CVE-2026-9518	A vulnerability was identified in hemant6488 CodeIgniter-StudentManagementSystem. The impacted element is the function addStudent of the file view_students.p rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed c
CVE-2026-9519	A security flaw has been discovered in stonith404 pingvin-share up to 1.13.0. This affects the function getServerSideProps of the file frontend/src/pages/auth/signIr The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-9520	A weakness has been identified in blitz-js blitz up to 3.0.2 on GitHub. This impacts an unknown function of the file packages/generator/templates/app/src/app/auth/ attacks. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-25444	Missing Authorization vulnerability in Magepeople inc. WpBookingly allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WpBo
CVE-2026-24520	Missing Authorization vulnerability in bPlugins Tiktok Feed allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Tiktok Feed: fr
CVE-2026-9527	A vulnerability was determined in itsourcecode Electronic Judging System 1.0. This issue affects some unknown processing of the file /admin/judges.php. This mani
CVE-2026-9566	A vulnerability was identified in teableio teable up to 1.9.x. This impacts an unknown function of the file apps/nextjs-app/src/features/auth/pages/LoginPage.tsx of t 21T08-57-20Z.1513 will fix this issue. The affected component should be upgraded. The vendor confirms: "The default branch of teableio/teable is develop, and the
CVE-2026-38587	An Insecure Direct Object Reference (IDOR) vulnerability was discovered in ONLYOFFICE DocSpace before 3.2.1. The flaw exists in multiple REST API endpoints. Thi

CVE-2026-34754	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and prior allow an authenticated user to upload attachments to private Issues they
CVE-2026-9604	A vulnerability was detected in JeecgBoot up to 3.9.1. This vulnerability affects unknown code of the component AiragModelController. The manipulation of the argu upgraded.
CVE-2026-9224	Missing authorization in the user profile update feature in Devolutions Server allows an authenticated Active Directory user to modify their own profile attributes vi
CVE-2026-27349	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in WPFunnels Team Mail Mint allows Retrieve Embedded Sensitive Data.
CVE-2026-9115	Insufficient policy enforcement in Service Worker in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to bypass same origin policy via a crafte
CVE-2026-9116	Insufficient policy enforcement in ServiceWorker in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to leak cross-origin data via a crafted HTI
CVE-2026-40094	nimiq-blockchain provides persistent block storage for Nimiq's Rust implementation. In versions 1.3.0 and prior, network-libp2p discovery accepts signed PeerConta PeerContactBook::known_peers builds an address book by taking addresses.first().expect("every peer should have at least one address"). If the attacker has insert
CVE-2026-1881	The Broadstreet plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.52.2 via the get_sponsored_meta AJAX
CVE-2018-25343	Smartshop 1 contains a cross-site request forgery vulnerability that allows attackers to modify user profiles by tricking authenticated users into submitting maliciou
CVE-2018-25363	Twitter-Clone 1 contains a cross-site request forgery vulnerability that allows remote attackers to force victims to delete posts by crafting malicious HTML forms. At
CVE-2018-25354	Joomla Component jomres 9.11.2 contains a cross-site request forgery vulnerability that allows attackers to modify user account information by tricking authentica
CVE-2026-7615	The Widget Context plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.3. This is due to missing or incorrect n admin/widgets.php via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2026-9448	A vulnerability was determined in code-projects Employee Management System 1.0. This affects an unknown function of the file /applyleave.php. Executing a mani
CVE-2026-7249	The Location Weather plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on the `splw_update_block_options( cache transients. The nonce required for these actions is exposed to all authenticated users via `wp_localize_script()` on the `init` hook.
CVE-2026-9358	A vulnerability was determined in postcss up to 7.1.1. Affected is the function toString of the file src/selectors/container.js of the component AST Serialization. Exec user-generated CSS is low risk for us (since most users compile own CSS with PostCSS)."
CVE-2026-4070	The Alfie – Feed Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.1. This is due to missing nonce valid alfie_reactions, and alfie_searchproduct tables) via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2026-4055	Mattermost versions 11.5.x <= 11.5.1 fail to validate team-level run_create permission against the target team when creating a playbook run which allows an auth
CVE-2026-2518	The FastX theme for WordPress is vulnerable to unauthorized limited plugin installation and activation due to missing capability checks on the 'ultp_install_callback
CVE-2026-9410	A vulnerability has been found in Sushmi-pal Invoice-System up to a0a3faa16dee2621b231ae227333f5761607283b. This vulnerability affects unknown code of the takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was
CVE-2026-9246	Improper access control in the entry documentation and attachment features in Devolutions Server allows an authenticated user with vault read access to retrieve
CVE-2026-9419	A vulnerability has been found in code-projects Employee Management System 1.0. Affected by this issue is some unknown functionality of the file /empproject.php
CVE-2026-9418	A flaw has been found in code-projects Employee Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /changepassemp.ph
CVE-	

2026-9417	A vulnerability was detected in code-projects Employee Management System 1.0. Affected is an unknown function of the file /myprofileup.php. Performing a manip
CVE-2026-8327	Concrete CMS below 9.5.0 and below is vulnerable to password change without reauthorization and session-hardening bypass. The user-profile edit controller pass validator which is meant to detect hijacking. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 5.3 with vector CVSS:4.0/AV:N/AC:L/AT:
CVE-2026-8236	Concrete CMS 9.5.0 and below is vulnerable to IDOR combined with a missing authentication gate. The endpoint /ccm/system/dialogs/file/usage/{fID} accepts an ir vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting.
CVE-2026-7886	Concrete CMS 9.5.0 and below is vulnerable to IDOR in AddMessage/UpdateMessage via attachments[] parameter which can lead to file permission bypass. The `A post in any conversation can reference any file in the CMS file manager by its sequential ID, effectively bypassing the file permission system. The Concrete CMS se private storage location https://documentation.concretecms.org/user-guide/editors-reference/dashboard/system-and-maintenance/files/file-storage-locations outsid
CVE-2026-7882	Concrete CMS 9.5.0 and below is vulnerable to unauthorized file deletion due to an Inverted CSRF token check in the DeleteFile controller. The code throws an erro permission to edit conversation messages. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.3 with a vector of CVSS:4.0/AV:N/AC:L/A
CVE-2026-4843	The GSheet For Woo Importer plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the process_ajax_restore_action(
CVE-2026-9416	A security vulnerability has been detected in code-projects Employee Management System 1.0. This impacts an unknown function of the file /myprofile.php. Such r
CVE-2026-7881	Concrete CMS 9.5.0 and below is subject to Insecure Direct Object Reference (IDOR) in the Express Entry Detail block via the exEntryID parameter. This IDOR leads Madani for reporting.
