SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 August 2025

Generated on 13 August 2025

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-2025-53767	Azure OpenAI Elevation of Privilege Vulnerability	10.0	More Details
CVE-2025-42950	SAP Landscape Transformation (SLT) allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of the system.	9.9	More Details
CVE-2025-42957	SAP S/4HANA allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of the system.	9.9	More Details
CVE-2025-8356	In Xerox FreeFlow Core version 8.0.4, an attacker can exploit a Path Traversal vulnerability to access unauthorized files on the server. This can lead to Remote Code Execution (RCE), allowing the attacker to run arbitrary commands on the system.	9.8	More Details
CVE-2025-54951	A group of related buffer overflow vulnerabilities in the loading of ExecuTorch models can cause the runtime to crash and potentially result in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit cea9b23aa8ff78aff92829a466da97461cc7930c.	9.8	More Details
CVE-2025-54952	An integer overflow vulnerability in the loading of ExecuTorch models can cause smaller-than-expected memory regions to be allocated, potentially resulting in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit 8f062d3f661e20bb19b24b767b9a9a46e8359f2b.	9.8	More Details
CVE-2025-8059	The B Blocks plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization and improper input validation within the rgfr_registration() function in all versions up to, and including, 2.0.6. This makes it possible for unauthenticated attackers to create a new account and assign it the administrator role.	9.8	More Details
CVE-2025-6994	The Reveal Listing plugin by smartdatasoft for WordPress is vulnerable to privilege escalation in versions up to, and including, 3.3. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'listing_user_role' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role.	9.8	More Details
CVE-2025-53606	Deserialization of Untrusted Data vulnerability in Apache Seata (incubating). This issue affects Apache Seata (incubating): 2.4.0. Users are recommended to upgrade to version 2.5.0, which fixes the issue.	9.8	More Details
CVE-2025-8730	A vulnerability was found in Belkin F9K1009 and F9K1010 2.00.04/2.00.09 and classified as critical. Affected by this issue is some unknown functionality of the component Web Interface. The manipulation leads to hard-coded credentials. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-48913	If untrusted users are allowed to configure JMS for Apache CXF, previously they could use RMI or LDAP URLs, potentially leading to code execution capabilities. This interface is now restricted to reject those protocols, removing this possibility. Users are recommended to upgrade to versions 3.6.8, 4.0.9 or 4.1.3, which fix this issue.	9.8	More Details
CVE-2025-54950	An out-of-bounds access vulnerability in the loading of ExecuTorch models can cause the runtime to crash and potentially result in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit b6b7a16df5e7852d976d8c34c8a7e9a1b6f7d005.	9.8	More Details
CVE-2025-8284	By default, the Packet Power Monitoring and Control Web Interface do not enforce authentication mechanisms. This vulnerability could allow unauthorized users to access and manipulate monitoring and control functions.	9.8	More Details

CVE-2025-52913	A vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab through 9.8 SP2 (9.8.2.12) could allow an unauthenticated attacker to conduct a path traversal attack due to insufficient input validation. A successful exploit could allow unauthorized access, enabling the attacker to view, corrupt, or delete users' data and system configurations.	9.8	More Details
CVE-2025-5095	Burk Technology ARC Solo's password change mechanism can be utilized without proper authentication procedures, allowing an attacker to take over the device. A password change request can be sent directly to the device's HTTP endpoint without providing valid credentials. The system does not enforce proper authentication or session validation, allowing the password change to proceed without verifying the request's legitimacy.	9.8	More Details
CVE-2025-6573	Kernel software installed and running inside an untrusted/rich execution environment (REE) could leak information from the trusted execution environment (TEE).	9.8	More Details
CVE-2025-8853	Official Document Management System developed by 2100 Technology has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to obtain any user's connection token and use it to log into the system as that user.	9.8	More Details
CVE-2025-45146	ModelCache for LLM through v0.2.0 was discovered to contain an deserialization vulnerability via the component /manager/data_manager.py. This vulnerability allows attackers to execute arbitrary code via supplying crafted data.	9.8	More Details
CVE-2025-8731	A vulnerability was identified in TRENDnet TI-G160i, TI-PG102i and TPL-430AP up to 20250724. This affects an unknown part of the component SSH Service. The manipulation leads to use of default credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The vendor explains: "For product TI-PG102i and TI-G160i, by default, the product's remote management options are all disabled. The root account is for troubleshooting purpose and the password is encrypted. However, we will remove the root account from the next firmware release. For product TPL-430AP, the initial setup process requires user to set the password for the management GUI. Once that was done, the default password will be invalid."	9.8	More Details
CVE-2025-54949	A heap buffer overflow vulnerability in the loading of ExecuTorch models can potentially result in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit ede82493dae6d2d43f8c424e7be4721abe5242be	9.8	More Details
CVE-2025-30405	An integer overflow vulnerability in the loading of ExecuTorch models can cause objects to be placed outside their allocated memory area, potentially resulting in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit 0830af8207240df8d7f35b984cdf8bc35d74fa73.	9.8	More Details
CVE-2025-30404	An integer overflow vulnerability in the loading of ExecuTorch models can cause overlapping allocations, potentially resulting in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit d158236b1dc84539c1b16843bc74054c9dcba006.	9.8	More Details
CVE-2025-50165	Untrusted pointer dereference in Microsoft Graphics Component allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2025-53766	Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2025-48709	An issue was discovered in BMC Control-M 9.0.21.300. When Control-M Server has a database connection, it runs DBUStatus.exe frequently, which then calls dbu_connection_details.vbs with the username, password, database hostname, and port written in cleartext, which can be seen in event and process logs in two separate locations.	9.8	More Details
CVE-2025-50692	FoxCMS <=v1.2.5 is vulnerable to Code Execution in admin/template_file/editFile.html.	9.8	More Details
CVE-2023-41530	Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the app_contact parameter in appsearch.php.	9.8	More Details
CVE-2023-41528	Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in contact.php via the txtname, txtphone, and txtmail parameters.	9.8	More Details
CVE-2023-41527	Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the password2 parameter in func.php.	9.8	More Details
CVE-2023-41526	Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in func1.php via the username3 and password3 parameters.	9.8	More Details
CVE-2023-41525	Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the patient_contact parameter in patientsearch.php.	9.8	More Details
CVE-2025-30127	An issue was discovered on Marbella KR8s Dashcam FF 2.0.8 devices. Once access is gained either by default, common, or cracked passwords, the video recordings (containing sensitive routes, conversations, and footage) are open for downloading by creating a socket to command port 7777, and then downloading video via port 7778 and audio via port 7779.	9.8	More Details
CVE-2025-25256	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiSIEM version 7.3.0 through 7.3.1, 7.2.0 through 7.2.5, 7.1.0 through 7.1.7, 7.0.0 through 7.0.3 and before 6.7.9 allows an unauthenticated attacker to execute unauthorized code or commands via crafted CLI requests.	9.8	More Details
CVE-2025-23311	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a stack overflow through specially crafted HTTP requests. A successful exploit of this vulnerability might lead to remote code execution, denial of service, information disclosure, or data tampering.	9.8	More Details
CVE-2025-23310	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause stack buffer overflow by specially crafted inputs. A successful exploit of this vulnerability might lead to remote code execution, denial of service, information disclosure, and data tampering.	9.8	More Details
CVE-2024-32640	MASA CMS is an Enterprise Content Management platform based on open source technology. Versions prior to 7.4.6, 7.3.13, and 7.2.8 contain a SQL injection vulnerability in the `processAsyncObject` method that can result in remote code execution. Versions 7.4.6, 7.3.13, and 7.2.8 contain a fix for the issue.	9.8	More Details
CVE-2025-49457	Untrusted search path in certain Zoom Clients for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access	9.6	More Details
	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and		