CVE-2026-9415	A weakness has been identified in code-projects Employee Management System 1.0. This affects an unknown function of the file /eloginwel.php. This manipulation
CVE-2026-9409	A flaw has been found in Sushmi-pal Invoice-System up to a0a3faa16dee2621b231ae227333f5761607283b. This affects an unknown part of the file /user of the co release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disc
CVE-2026-9113	Out of bounds read in GPU in Google Chrome on Mac prior to 148.0.7778.179 allowed a remote attacker to perform an out of bounds memory read via a crafted HT
CVE-2026-9303	A vulnerability was identified in calcom cal.diy up to 4.9.4. Impacted is an unknown function. The manipulation leads to cross-site request forgery. It is possible to i
CVE-2026-9101	Prototype pollution in csv parsing logic during import can lead to untrusted file paths (but not arguments) entering shell.openExternal after specific user behavior l
CVE-2026-8488	Allocation of resources without limits or throttling vulnerability in Progress Software MOVEit Automation allows Excessive Allocation. This issue affects MOVEit Auto
CVE-2026-24554	Cross-Site Request Forgery (CSRF) vulnerability in Convers Lab WPSubscription allows Cross Site Request Forgery. This issue affects WPSubscription: from n/a throu
CVE-2026-24527	Missing Authorization vulnerability in Patterns in the cloud Autoship Cloud for WooCommerce Subscription Products allows Exploiting Incorrectly Configured Access
CVE-2026-6400	The Child Height Predictor by Ostheimer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 1.3. This is due to miss possible for unauthenticated attackers to trick a site administrator into clicking a link or visiting a malicious page that submits a forged POST request, causing unau
CVE-2026-6401	The Bottom Bar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 0.1.7. This is due to missing nonce verification c check_admin_referer() or any equivalent nonce validation before processing POST data and calling update_option(). This makes it possible for unauthenticated atta
CVE-2026-9223	Missing authorization in the vault import feature in Devolutions Server 2026.1.16.0 and earlier allows a low-privileged authenticated user to create new vaults via
CVE-2026-6452	The Bigfishgames Syndicate plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2. This is due to missing or inco performing an action such as clicking on a link.
CVE-2026-5171	Improper access control in the entry activity log feature in Devolutions Server allows an authenticated user with access to an entry but without the required permis
CVE-2026-8418	The Games Catalog plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.0. This is due to missing or incorrect nonc game catalog entries (including the associated WordPress post created for the game) via a forged request, granted they can trick a site administrator into performi
CVE-	

2026-8419	The Amazon Scraper 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 no on a link.
CVE-2026-8423	The JaviBola Custom Theme Test plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.5. This is due to missing into performing an action such as clicking on a link.
CVE-2026-8424	The Remove Yellow BGBOX plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incor into performing an action such as clicking on a link.
CVE-2026-8610	The TypeSquare Webfonts for ConoHa plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.0.4. This is due to the plugin option (fontThemeUseType), show_post_form, and typesquare_fonttheme, by submitting a POST request to any wp-admin page. For fontThemeUseType values 1 a
CVE-2026-5075	The All in One SEO plugin for WordPress is vulnerable to Sensitive Information Exposure via 'internalOptions' localized script data in versions up to, and including, 4 above, to view configured API/OAuth tokens and license-related values from page source.
CVE-2026-6566	The Photo Gallery, Sliders, Proofing and Themes – NextGEN Gallery plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to and inc gallery ownership or 'NextGEN Manage others gallery' permissions. This makes it possible for authenticated attackers, with Subscriber-level privileges and 'NextGE
CVE-2026-6405	The Anomify AI – Anomaly Detection and Alerting plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) leading to Stored Cross-Site Scripting (XS handler performs no check_admin_referer() check, meaning any cross-origin POST can modify plugin settings. The API key field is sanitized only with sanitize_text_ and storage. This makes it possible for unauthenticated attackers to inject arbitrary web scripts by tricking a logged-in administrator into visiting a malicious page
CVE-2026-24597	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart allows Cross Site Request Forgery. This issue affects Organization chart: from n/a t
CVE-2026-24545	Missing Authorization vulnerability in Nikki Blight QR Redirector allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects QR Redire
CVE-2026-9486	A security flaw has been discovered in SourceCodester Student Grades Management System 1.0. This affects an unknown part. The manipulation results in cross-si
CVE-2026-8347	Concrete CMS 9.5.0 and below is vulnerable to IDOR + wrong-authorization-level in the Express association Reorder dialog. This can cause Cross-entity state tamp vector CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting.
CVE-2026-8340	Concrete CMS 9.5.0 and below is vulnerable to CSRF via Backend\File::approveVersion. Victim with edit_file_contents permission is CSRF'd into publishing an attack vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting.
CVE-2026-24582	Missing Authorization vulnerability in WPPOOL FlexTable allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects FlexTable: from
CVE-2026-4646	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to validate user-supplied input in API request handlers which
CVE-2026-9467	A vulnerability was identified in debugmcp mcp-debugger up to 0.20.0. Impacted is the function handleGetSourceContext of the file src/server.ts. The manipulation
CVE-2026-3636	Mattermost versions 11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14 fail to sanitize team member data when returned via API to users
CVE-2026-27424	Missing Authorization vulnerability in WP Chill Image Photo Gallery Final Tiles Grid allows Exploiting Incorrectly Configured Access Control Security Levels. This issu
CVE-2026-8692	The Vedrixa Forms – User Registration Form, Signup Form & Drag & Drop Form Builder plugin for WordPress is vulnerable to authorization bypass in all versions up any form — adding, removing, or altering fields — by writing attacker-controlled data to the plugin's FORMS database table. The 'ajax-nonce' nonce used by this ha
CVE-2026-7636	The Slider by Soliloquy – Responsive Image Slider for WordPress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and inclu by administrators or editors.
CVE-2026-9413	A vulnerability was identified in SourceCodester Indian Invoicing System 1.0. The affected element is an unknown function of the file /Invoicing/category.php. The r
CVE-2025-32745	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Improper Certificate Validation vulnerability. An unauthenticated attacker with adjacent network access
CVE-2026-44065	An off-by-two error in lp_write() in papd in Netatalk 2.0.0 through 4.4.2 allows an adjacent network attacker to modify limited data or cause a minor service disrupt
CVE-	

2026-9110	Inappropriate implementation in UI in Google Chrome on Windows prior to 148.0.7778.179 allowed a remote attacker who had compromised the renderer process
CVE-2026-44063	An LDAP injection vulnerability in Netatalk 2.1.0 through 4.4.2 allows a remote authenticated attacker to manipulate LDAP queries and obtain limited information o
CVE-2026-44067	A heap over-read in extended attribute (EA) header parsing in Netatalk 2.1.0 through 4.4.2 allows a remote authenticated attacker to obtain limited information or
CVE-2026-48136	When Compliance is enabled on Check Point Multi-Domain Management, an authenticated administrator with read-write access to one Management Domain (CMA)
CVE-2025-31973	HCL BigFix Service Management (SM) is susceptible to a Configuration – 'Insecure Use of Base Image Version'. Using outdated or insecure base images may introdu
CVE-2025-32746	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Insecure Storage of Sensitive Information vulnerability. An unauthenticated attacker with local access co
CVE-2026-45498	Microsoft Defender Denial of Service Vulnerability
CVE-2023-7346	Ledger Bitcoin app versions 2.1.0 and 2.1.1 contain an address derivation vulnerability that allows attackers to cause incorrect Bitcoin addresses to be displayed by sent to unintended addresses.
CVE-2026-44069	An integer underflow in the volxlate function in Netatalk 3.0.0 through 4.4.2 allows a local privileged user to obtain limited information, modify limited data, or caus
CVE-2026-44410	This vulnerability stems from a business logic flaw.Attackers can exploit legitimate application functions in unintended and abnormal ways, deviating from the desi
CVE-2026-9373	A vulnerability has been found in JeecgBoot 3.9.1. This issue affects some unknown processing of the file /openapi/call/ of the component OpenAPI Endpoint. Such r did not respond in any way.
CVE-2026-44075	A missing break statement in DSI OpenSession processing in Netatalk 1.5.0 through 4.4.2 causes a DSIOPT_ATTNQUANT switch case to fall through into DSIOPT_SE
CVE-2026-48852	PuTTY 0.71 before 0.84 has an assertion failure in ECDSA signature verification.
CVE-2026-48850	PuTTY 0.72 before 0.84 has a double free in RSA KEX.
CVE-2026-7837	A time-of-check time-of-use (TOCTOU) condition in the ad_flush function in Netatalk 3.0.0 through 4.4.2 involves root-privileged file operations, which may allow a r
CVE-2026-48847	Roundcube Webmail 1.6.x before 1.6.16, and 1.7.x before 1.7.1 allows pre-authentication arbitrary file deletion via redis/memcache session poisoning bypass.
CVE-2025-31985	HCL BigFix Service Management (SM) is affected by a security misconfiguration due to a missing or insecure “X-Content-Type-Options” header. This could allow bro
CVE-2026-9370	A weakness has been identified in ulisesbocchio jasypt-spring-boot up to 3.0.5/4.0.4. Affected by this vulnerability is the function getSecretKeySaltGenerator of the attack can be launched remotely. The attack requires a high level of complexity. The exploitation appears to be difficult. The exploit has been made available to th
CVE-2026-9396	A security flaw has been discovered in Besen BS20 EV Charging Station up to 20260426. Affected by this vulnerability is an unknown functionality of the componer original disclosure mentions, that "[t]hese vulnerabilities have been reported to Besen and we have received their acknowlegement that they are reviewing this as
CVE-2026-9306	A security vulnerability has been detected in QuantumNous new-api up to 0.12.1. This affects the function RelayMidjourneyImage/GetByOnlyMJId of the file router/r difficult. 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.
CVE-2026-44074	Netatalk 2.1.0 through 4.4.2 combines multiple errno values using bitwise OR, resulting in incorrect error codes when multiple error conditions occur simultaneousl
CVE-2026-44071	Netatalk 3.1.2 through 4.4.2 is compiled without FORTIFY_SOURCE, which disables built-in buffer overflow detection at runtime, potentially allowing a remote attac
CVE-	

2025-46371	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) a Use of a Broken or Risky Cryptographic Algorithm vulnerability in the ssh. A low privileged attacker with l
CVE-2026-9395	A vulnerability was identified in Besen BS20 EV Charging Station up to 20260426. Affected is an unknown function of the component BLE/UDP. The manipulation le that they are reviewing this as of April 2026."
CVE-2026-9471	A vulnerability was detected in yashpokharna2555 StudentManagementSystem cb2f558ddf8d19396de0f92abf2d224d46a0a203. This impacts an unknown functior 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 r
CVE-2026-48832	action/cookie.php in ecrire in SPIP before 4.4.15 is prone to an open redirect vulnerability.
CVE-2026-9485	A vulnerability was identified in SourceCodester Student Grades Management System 1.0. Affected by this issue is some unknown functionality of the file students.
CVE-2026-42448	Magic Wormhole makes it possible to get arbitrary-sized files and directories from one computer to another. Prior to 0.24.0, there is a path traversal when a receiv
CVE-2026-9357	A vulnerability was found in vBulletin 6.x. This impacts an unknown function of the component Login. Performing a manipulation results in cross site scripting. It is disclosure but did not respond in any way.
CVE-2026-9414	A security flaw has been discovered in SourceCodester Indian Invoicing System up to 0.x/1.0. The impacted element is an unknown function of the file /Invoicing/ac public and may be used for attacks.
CVE-2026-9572	A security vulnerability has been detected in GPAC up to 2.4.0. Affected by this issue is the function Media_GetSample of the file src/isomedia/media.c of the comp e79c5cbe8b3fed27f4854ec229457d30c96206f1. It is best practice to apply a patch to resolve this issue.
CVE-2026-9567	A security flaw has been discovered in GPAC up to 2.4.0. Affected is the function MergeFragment of the file src/isomedia/isom_intern.c of the component MP4Box. T 525bf1af642c30af04e4df5345e6d798c0a4d8a1. It is advisable to implement a patch to correct this issue.
CVE-2026-9504	A weakness has been identified in GNU LibreDWG up to 0.14. Affected is the function bit_convert_TU of the file programs/dwggrep.c of the component Dwggrep Uti Applying a patch is the recommended action to fix this issue.
CVE-2026-9530	A weakness has been identified in GNU LibreDWG up to 0.14. The impacted element is the function read_2004_compressed_section of the file src/decode.c of the c 8f03865f37f5d4ffd616fef802acc980be54d300. It is advisable to implement a patch to correct this issue.
CVE-2026-9503	A security flaw has been discovered in GNU LibreDWG up to 0.14. This impacts the function dwg_next_entity of the file src/decode.c of the component DWG File Ha 8f03865f37f5d4ffd616fef802acc980be54d300. Upgrading the affected component is advised.
CVE-2026-9501	A vulnerability was determined in GNU LibreDWG up to 0.14. The impacted element is the function decompress_R2004_section of the file src/decode.c of the comp e501cb9926c1e9a07a0d1cc997f3e69e9be801c9. A patch should be applied to remediate this issue.
CVE-2026-9529	A security flaw has been discovered in GNU LibreDWG up to 0.14. The affected element is the function match_BLOCK_HEADER of the file dwggrep.c of the compone
CVE-2026-9249	Unverified password change in Devolutions Server allows an attacker to change a user's password without providing the previous one via a crafted password chang
CVE-2026-44070	An unbounded memory reallocation in the charset conversion code in Netatalk 2.0.0 through 4.4.2 allows a remote authenticated attacker to cause a minor denial
CVE-2026-7835	A format string argument mismatch in Netatalk 3.0.3 through 4.4.2 allows a remote authenticated attacker to cause a minor denial of service via crafted input that
CVE-2026-39967	TypeBot is a chatbot builder tool. In versions 3.15.2 and prior, the bot engine's the findResult query does not filter results by typebotId, allowing an authenticated u infeasible), the requirement that rememberUser be enabled, and the need for matching variable names in the current typebot. If successfully exploited, an attacke
CVE-2026-44057	A dead bounds check in the Spotlight RPC unmarshaller in Netatalk 3.0.0 through 4.4.2 results in an unreachable code path that provides no effective bounds prote
CVE-2026-9398	A security vulnerability has been detected in Besen BS20 EV Charging Station up to 20260426. This affects an unknown part of the component BLE/WiFi. Such man mentions, that "[t]hese vulnerabilities have been reported to Besen and we have received their acknowlegement that they are reviewing this as of April 2026."
CVE-2026-9394	A vulnerability was determined in Besen BS20 EV Charging Station up to 20260426. This impacts an unknown function of the component Bluetooth Low Energy Ha mentions, that "[t]hese vulnerabilities have been reported to Besen and we have received their acknowlegement that they are reviewing this as of April 2026."
CVE-2026-	Bugsink is a self-hosted error tracking tool. Prior to 2.2.0, In affected versions, the issue list view authorizes access through the project in the URL, but applies the r

47716	
CVE-2026-47715	Bugsink is a self-hosted error tracking tool. Prior to 2.2.0, Bugsink issue event pages accept a direct event identifier from the URL and, in affected versions, look up access. The affected views include the stacktrace, details, and breadcrumbs pages for an issue event. This vulnerability is fixed in 2.2.0.
CVE-2026-7836	An incorrect calculation in the hextoint macro in Netatalk 2.0.0 through 4.4.2 due to improper uppercase character handling allows a remote authenticated attacke
CVE-2026-48851	PuTTY 0.77 before 0.84 uses a copy of the PuTTY icon as a trust indication for TELNET data but the trust status is not cleared between proxy authentication and the
CVE-2026-45232	Rsync versions before 3.4.3 contain an off-by-one out-of-bounds stack write vulnerability in the establish_proxy_connection() function in socket.c that allows netwo bytes without a newline terminator, causing a null byte to be written to an out-of-bounds stack address when the RSYNC_PROXY environment variable is set.