CVE-2025-54997	keys. In versions 2.3.1 and below, some OpenBao deployments intentionally limit privileged API operators from executing system code or making network connections. However, these operators can bypass both restrictions through the audit subsystem by manipulating log prefixes. This allows unauthorized code execution and network access that violates the intended security model. This issue is fixed in version 2.3.2. To workaround, users can block access to sys/audit/* endpoints using explicit deny policies, but root operators cannot be restricted this way.	9.1	More Details
CVE-2025-54887	jwe is a Ruby implementation of the RFC 7516 JSON Web Encryption (JWE) standard. In versions 1.1.0 and below, authentication tags of encrypted JWEs can be brute forced, which may result in loss of confidentiality for those JWEs and provide ways to craft arbitrary JWEs. This puts users at risk because JWEs can be modified to decrypt to an arbitrary value, decrypted by observing parsing differences and the GCM internal GHASH key can be recovered. Users are affected by this vulnerability even if they do not use an AES-GCM encryption algorithm for their JWEs. As the GHASH key may have been leaked, users must rotate the encryption keys after upgrading. This issue is fixed in version 1.1.1.	9.1	More Details
CVE-2025-40746	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.2). Affected products do not properly validate input for a backup script. This could allow an authenticated remote attacker with high privileges in the application to execute arbitrary code with 'NT Authority/SYSTEM' privileges.	9.1	More Details
CVE-2025-55010	Kanboard is project management software that focuses on the Kanban methodology. Prior to version 1.2.47, an unsafe deserialization vulnerability in the ProjectEventActvityFormatter allows admin users the ability to instantiate arbitrary php objects by modifying the event["data"] field in the project_activities table. A malicious actor can update this field to use a php gadget to write a web shell into the /plugins folder, which then gives remote code execution on the host system. This issue has been patched in version 1.2.47.	9.1	More Details
CVE-2025-53792	Azure Portal Elevation of Privilege Vulnerability	9.1	More Details
CVE-2025-50171	Missing authorization in Remote Desktop Server allows an unauthorized attacker to perform spoofing over a network.	9.1	More Details
CVE-2025-45765	ruby-jwt v3.0.0.beta1 was discovered to contain weak encryption. NOTE: the Supplier's perspective is "keysize is not something that is enforced by this library. Currently more recent versions of OpenSSL are enforcing some key sizes and those restrictions apply to the users of this gem also."	9.1	More Details
CVE-2025-23317	NVIDIA Triton Inference Server contains a vulnerability in the HTTP server, where an attacker could start a reverse shell by sending a specially crafted HTTP request. A successful exploit of this vulnerability might lead to remote code execution, denial of service, data tampering, or information disclosure.	9.1	More Details
CVE-2025-54594	react-native-bottom-tabs is a library of Native Bottom Tabs for React Native. In versions 0.9.2 and below, the github/workflows/release-canary.yml GitHub Actions repository workflow improperly used the pull_request_target event trigger, which allowed for untrusted code from a forked pull request to be executed in a privileged context. An attacker could create a pull request containing a malicious preinstall script in the package.json file and then trigger the vulnerable workflow by posting a specific comment (!canary). This allowed for arbitrary code execution, leading to the exfiltration of sensitive secrets such as GITHUB_TOKEN and NPM_TOKEN, and could have allowed an attacker to push malicious code to the repository or publish compromised packages to the NPM registry. There is a remediation commit which removes github/workflows/release-canary.yml, but a version with this fix has yet to be released.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2025-24000	Authentication Bypass Using an Alternate Path or Channel vulnerability in WPExperts Post SMTP allows Authentication Bypass.This issue affects Post SMTP: from n/a
CVE-2025-54788	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. In versions and below, the InboundEmail module all implications on confidentiality, integrity, and availability, as database data can be retrieved, modified, or removed entirely. This issue is fixed in version 7.14.7.
CVE-2025-8831	A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This affects the function remoteManagement of the f is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but
CVE-2025-8817	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this vulnerability is the function setLa attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not r
CVE-2025-49759	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a networ
CVE-2025-49758	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a networ
CVE-2025-49757	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.
CVE-2025-49712	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.
CVE-2025-8816	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected is the function setOpMode of the file /g launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respor

CVE-2025-52914	A vulnerability in the Suite Applications Services component of Mitel MiCollab 10.0 through SP1 FP1 (10.0.1.101) could allow an authenticated attacker to conduct a arbitrary SQL database commands.
CVE-2025-24999	Improper access control in SQL Server allows an authorized attacker to elevate privileges over a network.
CVE-2025-53145	Access of resource using incompatible type ('type confusion') in Windows Message Queuing allows an authorized attacker to execute code over a network.
CVE-2025-54785	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. In versions 7.14.6 and 8.8.0, user-supplied input is r escalation, sensitive data exposure, Denial of Service, cryptomining and ransomware. This issue is fixed in version 7.14.7 and 8.8.1.
CVE-2025-8578	Use after free in Cast in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromiu
CVE-2025-53144	Access of resource using incompatible type ('type confusion') in Windows Message Queuing allows an authorized attacker to execute code over a network.
CVE-2025-53143	Access of resource using incompatible type ('type confusion') in Windows Message Queuing allows an authorized attacker to execute code over a network.
CVE-2025-8826	A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This vulnerability affects the function um_rp_au leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacte
CVE-2025-8824	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this issue is the function setRIP of t attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not
CVE-2025-53778	Improper authentication in Windows NTLM allows an authorized attacker to elevate privileges over a network.
CVE-2025-8822	A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected is the function algDisable of the file /go launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respor
CVE-2025-53772	Deserialization of untrusted data in Web Deploy allows an authorized attacker to execute code over a network.
CVE-2025-47954	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a networ
CVE-2025-8820	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This vulnerability affects the function wirelessB overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure
CVE-2025-8819	A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This affects the function setWan of the file /goform/s remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8576	Use after free in Extensions in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extensi
CVE-2025-53520	The affected product allows firmware updates to be downloaded from EG4's website, transferred via USB dongles, or installed through EG4's Monitoring Center (rer TTComp archive format used for the firmware is unencrypted and can be unpacked and altered without detection.
CVE-2025-4796	The Eventin plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 4.0.34. This is due to the plugin not 'Eventin\Speaker\Api\SpeakerController::update_item' function. This makes it possible for unauthenticated attackers with contributor-level and above permissions t gain access to their account.
CVE-2025-51629	A cross-site scripting (XSS) vulnerability in the PdfViewer component of Agenzia Impresa Eccobook 2.81.1 allows attackers to execute arbitrary web scripts or HTML
CVE-2023-41522	Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabilities in createStudents.php via the Id, firstname, and admis
CVE-2025-53131	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code over a network.
CVE-2023-41521	Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabilities in createSessionTerm.php via the id, termId, and sess
CVE-	