CVE-2026-44072	Netatalk 2.2.1 through 4.4.2 calls system() after a failed chdir() without properly handling the error condition, which allows a local privileged user to execute uninte
CVE-2026-8477	Improper enforcement of the sealed-entry workflow in the entry sensitive-data retrieval feature in Devolutions Server allows an authenticated user with access to a
CVE-2026-9248	Authorization bypass in the entry duplication feature in Devolutions Server allows an authenticated user with write access to any vault to copy documentation and
CVE-2026-9564	A vulnerability was found in SourceCodester/oretnom23 Hospitals Patient Records Management System 1.0. The impacted element is an unknown function of the fi
CVE-2026-9247	Insufficient logging in the entry export feature in Devolutions Server allows an authenticated user with export permissions to export a sealed entry without triggeri
CVE-2026-9377	A vulnerability was identified in SourceCodester SUP Online Shopping 1.0. The impacted element is an unknown function of the file /admin/productedit.php. The ma
CVE-2026-47072	Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability in benoitc hackney allows HTTP Request/Response Splitting. The WebSocket upgrade coc request by binary concatenation in do_handshake/1. No CRLF or NUL stripping is performed at any of these four injection sites. An attacker who controls any of the credential spoofing toward the upstream server, log and cache poisoning, or request smuggling via intermediary proxies. This issue affects hackney: from 2.0.0 be
CVE-2025-68708	SailingLab AppLock (aka com.alpha.applock) 4.3.8 for Android allows a local attacker with physical access to bypass the PIN lock. The lock is implemented as an ov an attacker can evade lockscreen verification and access protected apps (e.g., Chrome). This results in information disclosure and privilege escalation.
CVE-2025-68711	AppLockZ App Lock and Fingerprint Lock (applock.passwordfingerprint.applockz) 4.2.11 for Android allows a local attacker with physical access to bypass the PIN lo via advertisement or browser intents, an attacker can evade lockscreen verification and access protected apps (e.g., Chrome). This results in information disclosure
CVE-2026-36239	PbootCMS v.3.2.11 contains a code injection vulnerability in its site configuration functionality
CVE-2026-42335	MaxKB is an open-source AI assistant for enterprise. Prior to 2.8.1, MaxKB v2.8.0 and prior are vulnerable to a server-side request forgery (SSRF) bypass in the OSS This vulnerability is fixed in 2.8.1.
CVE-2026-42336	MaxKB is an open-source AI assistant for enterprise. MaxKB 2.8.0 and prior are vulnerable to a server-side request forgery (SSRF) bypass in the OSS file service UR
CVE-2026-42496	Archive::Tar versions before 3.08 for Perl extract symlinks with attacker controlled targets outside the extraction directory. _make_special_file() passes the tar head reads or writes the attacker chosen path.
CVE-2026-42337	MaxKB is an open-source AI assistant for enterprise. MaxKB 2.8.0 and prior are vulnerable to a broken access control vulnerability in the OSS file service URL fetch
CVE-2026-47073	Allocation of Resources Without Limits or Throttling vulnerability in benoitc hackney allows Flooding. The WebSocket client in src/hackney_ws.erl imposes no upper without ever sending \r\n\r\n causes the buffer to grow until memory is exhausted. Second, parse_payload/9 and parse_active_payload/8 do not validate the declar frag_buffer field in #ws_data{} accumulates continuation frames indefinitely; a server that sends an endless stream of non-final (nofin) fragmented frames without This issue affects hackney: from 2.0.0 before 4.0.1.
CVE-2026-47070	Sensitive Data Exposure vulnerability in benoitc hackney allows Retrieve Embedded Sensitive Data. The HTTP/3 redirect handler in src/hackney_h3.erl passes the c with a 3xx redirect to a different host will cause the client to forward those credentials verbatim to the new origin. The main hackney.erl module has maybe_strip_a
CVE-2026-9102	A path traversal vulnerability exists in the Altium Enterprise Server ComparisonService due to missing filename sanitization in the Gerber file upload APIs. A regular content-controlled files can be written to web-accessible directories, this can be escalated to remote code execution in the context of the service account. It can als
CVE-	

2026-39405	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. In versions 2.50.0 and below, a user with course editing r
CVE-2026-39352	Frappe is a full-stack web application framework. Versions prior to 15.105.0 and 16.15.0 contain a possible Arbitrary File Read vulnerability via Path Traversal. The
CVE-2026-33137	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki Platform is a generic wiki platform. In versions starting w update documents in the target wiki. This vulnerability has been patched in XWiki 16.10.17, 17.4.9, 17.10.3, 18.0.1 and 18.1.0-rc-1.
CVE-2026-47071	Uncontrolled Resource Consumption vulnerability in benoitc hackney allows Flooding. The SOCKS5 transport in src/hackney_socks5.erl correctly applies the caller-s forwarded. A hostile SOCKS5 proxy that completes the SOCKS5 handshake normally and then goes silent (or sends a partial TLS ServerHello and stalls) will cause t
CVE-2026-9136	A vulnerability was identified in the ShadowAttribute proposal creation workflow. The add action accepted user-controlled ShadowAttribute request data without re the identifier of an existing ShadowAttribute and cause that record to be updated instead of creating a new proposal. This can result in unauthorized modification o data across event contexts. The vulnerability is caused by trusting a client-supplied primary key during object creation. The fix removes the id field from incoming
CVE-2026-9129	A path traversal vulnerability exists in the Altium Enterprise Server Viewer StorageController due to improper handling of file path route parameters. On on-premis and allowing arbitrary files to be read from the server filesystem. Because the readable files include the server's master configuration, which stores database crede and do not enable this component.
CVE-2026-8453	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this car
CVE-2026-9058	Szafir SDK returns a success status code from the cryptographic digital signature verification process (i.e. /VerifyingTaskItem/Signature/VerificationResult/Result/@ consuming applications to incorrectly treat the signature as valid despite an unverified certificate chain, enabling authentication bypass and user impersonation. Th
CVE-2026-8680	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-47066	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in benoitc hackney allows Excessive Allocation. The Alt-Svc response header parser in src/hackn first byte is not a comma. parse_entries/2 then recurses with identical data, creating a tight infinite tail-recursive loop that pins a scheduler at 100% CPU. The callir by any HTTP origin the client connects to. This issue affects hackney: from 2.0.0-beta.1 before 4.0.1.
CVE-2025-68709	SailingLab AppLock (aka com.alpha.applock) 4.3.8 for Android allows a local attacker to trigger arbitrary JavaScript execution via BrowserMainActivity, which accep
CVE-2026-8647	Crypt::ScryptKDF versions through 0.010 for Perl uses insecure random number source when no CSPRNG module is available. The random_bytes function fell back
CVE-2026-46740	Mojolicious::Plugin::Statsd versions through 0.04 for Perl allowed metric injections. The metric names and set values were not checked for newlines, colons or pipes similar issue (CVE-2026-46720).
CVE-2025-68710	Easyelife App lock (aka Fingerprint,Applock or locker.app.safe.applocker) 1.9.2 for Android allows a local attacker with physical access to bypass the PIN lock. The l advertisement or browser intents - an attacker can evade lockscreen verification and access protected apps (e.g., Chrome), resulting in information disclosure and
CVE-2026-2734	In mlflow/mlflow versions up to 3.9.0, the `SearchModelVersions` REST API endpoint and the `mlflowSearchModelVersions` GraphQL query lack proper per-model a `SearchModelVersions` in the `BEFORE_REQUEST_VALIDATORS` and `AFTER_REQUEST_HANDLERS` for the REST API, and its omission from `GraphQLAuthorization multi-tenant environments. The issue is resolved in version 3.10.0.