2025-8418	The B Slider- Gutenberg Slider Block for WP plugin for WordPress is vulnerable to Arbitrary Plugin Installation in all versions up to, and including, 1.1.30. This is due subscriber-level access and above, to install arbitrary plugins on the server which can make remote code execution possible.
CVE-2023-41531	Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in func3.php via the username1 and password2 parameters.
CVE-2023-41532	Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the doctor_contact parameter in doctorsearch.php.
CVE-2025-24325	Improper input validation in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user to potentiall
CVE-2025-8810	A vulnerability classified as critical was found in Tenda AC20 16.03.08.05. Affected by this vulnerability is the function strcpy of the file /goform/SetFirewallCfg. The exploit has been disclosed to the public and may be used.
CVE-2025-53727	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a networ
CVE-2025-46387	CWE-639 Authorization Bypass Through User-Controlled Key
CVE-2025-46386	CWE-639 Authorization Bypass Through User-Controlled Key
CVE-2025-42951	Due to broken authorization, SAP Business One (SLD) allows an authenticated attacker to gain administrator privileges of a database by invoking the corresponding
CVE-2023-41523	Student Attendance Management System v1 was discovered to contain a SQL injection vulnerability via the emailAddress parameter at createClassTeacher.php.
CVE-2025-54627	Out-of-bounds write vulnerability in the skia module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2025-8833	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This issue affects the function langSwitchBack of overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosur
CVE-2025-55158	Vim is an open source, command line text editor. In versions from 9.1.1231 to before 9.1.1406, when processing nested tuples during Vim9 script import operation the clear_tv() function may attempt to free memory that has already been deallocated, due to improper lifetime handling in the handle_import / ex_import code pa issue has been patched in version 9.1.1406.
CVE-2025-8748	MiR software versions prior to version 3.0.0 are affected by a command injection vulnerability. A malicious HTTP request crafted by an authenticated user could all
CVE-2025-55157	Vim is an open source, command line text editor. In versions from 9.1.1231 to before 9.1.1400, When processing nested tuples in Vim script, an error during evalua may access already freed memory due to improper lifetime handling, leading to memory corruption. The exploit requires direct user interaction, as the script must
CVE-2023-41520	Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabilities in createClassArms.php via the classId and classArmN
CVE-2025-50163	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.
CVE-2025-8832	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This vulnerability affects the function setDMZ o attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not re
CVE-2020-9322	The /users endpoint in Statamic Core before 2.11.8 allows XSS to add an administrator user. This can be exploited via CSRF. Stored XSS can occur via a JavaScript
CVE-2023-41524	Student Attendance Management System v1 was discovered to contain a SQL injection vulnerability via the username parameter at index.php.
CVE-2025-49557	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerab scripts may be used to escalate privileges within the application or compromise sensitive user data. Exploitation of this issue requires user interaction in that a vict
CVE-2025-51055	Insecure Data Storage of credentials has been found in /api_vedo/configuration/config.yml file in Vedo Suite version 2024.17. This file contains clear-text credential
CVE-	Stirling-PDF is a locally hosted web application that performs various operations on PDF files. Prior to version 1.1.0, when using the /api/v1/convert/markdown/pdf e

2025-55161	security sanitization which can be bypassed and result in SSRF. This issue has been patched in version 1.1.0.
CVE-2025-40920	Catalyst::Authentication::Credential::HTTP versions 1.018 and earlier for Perl generate nonces using the Perl Data::UUID library. * Data::UUID does not use a strong and are unsuitable for security, as per RFC 9562. * The nonces should be generated from a strong cryptographic source, as per RFC 7616.
CVE-2025-25235	Server-Side Request Forgery (SSRF) in Omnissa Secure Email Gateway (SEG) in SEG prior to 2.32 running on Windows and SEG prior to 2503 running on UAG allows
CVE-2025-55150	Stirling-PDF is a locally hosted web application that performs various operations on PDF files. Prior to version 1.1.0, when using the /api/v1/convert/html/pdf endpoi sanitization which can be bypassed and result in SSRF. This issue has been patched in version 1.1.0.
CVE-2025-55151	Stirling-PDF is a locally hosted web application that performs various operations on PDF files. Prior to version 1.1.0, the "convert file to pdf" functionality (/api/v1/co process. This issue has been patched in version 1.1.0.
CVE-2025-54878	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications betwee NASA CryptoLib version 1.4.0 and prior in the IV setup logic for telecommand frames. The problem arises from missing bounds checks when copying the Initializati one byte past the end of the heap buffer, leading to heap corruption and undefined behaviour. An attacker supplying a malformed telecommand frame can corrupt severe exploitation. This issue has been patched in version 1.4.0.
CVE-2025-53740	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.
CVE-2025-27128	in OpenHarmony v5.0.3 and prior versions allow a local attacker arbitrary code execution in tcb through use after free.
CVE-2025-53784	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.
CVE-2025-24298	in OpenHarmony v5.0.3 and prior versions allow a local attacker arbitrary code execution in tcb through use after free.
CVE-2025-25278	in OpenHarmony v5.0.3 and prior versions allow a local attacker arbitrary code execution in tcb through race condition.
CVE-2025-27577	in OpenHarmony v5.0.3 and prior versions allow a local attacker arbitrary code execution in tcb through race condition.
CVE-2025-54886	skops is a Python library which helps users share and ship their scikit-learn based models. In versions 0.12.0 and below, the Card.get_model does not contain any l When loading .skops models, it uses skops' secure loading with trusted type validation, raising errors for untrusted types unless explicitly allowed. However, when arbitrary code execution during loading, bypassing security measures and potentially enabling malicious code execution. This issue is fixed in version 0.13.0.
CVE-2025-53731	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.
CVE-2025-54653	Path traversal vulnerability in the virtualization file module. Successful exploitation of this vulnerability may affect the confidentiality of the virtualization file modul
CVE-2025-54652	Path traversal vulnerability in the virtualization base module. Successful exploitation of this vulnerability may affect the confidentiality of the virtualization module.
CVE-2025-53733	Incorrect conversion between numeric types in Microsoft Office Word allows an unauthorized attacker to execute code locally.
CVE-2025-6633	A maliciously crafted RBG file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnera
CVE-2025-54622	Binding authentication bypass vulnerability in the devicemanager module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2025-40743	A vulnerability has been identified in SINUMERIK 828D PPU.4 (All versions < V4.95 SP5), SINUMERIK 828D PPU.5 (All versions < V5.25 SP1), SINUMERIK 840D sl (All SINUMERIK ONE (All versions < V6.25 SP1), SINUMERIK ONE V6.15 (All versions < V6.15 SP5). The affected application improperly validates authentication for its V unauthorized remote access and potentially compromise system confidentiality, integrity, or availability.
CVE-2025-20093	Improper check for unusual or exceptional conditions in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an auth
CVE-2024-	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), SIMATIC PCS neo V6.0 (All versions), SIMATIC S7-PLC versions < V19 Update 4), SIMATIC STEP 7 V20 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V18 (All versions), SIMATIC WinCC V19 (All versions SIMOCODE ES V19 (All versions), SIMOCODE ES V20 (All versions), SIMOTION SCOUT TIA V5.4 (All versions), SIMOTION SCOUT TIA V5.5 (All versions), SIMOTION SC versions), SINAMICS Startdrive V18 (All versions), SINAMICS Startdrive V19 (All versions), SINAMICS Startdrive V20 (All versions), SIRIUS Safety ES V17 (TIA Portal) (Safety ES V20 (TIA Portal) (All versions), SIRIUS Soft Starter ES V17 (TIA Portal) (All versions), SIRIUS Soft Starter ES V18 (TIA Portal) (All versions), SIRIUS Soft Start

54678	versions), TIA Portal Cloud V18 (All versions), TIA Portal Cloud V19 (All versions < V5.2.1.1), TIA Portal Cloud V20 (All versions), TIA Portal Test Suite V20 (All versio Pipe accessible to all local users. This could allow an authenticated local attacker to cause a type confusion and execute arbitrary code within the affected applicat
CVE-2025-51056	An unrestricted file upload vulnerability in Vedo Suite version 2024.17 allows remote authenticated attackers to write to arbitrary filesystem paths by exploiting the execution (RCE).
CVE-2025-55165	Autocaliweb is a web app that offers an interface for browsing, reading, and downloading eBooks using a valid Calibre database. Prior to version 0.8.3, the debug p to_dict() method, used to serialize configuration for the debug pack, doesn't adequately filter out sensitive fields such as API tokens. Users, unaware of the full cont 0.8.3.
CVE-2025-53787	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability
CVE-2025-42976	SAP NetWeaver Application Server ABAP (BIC Document) allows an authenticated attacker to craft a request that, when submitted to a BIC Document application, c Multiple submissions can make the target completely unavailable. A similarly crafted submission can be used to perform an out-of-bounds read operation as well, r
CVE-2025-46414	The affected product does not limit the number of attempts for inputting the correct PIN for a registered product, which may allow an attacker to gain unauthorized the correct PIN is entered. This vulnerability was patched in a server-side update on April 6, 2025.
CVE-2025-3354	IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 20 is vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote attack
CVE-2024-26009	An authentication bypass using an alternate path or channel [CWE-288] vulnerability in Fortinet FortiOS version 6.4.0 through 6.4.15 and before 6.2.16, FortiProxy unauthenticated attacker to seize control of a managed device via crafted FGFM requests, if the device is managed by a FortiManager, and if the attacker knows th
CVE-2025-23319	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause an out-of-bounds write by sen tampering, or information disclosure.
CVE-2025-3831	Log files uploaded during troubleshooting by the Harmony SASE agent may have been accessible to unauthorized parties.
CVE-2025-49555	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnera actions on a web application where the victim is authenticated, potentially allowing unauthorized access or modification of sensitive data. Exploitation of this issue
CVE-2025-23318	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause an out-of-bounds write. A succ disclosure.
CVE-2025-52970	A improper handling of parameters in Fortinet FortiWeb versions 7.6.3 and below, versions 7.4.7 and below, versions 7.2.10 and below, and 7.0.10 and below may admin privileges on the device via a specially crafted request.
CVE-2025-3320	IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 20 is vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote attack
CVE-2025-50286	A Remote Code Execution (RCE) vulnerability in Grav CMS v1.7.48 allows an authenticated admin to upload a malicious plugin via the /admin/tools/direct-install int reverse shell access.
CVE-2025-8420	The Request a Quote Form plugin for WordPress is vulnerable to Remote Code Execution in version less than, or equal to, 2.5.2 via the emd_form_builder_lite_page it possible for unauthenticated attackers to execute code on the server, however, parameters can not be passed to the functions called.
CVE-2025-47219	In GStreamer through 1.26.1, the isomp4 plugin's qtdemux_parse_trak function may read past the end of a heap buffer while parsing an MP4 file, possibly leading t
CVE-2025-5391	The WooCommerce Purchase Orders plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_file() function in and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).
CVE-2025-54655	Race condition vulnerability in the virtualization base module. Successful exploitation of this vulnerability may affect the confidentiality and integrity of the virtualiz
CVE-2025-50177	Use after free in Windows Message Queuing allows an unauthorized attacker to execute code over a network.
CVE-2025-50160	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.
CVE-2025-50164	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.

CVE-2025-53132	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to elevate p
CVE-2025-50162	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.
CVE-2025-53786	On April 18th 2025, Microsoft announced Exchange Server Security Changes for Hybrid Deployments and accompanying non-security Hot Fix. Microsoft made thes investigation, Microsoft identified specific security implications tied to the guidance and configuration steps outlined in the April announcement. Microsoft is issuing announcement. Microsoft strongly recommends reading the information, installing the April 2025 (or later) Hot Fix and implementing the changes in your Exchange
CVE-2025-53720	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.
CVE-2025-54634	Vulnerability of improper processing of abnormal conditions in huge page separation. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54063	Cherry Studio is a desktop client that supports for multiple LLM providers. From versions 1.4.8 to 1.5.0, there is a one-click remote code execution vulnerability thr crafted URL on any website. If a victim clicks the exploit link in their browser, the app's custom URL handler is triggered, leading to remote code execution on the v
CVE-2025-49707	Improper access control in Azure Virtual Machines allows an authorized attacker to perform spoofing locally.
CVE-2025-22889	Improper handling of overlap between protected memory ranges for some Intel(R) Xeon(R) 6 processor with Intel(R) TDX may allow a privileged user to potentially
CVE-2025-54187	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of
CVE-2025-27069	Memory corruption while processing DDI command calls.
CVE-2025-27075	Memory corruption while processing IOCTL command with larger buffer in Bluetooth Host.
CVE-2025-27076	Memory corruption while processing simultaneous requests via escape path.
CVE-2025-53723	Numeric truncation error in Windows Hyper-V allows an authorized attacker to elevate privileges locally.
CVE-2025-53724	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.
CVE-2025-27068	Memory corruption while processing an IOCTL command with an arbitrary address.
CVE-2025-53725	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.
CVE-2025-53726	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.
CVE-2025-49572	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context c
CVE-2025-53729	Improper access control in Azure File Sync allows an authorized attacker to elevate privileges locally.
CVE-2025-53730	Use after free in Microsoft Office Visio allows an unauthorized attacker to execute code locally.
CVE-2025-50675	GPMAW 14, a bioinformatics software, has a critical vulnerability related to insecure file permissions in its installation directory. The directory is accessible with full including executable files like GPMAW3.exe, Fragment.exe, and the uninstaller GPsetup64_17028.exe. An attacker with user-level access can exploit this misconfig itself runs in the user's context, the uninstaller is typically executed with administrative privileges when an administrator attempts to uninstall the software. By exp resulting in privilege escalation.
CVE-2025-49560	Substance3D - Viewer versions 0.25 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the conte