CVE-2026-9152	A missing authentication vulnerability exists in the Altium 365 SearchService. A legacy SOAP endpoint exposes search index operations without requiring authentic exploitation allows reading a workspace's indexed contents (such as component data, project and folder names, and user metadata) and injecting, modifying, or de cloud deployments are affected; on-premise Altium Enterprise Server is not affected.
CVE-2026-47067	Allocation of Resources Without Limits or Throttling vulnerability in benoitc hackney allows Flooding. The URL parser in src/hackney_url.erl converts every unrecogn prefixes — directly as request targets, as configured webhook URLs, or via Location headers followed during redirects — can exhaust the atom table and crash the
CVE-2026-8399	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-47782	Android App "RoboForm Password Manager" provided by Siber Systems, Inc. handles Android intents without sufficient URL validation, user confirmation nor notific
CVE-2026-47069	Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability in benoitc hackney allows HTTP Response Splitting. The hackney_cookie:setcookie/3 func either option — for example by supplying a Host header value forwarded as the cookie domain, or a request path forwarded as the cookie path — can inject a litera
CVE-2026-9137	The CSP report endpoint intended to limit logged CSP reports to 1 KB but incorrectly allowed reports up to 1 MB before truncation. On deployments where the endp
CVE-2026-44844	eml_parser serves as a python module for parsing eml files and returning various information found in the e-mail as well as computed information. Prior to 3.0.1, Er triggers an unhandled RecursionError and aborts parsing of the message. A 12 KB EML file is enough to crash a worker. Though this causes the parser to crash, it is
CVE-	

2026-23734	XWiki Platform is a generic wiki platform. Versions prior to 18.1.0-rc-1, 17.10.3, 17.4.9, and 16.10.17 allow access to read configuration files by using URLs such as issue has been patched in 18.1.0-rc-1, 17.10.3, 17.4.9, 16.10.17.
CVE-2026-44896	Mistune is a Python Markdown parser with renderers and plugins. In 3.2.0 and realier, in src/mistune/directives/image.py, the render_figure() function concatenates
CVE-2026-8376	Perl versions through 5.43.10 have a heap buffer overflow when compiling regular expressions with a repeated fixed string on 32-bit builds. Perl_study_chunk in re SvGROW allocation; the subsequent copy writes past the end of the buffer. A caller that compiles an attacker-controlled regular expression on a 32-bit perl build tri
CVE-2025-43290	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be a
CVE-2025-43451	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.
CVE-2025-46280	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Tahoe 26. An app may be able to cause unexpected system ter
CVE-2025-46284	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.7, macOS Tahoe 26. An app may be able to gain root privileges.
CVE-2025-46307	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.
CVE-2026-9065	SureCart version prior to 4.2.1 are vulnerable to authenticated SQL injection via multiple parameters ('model_name', 'model_id', 'integration_id', 'provider') on the F contain a dot ('.') or the WordPress table prefix ('wp_'). By including a dot anywhere in the payload, an attacker completely bypasses the escaping logic and injects
CVE-2026-9059	NextGEN Gallery version prior to 4.2.1 are vulnerable to authenticated SQL injection via the 'orderby' parameter on the REST API endpoints '/imagely/v1/galleries' a 'NextGEN Gallery overview' capability (assigned to the Administrator role by default) to inject arbitrary SQL into the 'ORDER BY' clause.
CVE-2026-44985	Dozzle is a realtime log viewer for docker containers. Prior to 10.5.2, he WebSocket upgrader for the /exec and /attach endpoints uses CheckOrigin: func(r *http.Re sibling subdomain, or another service on localhost) can initiate a WebSocket connection to the exec endpoint that carries the victim's valid JWT cookie, gaining inte
CVE-2026-44598	With valid login credentials, URL Redirection to Untrusted Site ('Open Redirect'), Server-Side Request Forgery (SSRF) vulnerability in Apache Shiro. This issue affect After successful login, Jakarta EE integration module uses shiroSavedRequest cookie to redirect to a particular web page after login. This cookie was not validated,
CVE-2026-43827	Default configurations of Apache Shiro have a session fixation vulnerability. This issue affects Apache Shiro from 1.0 to 2.1.0, and 3.0.0-alpha-1. Users are recomm
CVE-2026-43828	Default configurations of Apache Shiro send sensitive cookies in HTTPS session without 'Secure' attribute. This issue affects Apache Shiro from 1.0 to 2.1.0, and 3.0 rememberMe cookies without 'secure' attribute by default.
CVE-2026-44392	Missing authorization vulnerability exists in Movable Type. Under certain conditions, when a user without administrator privileges signs in to the product, unintende
CVE-2026-42497	Archive::Tar versions before 3.08 for Perl extract hardlinks to attacker controlled paths outside the extraction directory. _make_special_file() passes the tar header' chown, and utime block in _extract_file() (guarded only against symlinks via -l) applies the tar header's mode, owner, and timestamps to the shared inode during e
CVE-2026-44895	GitLab MCP Server lets an AI agent talk directly to GitLab. Prior to 0.6.0, the HTTP transport in src/transport.ts ships with no authentication layer at all and a wildca credential check, then advertises itself to every cross-origin browser context via the wildcard CORS header. The httpServer.listen(port) call at line 97 also passes n
CVE-2026-7460	mailcow-dockerized contains a stored cross-site scripting vulnerability in the administrator Queue Manager. The Queue Manager fetches mail queue entries from /a
CVE-2025-71310	The GDPR cookies module for Backdrop CMS (before 1.x-1.3.5) doesn't sufficiently protect visitors from Cross Site Scripting (XSS) if a malicious value has been pro added a YouTube service as configuration.
CVE-2025-43306	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. A malicious app may be able
CVE-2025-43289	A logic issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. A malicious app may be a
CVE-2026-47075	Improper Neutralization of CRLF Sequences vulnerability in benoitc hackney allows HTTP Request Splitting. hackney does not percent-encode carriage return (\r) or query binary directly without validation or escaping. An attacker who can control all or part of a URL passed to hackney can inject raw CRLF sequences into the que
CVE-	

2026-9538	Archive::Tar versions before 3.10 for Perl allow memory exhaustion via attacker controlled entry size field in tar header. _read_tar() reads each entry's payload with
CVE-2026-44903	Prometheus is an open-source monitoring system and time series database. From 2.49.0 to before 3.5.3 and 3.11.3, in the Prometheus server's legacy web UI (ena execute JavaScript in the browser of any Prometheus user who views the metric in the heatmap chart UI. This vulnerability is fixed in 3.5.3 and 3.11.3.
CVE-2026-8342	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this car
CVE-2026-9084	MISP's OIDC authentication plugin allowed automatic linking of an OIDC identity to an existing local user account based on the email claim when the local account takeover.
CVE-2026-47076	Interpretation Conflict vulnerability in benoitc hackney allows Server Side Request Forgery. hackney_url:normalize/2 URL-decodes the host component after the UR validator with host %31%32%37%2E%30%2E%30%2E%31 (not an IP address), which passes the allowlist check. hackney's normalizer then decodes the host to 12 metadata services (169.254.169.254), RFC1918 networks, and any admin interface listening on localhost. This issue affects hackney: from 0.13.0 before 4.0.1.