CVE-2025-53789	Missing authentication for critical function in Windows StateRepository API allows an authorized attacker to elevate privileges locally.
CVE-2025-49569	Substance3D - Viewer versions 0.25 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of th
CVE-2025-49561	Animate versions 23.0.12, 24.0.9 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current
CVE-2025-49570	Photoshop Desktop versions 25.12.3, 26.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the conte
CVE-2025-49571	Substance3D - Modeler versions 1.22.0 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution i programs, an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue
CVE-2025-6634	A maliciously crafted TGA file, when linked or imported into Autodesk 3ds Max, can force a Memory Corruption vulnerability. A malicious actor can leverage this vul
CVE-2025-53773	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio allows an unauthorized attacker to execu
CVE-2025-53761	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.
CVE-2025-53759	Use of uninitialized resource in Microsoft Office Excel allows an unauthorized attacker to execute code locally.
CVE-2025-53741	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.
CVE-2025-53739	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.
CVE-2025-53738	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.
CVE-2025-53737	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.
CVE-2025-38747	Dell SupportAssist OS Recovery, versions prior to 5.5.14.0, contain a Creation of Temporary File With Insecure Permissions vulnerability. A local authenticated attac
CVE-2025-53735	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.
CVE-2025-27062	Memory corruption while handling client exceptions, allowing unauthorized channel access.
CVE-2025-53734	Use after free in Microsoft Office Visio allows an unauthorized attacker to execute code locally.
CVE-2025-49573	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context c
CVE-2025-53732	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.
CVE-2025-27067	Memory corruption while processing DDI call with invalid buffer.
CVE-2025-21461	Memory corruption when programming registers through virtual CDM.
CVE-2025-54221	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the curre
CVE-	

2025-54223	InCopy versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current use
CVE-2025-54211	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the co
CVE-2025-22836	Integer overflow or wraparound in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user to pot
CVE-2025-54212	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the co
CVE-2025-54213	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context o
CVE-2025-54215	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the curre
CVE-2025-20109	Improper Isolation or Compartmentalization in the stream cache mechanism for some Intel(R) Processors may allow an authenticated user to potentially enable esc
CVE-2025-20074	Time-of-check Time-of-use race condition for some Intel(R) Connectivity Performance Suite software installers before version 40.24.11210 may allow an authentica
CVE-2025-54216	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the curre
CVE-2025-54217	InCopy versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of th
CVE-2025-53149	Heap-based buffer overflow in Kernel Streaming WOW Thunk Service Driver allows an authorized attacker to elevate privileges locally.
CVE-2025-54218	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the curre
CVE-2025-54219	InCopy versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of th
CVE-2025-54220	InCopy versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of th
CVE-2025-40767	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application runs docker containers without a accessing sensitive host system resources.
CVE-2025-40764	A vulnerability has been identified in Simcenter Femap V2406 (All versions < V2406.0003), Simcenter Femap V2412 (All versions < V2412.0002). The affected app attacker to execute code in the context of the current process.
CVE-2025-54210	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context o
CVE-2025-22893	Insufficient control flow management in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user
CVE-2025-53133	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.
CVE-2025-49563	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the c
CVE-2025-54207	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in th file.
CVE-2025-54206	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context o
CVE-	

2025-54209	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the co
CVE-2025-53141	Null pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.
CVE-2025-54229	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of
CVE-2025-49564	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context
CVE-2025-25273	Insufficient control flow management in the Linux kernel-mode driver for some Intel(R) 700 Series Ethernet before version 2.28.5 may allow an authenticated user
CVE-2025-54232	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of
CVE-2025-24486	Improper input validation in the Linux kernel-mode driver for some Intel(R) 700 Series Ethernet before version 2.28.5 may allow an authenticated user to potentiall
CVE-2025-21474	Memory corruption while processing commands from A2dp sink command queue.
CVE-2025-54230	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of
CVE-2025-54231	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of
CVE-2025-24484	Improper input validation in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user to potentiall
CVE-2025-24303	Improper check for unusual or exceptional conditions in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an autl
CVE-2025-40762	A vulnerability has been identified in Simcenter Femap V2406 (All versions < V2406.0003), Simcenter Femap V2412 (All versions < V2412.0002). The affected app attacker to execute code in the context of the current process.(ZDI-CAN-26692)
CVE-2025-54208	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context c
CVE-2025-53155	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to elevate privileges locally.
CVE-2025-21455	Memory corruption while submitting blob data to kernel space though IOCTL.
CVE-2025-50155	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.
CVE-2025-21456	Memory corruption while processing IOCTL command when multiple threads are called to map/unmap buffer concurrently.
CVE-2025-49761	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.
CVE-2025-53154	Null pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.
CVE-2025-54222	Substance3D - Stager versions 3.1.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of t
CVE-2025-41686	A low-privileged local attacker can exploit improper permissions on nssm.exe to escalate their privileges and gain administrative access.
CVE-2025-	Use after free in Desktop Windows Manager allows an authorized attacker to execute code locally.

53152	
CVE-2025-53151	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.
CVE-2025-50176	Access of resource using incompatible type ('type confusion') in Graphics Kernel allows an authorized attacker to execute code locally.
CVE-2025-21458	Memory corruption when IOCTL interface is called to map and unmap buffers simultaneously.
CVE-2025-30033	The affected setup component is vulnerable to DLL hijacking. This could allow an attacker to execute arbitrary code when a legitimate user installs an application t
CVE-2025-40759	A vulnerability has been identified in SIMATIC S7-PLCSIM V17 (All versions), SIMATIC STEP 7 V17 (All versions), SIMATIC STEP 7 V18 (All versions), SIMATIC STEP 7 V V18 (All versions), SIMATIC WinCC V19 (All versions < V19 Update 4), SIMATIC WinCC V20 (All versions), SIMOCODE ES V17 (All versions), SIMOCODE ES V18 (All ve SIMOTION SCOUT TIA V5.5 (All versions), SIMOTION SCOUT TIA V5.6 (All versions < V5.6 SP1 HF7), SIMOTION SCOUT TIA V5.7 (All versions), SINAMICS Startdrive V1 (All versions), SIRIUS Safety ES V17 (TIA Portal) (All versions), SIRIUS Safety ES V18 (TIA Portal) (All versions), SIRIUS Safety ES V19 (TIA Portal) (All versions), SIRIU V18 (TIA Portal) (All versions), SIRIUS Soft Starter ES V19 (TIA Portal) (All versions), SIRIUS Soft Starter ES V20 (TIA Portal) (All versions), TIA Portal Cloud V17 (All ve versions). Affected products do not properly sanitize stored security properties when parsing project files. This could allow an attacker to cause a type confusion ar
CVE-2025-50168	Access of resource using incompatible type ('type confusion') in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.
CVE-2025-21473	Memory corruption when using Virtual cdm (Camera Data Mover) to write registers.
CVE-2025-50170	Improper handling of insufficient permissions or privileges in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.
CVE-2025-54226	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the c
CVE-2025-50173	Weak authentication in Windows Installer allows an authorized attacker to elevate privileges locally.
CVE-2025-54225	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the c
CVE-2025-54224	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the c
CVE-2025-50153	Use after free in Desktop Windows Manager allows an authorized attacker to elevate privileges locally.
CVE-2025-53191	Missing Authentication for Critical Function vulnerability in ABB Aspect.This issue affects Aspect: before <3.08.04-s01.
CVE-2025-53781	Exposure of sensitive information to an unauthorized actor in Azure Virtual Machines allows an authorized attacker to disclose information over a network.
CVE-2025-54607	Authentication management vulnerability in the ArkWeb module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2025-40761	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions), RUGGEDCOM ROX MX5000RE (All versions), RUGGEDCOM ROX RX1400 (All versions versions), RUGGEDCOM ROX RX1511 (All versions), RUGGEDCOM ROX RX1512 (All versions), RUGGEDCOM ROX RX1524 (All versions), RUGGEDCOM ROX RX1536 (Self-Test (BIST) mode. This could allow an attacker with physical access to the serial interface to bypass authentication and get access to a root shell on the device
CVE-2025-51624	Cross-site scripting (XSS) vulnerability in Zone Bitaqati thru 3.4.0.
CVE-2025-8355	In Xerox FreeFlow Core version 8.0.4, improper handling of XML input allows injection of external entities. An attacker can craft malicious XML containing reference
CVE-2025-50154	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.
CVE-2025-47908	Middleware causes a prohibitive amount of heap allocations when processing malicious preflight requests that include a Access-Control-Request-Headers (ACRH) h middleware/server as an attempt to cause a denial of service.