CVE-2026-45412	MaxKB is an open-source AI assistant for enterprise. Prior to 2.9.1, SSRF via work_flow_template Import. Authenticated users can supply arbitrary URLs in work_flow
CVE-2026-45413	MaxKB is an open-source AI assistant for enterprise. Prior to 2.9.1, user passwords are stored using unsalted MD5 hashes, making them trivially crackable via rainb
CVE-2026-40127	OutSystems Lifetime is vulnerable to Authorization Bypass Through User-Controlled Key vulnerability in ApplicationID parameter. Any authenticated user, can read
CVE-2026-8469	Allocation of Resources Without Limits or Throttling vulnerability in phenixdigital phoenix_storybook allows unauthenticated denial-of-service via BEAM atom table of the psb-assign params map; 'Elixir.PhoenixStorybook.ExtraAssignsHelpers':handle_toggle_variation_assign/3 interns the "attr" value from psb-toggle events; 'Elix are never garbage-collected, so each unique attacker-controlled string is a permanent allocation. Once the atom table ceiling (~1,048,576 atoms) is reached, the e
CVE-2026-48592	Missing Authorization vulnerability in oban-bg oban_web ('Elixir.Oban.Web.Jobs.DetailComponent' modules) allows unauthorized job worker substitution. The handl with :read_only access can push a forged save-job LiveView WebSocket event to overwrite a job's worker field with any other existing Oban.Worker module in the a
CVE-2026-48593	Uncontrolled Resource Consumption vulnerability in oban-bg oban_web ('Elixir.Oban.Web.CronExpr' modules) allows memory exhaustion via unbounded cron range to render the expression. parse_range/1 parses both range endpoints via Integer.parse/1 with no bounds check, and the downstream helpers expand_dom_parts/1 helpers do not. This issue affects oban_web: from 2.12.0 before 2.12.5.
CVE-2026-8467	Code Injection vulnerability in phenixdigital phoenix_storybook allows unauthenticated remote code execution via unsanitized attribute value interpolation in HEEx to 'Elixir.PhoenixStorybook.Helpers.ExtraAssignsHelpers':handle_set_variation_assign/3, which stores them verbatim. When rendering, 'Elixir.PhoenixStorybook.Ren containing a closing quote followed by a HEEx expression block (e.g. foo" injected={EXPR} bar="), which causes EXPR to be treated as an inline Elixir expression. phoenix_storybook from 0.5.0 before 1.1.0.
CVE-2026-47068	Authorization Bypass Through User-Controlled Key vulnerability in phenixdigital phoenix_storybook allows cross-session PubSub topic injection via a URL query para self()} on it with no check that the topic belongs to the requesting session. The shared PhoenixStorybook.PubSub is used to coordinate playground LiveViews with query parameter, an attacker who loads /storybook/iframe/<story>?topic=<victim_topic> causes their iframe process pid to be announced on the victim's topic. T
CVE-2026-48589	Apache Shiro's Jakarta EE module used the HTTP Referer header in certain cases to issue redirect after a user login. In affected versions, insufficient validation of th integration module.
CVE-2026-47077	Allocation of Resources Without Limits or Throttling vulnerability in benoitc hackney allows Flooding. hackney_h3:await_response_loop/6 accumulates the HTTP/3 re server that emits one small chunk every Timeout - 1 ms with Fin = false and never sends a final frame keeps the loop alive indefinitely while the accumulation buff
CVE-2026-42782	Improper Isolation or Compartmentalization vulnerability in Apache Syncope. An administrator with adequate entitlements for Implementations can create a malici version 4.0.6 / 4.1.1, which fix this issue by forcing even the static initializer in Groovy code to run in a sandbox.
CVE-2026-7766	Kenik Camera management Panel is vulnerable to Path Traversal vulnerability. An unauthenticated attacker can send GET request with arbitrary file path and read
CVE-2026-39970	TypeBot is a chatbot builder tool. Versions 3.15.2 and prior contain a critical stored XSS vulnerability in the app.typebot.io profile picture upload form. The applicati code. This vulnerability directly enables stored XSS exploitation because the payload is persistently stored on your infrastructure (app.typebot.io) and accessible fr user data. This issue has been fixed in version 3.16.0.
CVE-2026-9274	This vulnerability exists in CP Plus Wi-Fi Camera due to improper protection of sensitive information in runtime memory. An attacker with physical access could exp Successful exploitation of this vulnerability could allow unauthorized access to encrypted communications and connected wireless network of the targeted device.
CVE-2026-3294	An authentication logic vulnerability in multiple TP-Link range extenders allows an unauthenticated attacker on an adjacent network to manipulate a login paramet
CVE-2026-40596	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.11.0 through 2.28.1 allow any authenticated user to inject arbitrary HTML by updating th been fixed in version 2.28.2.
CVE-2026-48091	Rejected reason: Further research determined the issue is not a vulnerability.

CVE-2026-40597	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions 2.28.1 and below, given any pre-existing XSS / HTML injection vulnerability, an attacker execution. The uploaded payload must be sniffed as a valid JavaScript MIME type by PHP finfo (see file_create_finfo() API function). Non-JavaScript MIME types will r 2.28.2.
CVE-2026-40598	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions 2.28.1 and below, improper escaping of the redirection page (retrieved from the request cross-site scripting. This issue has been fixed in version 2.28.2.
CVE-2026-48691	FastNetMon Community Edition through 1.2.9 contains an integer overflow in the BGP AS_PATH attribute encoder. In src/bgp_protocol.hpp, the IPv4UnicastAnnounc AS_PATH containing more than 63 ASNs (2 + 64*4 = 258 > 255) causes silent truncation. The truncated length is used for buffer sizing, while the actual data writte
CVE-2026-40607	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions 2.11.0 through 2.28.1, a Stored XSS vulnerability is caused by incorrect escaping of a sa in version 2.28.2. If developers are unable to update immediately, they can work around this issue by preventing display of users' real names (set $g_ show_user_r
CVE-2026-8997	vifm is vulnerable to a heap buffer overflow during the history merge process when saving the state file (vifminfo.json). This flaw occurs because the application la considered vulnerable. This issue was fixed in commit 23063c7
CVE-2026-48896	Insufficient state checks lead to a vector that allows to bypass 2FA checks.
CVE-2026-45836	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix null-ptr-deref in l2cap_sock_get_sndtimeo_cb() Add the same NULL guard a
CVE-2026-48897	Insufficient state checks lead to a vector that allows to bypass 2FA checks.
CVE-2026-41071	libheif is a HEIF and AVIF file format decoder and encoder. In versions 1.21.2 and prior, a crafted HEIF sequence file where the saiz box declares more samples thar validate that this count is consistent with the number of chunks in the chunks vector. When saiz declares more samples than the chunks cover, the loop increment open untrusted HEIF files is affected. This issue has been fixed in version 1.22.0.
CVE-2026-48901	The InputFilter::getInstance() method omitted a security sensitive parameter from the instance cache key.
CVE-2026-48902	The password and username reset features created plain http links for https connections if the "Force SSL" flag wasn't explicitly set.
CVE-2026-48687	FastNetMon Community Edition through 1.2.9 contains an OS command injection vulnerability in the Juniper router integration plugin. The _log() function in src/juni variable contains unsanitized data derived from command-line arguments argv[1] through argv[3], which represent the attack IP address, direction, and power. Wh orchestration system, or if future code changes pass string-sourced IPs, arbitrary commands can be injected. The correct fix is to replace exec() with file_put_conte
CVE-2026-41148	Mermaid is a JavaScript tool that uses Markdown-inspired text to create and modify diagrams and charts. Versions 10.9.5 and prior, in addition to 11.0.0-alpha.1 th unrestricted regex that matches everything up to a newline. That value then flows unsanitized through addStyleClass() into createCssStyles() and is assigned to sty exfiltration. This issue has been fixed in versions 10.9.6 and 11.15.0. If developers are unable to immediately upgrade, they can work around this issue by setting "
CVE-2026-25608	STER uses unencrypted TCP traffic to transmit data over the network. It allows an attacker to conduct a Man-In-The-Middle attack and obtain sensitive data such as
CVE-2026-39824	NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit numb
CVE-2026-45835	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix null-ptr-deref in l2cap_sock_new_connection_cb() Add the same NULL guarc
CVE-2026-5223	Cargo incorrectly handled symlinks inside of crate tarballs downloaded from third-party registries, allowing a malicious crate to override the source code of another
CVE-2026-35222	Improperly validated order clauses lead to a SQL injection vulnerability in com_tags.
CVE-2026-25900	Lack of output escaping leads to a XSS vector in the feed modules.
CVE-2026-25901	Lack of output escaping leads to a XSS vector in the multilingual associations component.
CVE-2026-2264	A vulnerability in the Google Cloud Apigee SetIntegrationRequest policy allowed remote attackers to perform Server-Side Request Forgery (SSRF) and exfiltrate ser
CVE-2026-30894	Lack of output escaping leads to a XSS vector in the content history component.

CVE-2026-30895	Lack of output escaping leads to a XSS vector in the readmore links for com_content.
CVE-2026-35220	Lack of CSRF token validation lead to a CSRF attack vector in the admin activation endpoint of com_users.
CVE-2026-35221	Improperly built filter clauses lead to a SQL injection vulnerability in the search query for com_finder.
CVE-2026-35223	An improper access check allows unauthorized access to com_config webservice endpoints.
CVE-2026-45834	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix null-ptr-deref in l2cap_sock_state_change_cb() Add the same NULL guard a
CVE-2026-40383	An improper validation of user-supplied input leads to a local file inclusion vulnerability.
CVE-2026-40384	An improper validation of the search parameter of the com_media files API endpoint leads to a path traversal vulnerability.
CVE-2026-43981	Algernon is a small self-contained pure-Go web server. Prior to 1.17.6, in engine/luahandler.go, the sync.RWMutex protecting LoadCommonFunctions is released be concurrency (ab -n 1000 -c 100). This vulnerability is fixed in 1.17.6.
CVE-2026-43982	Algernon is a small self-contained pure-Go web server. Prior to 1.17.6, uploadedFileSaveIn() in lua/upload/upload.go uses filepath.Join() with the caller-supplied dire
CVE-2026-44314	Traccar is an open source GPS tracking system. Prior to 6.13.0, DeviceResource.uploadImage authorizes the target device only through Condition.Permission(User. updateAccumulators, this route never invokes permissionsService.checkEdit(getUserId(), Device.class, false, false). The skipped guard is exactly where Traccar enf workflows that rely on the persisted image, despite other device update paths correctly rejecting the same identity. This vulnerability is fixed in 6.13.0.
CVE-2026-40166	authentik is an open-source identity provider. In versions prior to 2025.12.5 and 2026.2.0-rc1 through 2026.2.2, authenticated non-admin users with at least one O /api/v3/oauth2/access_tokens/. The API response includes a nested provider object containing client_id and client_secret for providers configured with client_type: c
CVE-2026-48700	An issue was discovered in all versions of PCManFM-Qt starting from 1.1.0. When a regular file's path is passed as a URI in an org.freedesktop.FileManager1.ShowF outcomes are potentially unwanted by most users; however, the behavior of the product does comply with the applicable specification, and a simplistic solution (er
CVE-2026-25607	Use of a weak password encoding algorithm in STER software allows the value of the password to be guessed after analyzing how passwords with known values ar
CVE-2026-25606	A SQL injection vulnerability has been identified in STER. Improper neutralization of input provided by user into multiple Search Filters allows for SQL Injection attac
CVE-2026-41149	Mermaid is a JavaScript tool that uses Markdown-inspired text to create and modify diagrams and charts. Versions 10.9.5 and earlier, as well as 11.0.0-alpha.1 thro prevents cross-site scripting (XSS). This issue has been fixed in versions 10.9.6 and 11.15.0. If developers are unable to immediately upgrade, they can work aroun
CVE-2026-43494	In the Linux kernel, the following vulnerability has been resolved: net/rds: reset op_nents when zerocopy page pin fails When iov_iter_get_pages2() fails in rds_mes cleanup loop iterates over the incorrectly non zero number of op_nents and frees them again. Fix this by properly resetting op_nents when it should be in rds_mess
CVE-2026-43497	In the Linux kernel, the following vulnerability has been resolved: fbdev: udlfb: add vm_ops to dlfb_ops_mmap to prevent use-after-free dlfb_ops_mmap() uses rem existing mmap PTEs are not invalidated. On USB disconnect, dlfb_ops_destroy() calls vfree() on the old pages while userspace PTEs still reference them, resulting in and return -EBUSY if the buffer is currently mapped, preventing buffer replacement while userspace holds stale PTEs. Tested with PoC using dummy_hcd + raw_ga
CVE-2026-44775	Kavita is a cross platform reading server. Prior to 0.9.0, the ReaderController.GetImage endpoint is decorated with [AllowAnonymous], allowing completely unauthe content on the server. This vulnerability is fixed in 0.9.0.
CVE-2026-44776	Kavita is a cross platform reading server. Prior to 0.9.0, the download, size-check, and chapter metadata endpoints do not enforce library-level authorization. A low /api/Download/volume-size, /api/Download/chapter-size, /api/Download/series-size, /api/Download/volume, /api/Download/chapter, /api/Download/series, and /api/Cl
CVE-2026-47202	Kavita is a cross platform reading server. Prior to 0.9.0.2, an Improper Token validation flaw permits a remote and unauthenticated threat actor to request a JWT fo
CVE-2026-43496	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_red: Replace direct dequeue call with peek and qdisc_dequeue_peeked When red will do the following: 1a. do a peek() - and when sensing there's an skb the child can offer, then - the child in this case(red) calls its child's (qfq) peek. qfq does the essentially just try to grab something of qfq's queue. [78.667668][T363] KASAN: null-ptr-deref in range [0x0000000000000048-0x000000000000004f] [78.66792 0010:qfq_dequeue+0x446/0xc90 [sch_qfq] [78.668718][T363] Code: 54 c0 e8 dd 90 00 f1 48 c7 c7 e0 03 54 c0 48 89 de e8 ce 90 00 f1 48 8d 7b 48 b8 ff ff 37 0 0000000000000000 RCX: 0000000000000000 [78.669790][T363] RDX: 0000000000000009 RSI: 0000000000000004 RDI: 0000000000000048 [78.670044][T36 0000000000000200 [78.670814][T363] FS: 00007f66a8f09c40(0000) GS:ffff888163428000(0000) knlGS:0000000000000000 [78.671110][T363] CS: 0010 DS: 0 [78.671936][T363] ? __pfx_qfq_dequeue+0x10/0x10 [sch_qfq] [78.672148][T363] ? __pfx__printk+0x10/0x10 [78.672322][T363] ? srso_alias_return_thunk+0x5 [sch_red] [78.673217][T363] ? srso_alias_return_thunk+0x5/0xfbef5 [78.673385][T363] tbf_dequeue.cold+0xb0/0x70c [sch_tbf] [78.673566][T363] __qdisc_run

CVE-2026-43495	In the Linux kernel, the following vulnerability has been resolved: net: wwan: t7xx: validate port_count against message length in t7xx_port_enum_msg_handler t7: triggers a slab-out-of-bounds read of up to 262140 bytes. Add a sizeof(*port_msg) check before accessing the port message header fields to guard against undersi against the actual remaining buffer to prevent OOB reads and signed integer overflow on offset. Pass msg_len from both call sites: skb->len at the DPMAIF path aft
CVE-2026-48696	FastNetMon Community Edition through 1.2.9 has a buffer overflow, a different vulnerability than CVE-2026-48686 and CVE-2026-48689.