CVE-2025-7036	The CleverReach® WP plugin for WordPress is vulnerable to time-based SQL Injection via the ‘title’ parameter in all versions up to, and including, 1.5.20 due to ins makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information fro
CVE-2025-55171	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Prior to version 3.4.8, the application does not check a Image files at endpoint /html/personalizacao_remover.php by defining imagem_0 as image id to delete. This issue has been patched in version 3.4.8.
CVE-2025-49556	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by an Incorrect Authorization vulnerability that gain unauthorized read access. Exploitation of this issue does not require user interaction, and scope is unchanged.
CVE-2025-53793	Improper authentication in Azure Stack allows an unauthorized attacker to disclose information over a network.
CVE-2025-50169	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB allows an unauthorized attacker to execute code ove
CVE-2025-46709	Possible memory leak or kernel exceptions caused by reading kernel heap data after free or NULL pointer dereference kernel exception.
CVE-2025-49554	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by an Improper Input Validation vulnerability th input, causing the application to crash or become unresponsive. Exploitation of this issue does not require user interaction.
CVE-2025-48807	Improper restriction of communication channel to intended endpoints in Windows Hyper-V allows an authorized attacker to execute code locally.
CVE-2025-53783	Heap-based buffer overflow in Microsoft Teams allows an unauthorized attacker to execute code over a network.
CVE-2025-21477	Transient DOS while processing CCCH data when NW sends data with invalid length.
CVE-2025-51532	Incorrect access control in Sage DPW 2024_12_004 and earlier allows unauthorized attackers to access the built-in Database Monitor via a crafted request. The ver
CVE-2025-33051	Exposure of sensitive information to an unauthorized actor in Microsoft Exchange Server allows an unauthorized attacker to disclose information over a network.
CVE-2025-21452	Transient DOS while processing a random-access response (RAR) with an invalid PDU length on LTE network.
CVE-2025-23320	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause the shared memory limit to be
CVE-2024-52504	A vulnerability has been identified in SIPROTEC 4 6MD61 (All versions), SIPROTEC 4 6MD63 (All versions), SIPROTEC 4 6MD66 (All versions), SIPROTEC 4 6MD665 (A V4.78), SIPROTEC 4 7SD610 (All versions < V4.78), SIPROTEC 4 7SJ61 (All versions), SIPROTEC 4 7SJ62 (All versions), SIPROTEC 4 7SJ63 (All versions), SIPROTEC 4 SIPROTEC 4 7UM61 (All versions), SIPROTEC 4 7UM62 (All versions), SIPROTEC 4 7UT612 (All versions), SIPROTEC 4 7UT613 (All versions), SIPROTEC 4 7UT63 (All v 4 Compact 7RW80 (All versions), SIPROTEC 4 Compact 7SD80 (All versions), SIPROTEC 4 Compact 7SJ80 (All versions), SIPROTEC 4 Compact 7SJ81 (All versions), S handle interrupted operations of file transfer. This could allow an unauthenticated remote attacker to cause a denial of service condition. To restore normal operati
CVE-2025-46390	CWE-204: Observable Response Discrepancy
CVE-2025-47444	Insertion of Sensitive Information Into Sent Data vulnerability in Liquid Web GiveWP allows Retrieve Embedded Sensitive Data.This issue affects GiveWP: from n/a b
CVE-2025-6253	The UiCore Elements – Free Elementor widgets and templates plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 1.3.0 via This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.
CVE-2025-54525	Mattermost Confluence Plugin version <1.5.0 fails to handle unexpected request body which allows attackers to crash the plugin via constant hit to create channel
CVE-2025-47324	Information disclosure while accessing and modifying the PIB file of a remote device via powerline.
CVE-2025-23322	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where multiple requests could cause a double free when a stream is cancelled before
CVE-2025-	Transient DOS while creating NDP instance.

27073	
CVE-2025-53722	Uncontrolled resource consumption in Windows Remote Desktop Services allows an unauthorized attacker to deny service over a network.
CVE-2025-52931	Mattermost Confluence Plugin version <1.5.0 fails to handle unexpected request body which allows attackers to crash the plugin via constant hit to update channe
CVE-2025-25231	Omnissa Workspace ONE UEM contains a Secondary Context Path Traversal Vulnerability. A malicious actor may be able to gain access to sensitive information by
CVE-2025-27066	Transient DOS while processing an ANQP message.
CVE-2025-27065	Transient DOS while processing a frame with malformed shared-key descriptor.
CVE-2025-46659	An issue was discovered in ExonautWeb in 4C Strategies Exonaut 21.6. Information disclosure can occur via an external HTTPS request.
CVE-2025-23321	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where a user could cause a divide by zero issue by issuing an invalid request. A succ
CVE-2025-23323	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where a user could cause an integer overflow or wraparound, leading to a segmentat
CVE-2025-23324	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where a user could cause an integer overflow or wraparound, leading to a segmentat
CVE-2025-22839	Insufficient granularity of access control in the OOB-MSM for some Intel(R) Xeon(R) 6 Scalable processors may allow a privileged user to potentially enable escalati
CVE-2025-21086	Improper input validation in the Linux kernel-mode driver for some Intel(R) 700 Series Ethernet before version 2.28.5 may allow an authenticated user to potentiall
CVE-2025-51040	Electrolink FM/DAB/TV Transmitter Web Management System Unauthorized access vulnerability via the /FrameSetCore.html endpoint in Electrolink 500W, 1kW, 2kV
CVE-2025-5462	A heap-based buffer overflow in Ivanti Connect Secure before 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 22.8R2.3-723 a attacker to trigger a denial of service.
CVE-2025-5456	A buffer over-read vulnerability in Ivanti Connect Secure before 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 2.8R2.3-723 a attacker to trigger a denial of service. CWE-125
CVE-2025-35970	On multiple products of SEIKO EPSON and FUJIFILM Corporation, the initial administrator password is easy to guess from the information available via SNMP. If the a with the administrator privilege.
CVE-2025-23331	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where a user could cause a memory allocation with excessive size value, leading to a service.
CVE-2025-23327	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause an integer overflow through specially crafted inputs. A
CVE-2025-23326	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause an integer overflow through a specially crafted input.
CVE-2025-23325	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause uncontrolled recursion through a specially crafted inp
CVE-2025-7679	Missing Authentication for Critical Function vulnerability in ABB Aspect.This issue affects Aspect: All versions.
CVE-2025-40769	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application uses a Content Security Policy t leading to cross-site scripting attacks.
CVE-2025-	LinkJoin through 882f196 mishandles lacks type checking in password reset.

55137	
CVE-2025-55138	LinkJoin through 882f196 mishandles token ownership in password reset.
CVE-2025-20625	Improper conditions check for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.110.0.5 may allow an unauthenticated user to potentiall
CVE-2025-22840	Sequence of processor instructions leads to unexpected behavior for some Intel(R) Xeon(R) 6 Scalable processors may allow an authenticated user to potentially en
CVE-2025-55077	Tyler Technologies ERP Pro 9 SaaS allows an authenticated user to escape the application and execute limited operating system commands within the remote Micr Windows environment settings to all ERP Pro 9 SaaS customer environments as of 2025-08-01.
CVE-2025-40770	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions). The affected application uses a monitoring interface that is not c middle attacks.
CVE-2025-8773	A vulnerability, which was classified as critical, was found in Dinstar Monitoring Platform 甘肃省危险品库监控平台 1.0. Affected is an unknown function of the file /itc/$ sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this
CVE-2025-50161	Heap-based buffer overflow in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.
CVE-2025-50159	Use after free in Remote Access Point-to-Point Protocol (PPP) EAP-TLS allows an authorized attacker to elevate privileges locally.
CVE-2025-8393	A TLS vulnerability exists in the phone application used to manage a connected device. The phone application accepts self-signed certificates when establishing TL include user credentials and sensitive session tokens.
CVE-2025-8752	A vulnerability was found in wangzhixuan spring-shiro-training up to 94812c1fd8f7fe796c931f4984ff1aa0671ab562. It has been declared as critical. This vulnerabil remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version det
CVE-2025-8798	A vulnerability was found in oitcode samarium up to 0.9.6. It has been classified as critical. Affected is an unknown function of the file /dashboard/product of the co remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8809	A vulnerability classified as critical has been found in code-projects Online Medicine Guide 1.0. Affected is an unknown function of the file /addelidetails.php. The m disclosed to the public and may be used.
CVE-2025-23241	Integer overflow or wraparound in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user to pot
CVE-2025-8815	A vulnerability was found in 猫宁i Morning up to bc782730c74ff080494f145cc363a0b4f43f7d3e. It has been classified as critical. Affected is an unknown function of the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore,
CVE-2025-40768	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application exposes an internal service port
CVE-2025-8838	A vulnerability has been found in WinterChenS my-site up to 1f7525f15934d9d6a278de967f6ec9f1757738d8. This vulnerability affects the function preHandle of th authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still do for affected nor updated releases are available. The code maintainer responded to the issue that "[he] tried it, and using this link automatically redirects to the logi
CVE-2025-8811	A vulnerability, which was classified as critical, has been found in code-projects Simple Art Gallery 1.0. Affected by this issue is some unknown functionality of the f remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8744	A vulnerability classified as critical was found in CesiumLab Web up to 4.0. This vulnerability affects unknown code of the file /lodmodels/. The manipulation of the may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-27071	Memory corruption while processing specific files in Powerline Communication Firmware.
CVE-2025-54606	Status verification vulnerability in the lock screen module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.
CVE-2025-54611	EXTRA_REFERRER resource read vulnerability in the Gallery module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2025-	Relative path traversal in Windows Kerberos allows an authorized attacker to elevate privileges over a network.

53779	
CVE-2025-8297	Incomplete restriction of configuration in Ivanti Avalanche before version 6.4.8.8008 allows a remote authenticated attacker with admin privileges to achieve remo
CVE-2025-8296	SQL injection in Ivanti Avalanche before version 6.4.8.8008 allows a remote authenticated attacker with admin privileges to execute arbitrary SQL queries. In certa
CVE-2025-24305	Insufficient control flow management in the Alias Checking Trusted Module (ACTM) firmware for some Intel(R) Xeon(R) processors may allow a privileged user to pc
CVE-2025-54478	Mattermost Confluence Plugin version <1.5.0 fails to enforce authentication of the user to the Mattermost instance which allows unauthenticated attackers to edit
CVE-2025-44004	Mattermost Confluence Plugin version <1.5.0 fails to check the authorization of the user to the Mattermost instance which allows attackers to create a channel sub
CVE-2025-26403	Out-of-bounds write in the memory subsystem for some Intel(R) Xeon(R) 6 processors when using Intel(R) SGX or Intel(R) TDX may allow a privileged user to poten
CVE-2025-53744	An incorrect privilege assignment vulnerability [CWE-266] in FortiOS Security Fabric version 7.6.0 through 7.6.2, 7.4.0 through 7.4.7, 7.2 all versions, 7.0 all versior admin via registering the device to a malicious FortiManager.
CVE-2025-20053	Improper buffer restrictions for some Intel(R) Xeon(R) Processor firmware with SGX enabled may allow a privileged user to potentially enable escalation of privilege
CVE-2025-32086	Improperly implemented security check for standard in the DDRIO configuration for some Intel(R) Xeon(R) 6 Processors when using Intel(R) SGX or Intel(R) TDX ma
CVE-2025-20037	Time-of-check time-of-use race condition in firmware for some Intel(R) Converged Security and Management Engine may allow a privileged user to potentially enab
CVE-2025-49813	An improper neutralization of special elements used in an OS Command ("OS Command Injection") vulnerability [CWE-78] in Fortinet FortiADC version 7.2.0 and be crafted HTTP parameters.
CVE-2025-54996	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys. In versions 2.3.1 and below, directly to the root policy. While the identity system allowed adding arbitrary policies, which in turn could contain capability grants on arbitrary paths, the root polic from child namespaces. This issue is fixed in version 2.3.2. To workaround this vulnerability, use of denied_parameters in any policy which has access to the affecte
CVE-2025-50465	OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the TestDefinitionDAO interfac
CVE-2025-55009	The AuthKit library for Remix provides convenient helpers for authentication and session management using WorkOS & AuthKit with Remix. In versions 0.14.1 and accessToken — by returning them from the authkitLoader. This caused them to be rendered into the browser HTML.
CVE-2025-55008	The AuthKit library for React Router 7+ provides helpers for authentication and session management using WorkOS & AuthKit with React Router. In versions 0.6.1 a accessToken by returning them from the authkitLoader. This caused them to be rendered into the browser HTML. This issue is fixed in version 0.7.0.
CVE-2025-53760	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.
CVE-2025-36119	IBM i 7.3, 7.4, 7.5, and 7.6 is affected by an authenticated user obtaining elevated privileges with IBM Digital Certificate Manager for i (DCM) due to a web session l actions in DCM as an administrator.
CVE-2024-41979	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S functionality level at server side. This could allow an authenticated attacker to gain complete access of the application.
CVE-2025-54882	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. In versions 0.8.0 through 0.9.21 and 1.0.0-beta through 1.1.0, Himmelblau stores th received credentials are stored as world readable. This is fixed in versions 0.9.22 and 1.2.0. To work around this issue, remove all read access to Himmelblau cache
CVE-2025-50466	OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the TestDefinitionDAO interfac
CVE-2025-53134	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized
CVE-2025-	The installer for SAN Host Utilities for Windows versions prior to 8.0 is susceptible to a vulnerability which when successfully exploited could allow a local user to es