CVE-2026-0393	The affected product may expose credentials remotely between low privileged visualization users during concurrent login operations due to insufficient isolation of
CVE-2026-34970	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and prior allow a bugnote author to access the note's Revisions page after losing ac
CVE-2026-9489	NitroSense 3.x before 3.01.3052 contains Local Privilege Escalation (LPE) vulnerability.The program exposes a Windows Named Pipe that uses a custom protocol to leveraging this, an attacker can execute arbitrary code on the target system with elevated privileges.
CVE-2026-6059	A cross-site scripting vulnerability exists in Aterm. Arbitrary scripts may be executed in the web browser of a user accessing the web management interface via ad
CVE-2026-8652	An OS Command Injection vulnerability exists in Aterm. If a malicious third person gains administrator access to the product’s web console, they may be able to ex
CVE-2026-2651	A vulnerability in MLflow versions <=3.10.1.dev0 allows unauthorized access to multipart upload (MPU) endpoints when the `--serve-artifacts` mode is enabled. Th supply chain poisoning, and arbitrary code execution when compromised models are loaded. The issue is resolved in version 3.10.0.
CVE-2026-9490	A security vulnerability has been identified in Acer Care Center where the ACCSvc service creates a Named Pipe with a weak Security Descriptor. This vulnerability disruption, Acer requires users to update the software to the latest version.
CVE-2026-5222	Cargo between 1.68 and 1.96 incorrectly normalized the URLs of third-party registries using the sparse index protocol. If a hosting provider allowed multiple registr extremely niche requirements needed to achieve the attack.
CVE-2026-9560	Privilege escalation via background service of OpenVPN Connect 3.5.1 through 3.8.1 on macOS allows attackers to execute arbitrary commands with elevated privi
CVE-2026-43498	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Disallow re-exporting imported GEM objects Prevent re-exporting of imported GEM bu corruption.
CVE-2026-43499	In the Linux kernel, the following vulnerability has been resolved: rtmutex: Use waiter::task instead of current in remove_waiter() remove_waiter() is used by the sl That results in several problems: 1) the rbtree dequeue happens without waiter::task::pi_lock being held 2) the waiter task's pi_blocked_on state is not cleared, whi tglx: Fixup rt_mutex_adjust_prio_chain(), add a comment and amend the changelog]
CVE-2026-43501	In the Linux kernel, the following vulnerability has been resolved: ipv6: rpl: reserve mac_len headroom when recompressed SRH grows ipv6_rpl_srh_rcv() decompre received one when the swap reduces the common-prefix length the segments share with daddr (CmprI=0, CmprE>0, seg[0][0] != daddr[0] gives the maximum +8 skb_set_mac_header(skb, -skb->mac_len); will store (data - head) - mac_len into the u16 mac_header field, which wraps to ~65530, and the following memmove() ipv6_rthdr_rcv. Fix this by expanding the head whenever the remaining room is less than the push size plus mac_len, and request that much extra so the rebuilt M
CVE-2026-43502	In the Linux kernel, the following vulnerability has been resolved: net/rds: handle zerocopy send cleanup before the message is queued A zerocopy send can fail af However, zerocopy ownership is really determined by the presence of op_mmp_znotifier, regardless of whether the message has reached the socket queue. Captu release the notifier before putting the payload pages. This keeps early send failure cleanup consistent with the zerocopy lifetime rules without changing the norma
CVE-2026-40564	Files or Directories Accessible to External Parties, Server-Side Request Forgery (SSRF) vulnerability in Apache Flink Kubernetes Operator. The FlinkSessionJob jarUR pluggable filesystem layer and access them through the submitted Flink job. Furthermore for fetching from http/https addresses there is currently no allowlist on th upgrade to version 1.15.0, which fixes the issue.
CVE-2026-3515	A vulnerability in the `GitHubRepository` block of the `prefect-github` integration in Prefect version 3.6.18 allows an attacker to inject arbitrary git command-line o potential Server-Side Request Forgery (SSRF), credential theft, or remote code execution (RCE). The vulnerability affects both the `aget_directory()` and `get_direc
CVE-2026-4372	A critical remote code execution vulnerability exists in all versions of the HuggingFace transformers library prior to version 5.3.0. The vulnerability allows an attack `AutoModelForCausalLM.from_pretrained()` API, the library downloads and executes arbitrary Python code from the attacker's repository with the victim's full OS p security mechanism, is invisible to the victim, and exploits the standard documented usage pattern, making it particularly severe. Users are advised to upgrade to
CVE-2026-9054	An attacker sending tcp, il, rudp, rudp, or gre packets with a length less than the header size would trigger a kernel panic.
CVE-2026-9053	Mothra would respect a default value given by a website for HTML file upload forms. An attacker could craft a website with a malicious default file path, and then c
CVE-2026-5297	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-43918. Reason: This candidate is a duplicate of CVE-2026-43918. Not

43919	
CVE-2026-42347	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-28496. Reason: This candidate is a duplicate of CVE-2026-28496. Not
CVE-2026-48831	Wine ships a .desktop file that registers itself as a MIME handler for EXE files and several other Windows executable file types. In some configurations, handling of a parties feel that this is not a bug to be addressed in Wine, because there is no known solution that avoids a severe loss of usability (Wine could be a binfmt-misc ha
CVE-2026-4929	Simple Hierarchical Select (SHS) for Drupal 7 contains cross-site scripting risk due to improper output escaping of term-derived text. Confirmed affected paths inclu 7.x-1.0 through (and including) 7.x-1.10.
CVE-2026-4093	In the Drupal 7 Term Reference Tree module, two stored XSS vectors exist in the widget/formatter rendering pipeline. Vector A (token display templates): When the HTML/JS that executes when the field is rendered. Vector B (term label rendering): Taxonomy term labels are not properly sanitized before being rendered in the w
CVE-2026-8352	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this can
CVE-2026-8479	IEC 60870-5-104 used in bidirectional mode in RTU500 is vulnerable for a NULL pointer dereferencing, if a specially crafted sequence of messages is sent for a cert
CVE-2026-7310	A heap-based buffer overflow vulnerability exists in XML parser functionality in the HiDraw. An authenticated malicious user with local access can exploit this vulne integrity of the affected system.
CVE-2026-6841	Request Tracker is vulnerable to a reflected cross-site scripting (XSS) vulnerability via the "Page" parameter in GET requests. An attacker can craft a URL that, whe
CVE-2026-43503	In the Linux kernel, the following vulnerability has been resolved: net: skbuff: propagate shared-frag marker through frag-transfer helpers Two frag-transfer helpers after copying frag descriptors, but that helper only carries over gso_{size,segs, type} and never touches skb_shinfo()->flags; skb_shift() moves frag descriptors dir that uses skb_has_shared_frag() to decide whether shared pages must be detoured through skb_cow_data(). ESP input is one such writer (esp4.c, esp6.c), and a sir via authencesn-ESN stray writes. Set SKBFL_SHARED_FRAG on the destination whenever frag descriptors were actually moved from the source. skb_copy() and skb exists in skb_gro_receive() and skb_gro_receive_list(). The former moves the incoming skb's frag descriptors into the accumulator's last sub-skb via two paths (a di nskb -- both p and lp must carry the marker. The same omission also exists in tcp_clone_payload(), which builds an MTU probe skb by moving frag descriptors from consumer depending on the marker would regress silently. The same omission exists in skb_segment(): the per-iteration flag merge takes only head_skb's flag, and