26513	
CVE-2025-53188	Insufficiently Protected Credentials vulnerability in ABB Aspect.This issue affects Aspect: before <3.08.04-s01.
CVE-2025-53135	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows DirectX allows an authorized attacker to elevate privileges
CVE-2025-53189	Authorization Bypass Through User-Controlled Key vulnerability in ABB Aspect.This issue affects Aspect: from o before <3.08.04-s01.
CVE-2025-53147	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.
CVE-2025-53142	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.
CVE-2025-53190	A vulnerability in ABB Aspect.This issue affects Aspect: before <3.08.04-s01.
CVE-2025-53137	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.
CVE-2025-8757	A vulnerability was found in TRENDnet TV-IP110WN 1.2.2 and classified as problematic. Affected by this issue is some unknown functionality of the file /server/boa. required to approach this attack. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public a
CVE-2025-53788	Time-of-check time-of-use (toctou) race condition in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.
CVE-2025-50167	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privilege
CVE-2025-3770	EDK2 contains a vulnerability in BIOS where an attacker may cause “Protection Mechanism Failure” by local access. Successful exploitation of this vulnerability will
CVE-2025-53187	Improper Control of Generation of Code ('Code Injection') vulnerability in ABB ASPECT.This issue affects ASPECT: before <3.08.04-s01.
CVE-2025-45766	poco v1.14.1-release was discovered to contain weak encryption.
CVE-2025-53718	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.
CVE-2025-50158	Time-of-check time-of-use (toctou) race condition in Windows NTFS allows an unauthorized attacker to disclose information locally.
CVE-2025-53140	Use after free in Kernel Transaction Manager allows an authorized attacker to elevate privileges locally.
CVE-2025-49762	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized
CVE-2025-53721	Use after free in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.
CVE-2025-47907	Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpe expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.
CVE-2025-8758	A vulnerability was found in TRENDnet TEW-822DRE FW103B02. It has been classified as problematic. This affects an unknown part of the component vsftpd. The r high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure b
CVE-2025-42946	Due to directory traversal vulnerability in SAP S/4HANA (Bank Communication Management), an attacker with high privileges and access to a specific transaction a could allow the attacker to potentially read or delete these files hence causing a high impact on confidentiality and low impact on integrity. There is no impact on a
CVE-2025-	The MOD3 command traffic between the monitoring application and the inverter is transmitted in plaintext without encryption or obfuscation. This vulnerability ma read/write operations for voltage, current, and power configuration, operational status, alarms, telemetry, system reset, or inverter control commands, potentially

52586	
CVE-2025-53736	Buffer over-read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.
CVE-2024-48892	A relative path traversal vulnerability [CWE-23] in FortiSOAR 7.6.0, 7.5.0 through 7.5.1, 7.4 all versions, 7.3 all versions may allow an authenticated attacker to rea
CVE-2025-49751	Missing synchronization in Windows Hyper-V allows an authorized attacker to deny service over an adjacent network.
CVE-2025-54617	Stack-based buffer overflow vulnerability in the dms_fwk module. Impact: Successful exploitation of this vulnerability can cause RCE.
CVE-2025-54630	:Vulnerability of insufficient data length verification in the DFA module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54632	Vulnerability of insufficient data length verification in the HVB module. Impact: Successful exploitation of this vulnerability may affect service integrity.
CVE-2025-54625	Race condition vulnerability in the kernel file system module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-24923	Uncontrolled search path in some Intel(R) AI for Enterprise Retrieval-augmented Generation software may allow an authenticated user to potentially enable escalat
CVE-2025-20087	Incorrect default permissions for some Intel(R) oneAPI DPC++/C++ Compiler software installers may allow an authenticated user to potentially enable escalation o
CVE-2025-49743	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to ele
CVE-2025-54633	Out-of-bounds read vulnerability in the register configuration of the DMA module. Impact: Successful exploitation of this vulnerability may affect service confidentia
CVE-2025-26404	Uncontrolled search path for some Intel(R) DSA software before version 25.2.15.9 may allow an authenticated user to potentially enable escalation of privilege via
CVE-2025-54629	Race condition issue occurring in the physical page import process of the memory management module. Impact: Successful exploitation of this vulnerability may a
CVE-2025-30027	An ACAP configuration file lacked sufficient input validation, which could allow for arbitrary code execution. This vulnerability can only be exploited if the Axis devic malicious ACAP application.
CVE-2025-27717	Uncontrolled search path for some Intel(R) Graphics Driver software may allow an authenticated user to potentially enable escalation of privilege via local access
CVE-2025-24302	Uncontrolled recursion for some TinyCBOR libraries maintained by Intel(R) before version 0.6.1 may allow an authenticated user to potentially enable escalation of
CVE-2025-27559	Incorrect default permissions for some AI Playground software before version v2.3.0 alpha may allow an authenticated user to potentially enable escalation of privi
CVE-2025-54631	Vulnerability of insufficient data length verification in the partition module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-20092	Uncontrolled search path for some Clock Jitter Tool software before version 6.0.1 may allow an authenticated user to potentially enable escalation of privilege via l
CVE-2025-3892	ACAP applications can be executed with elevated privileges, potentially leading to privilege escalation. This vulnerability can only be exploited if the Axis device is malicious ACAP application.
CVE-2025-27759	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiWeb version 7.6.0 through execute unauthorized code or commands via crafted CLI commands
CVE-2025-	Uncontrolled search path for some Intel(R) oneAPI Toolkit and component software installers may allow an authenticated user to potentially enable escalation of pr

20017	
CVE-2025-54641	Issue of buffer overflow caused by insufficient data verification in the kernel acceleration module. Impact: Successful exploitation of this vulnerability may affect av
CVE-2025-20099	Improper access control for some Intel(R) Rapid Storage Technology installation software may allow an authenticated user to potentially enable escalation of privile
CVE-2025-20048	Uncontrolled search path for the Intel(R) Trace Analyzer and Collector software all verions may allow an authenticated user to potentially enable escalation of privil
CVE-2025-20627	Uncontrolled search path for some Intel(R) oneAPI DPC++/C++ Compiler software before version 2025.0.1 may allow an authenticated user to potentially enable e
CVE-2025-20023	Incorrect default permissions for some Intel(R) Graphics Driver software installers may allow an authenticated user to potentially enable escalation of privilege via
CVE-2025-47857	A improper neutralization of special elements used in an os command ('os command injection') vulnerability [CWE-78] in Fortinet FortiWeb CLI version 7.6.0 throug
CVE-2025-22838	Uncontrolled search path for some Intel(R) RealSense(TM) Dynamic Calibrator software before version 2.14.2.0 may allow an authenticated user to potentially enab
CVE-2025-26470	Incorrect default permissions for some Intel(R) Distribution for Python software installers before version 2025.1.0 may allow an authenticated user to potentially en
CVE-2025-54642	Issue of buffer overflow caused by insufficient data verification in the kernel gyroscope module. Impact: Successful exploitation of this vulnerability may affect avai
CVE-2025-21093	Uncontrolled search path element for some Intel(R) Driver & Support Assistant Tool software before version 24.6.49.8 may allow an authenticated user to pote
CVE-2025-47183	In GStreamer through 1.26.1, the isomp4 plugin's qtdemux_parse_tree function may read past the end of a heap buffer while parsing an MP4 file, leading to inform
CVE-2025-44779	An issue in Ollama v0.1.33 allows attackers to delete arbitrary files via sending a crafted packet to the endpoint /api/pull.
CVE-2023-45584	A double free vulnerability [CWE-415] in Fortinet FortiOS version 7.4.0, version 7.2.0 through 7.2.5 and before 7.0.12, FortiProxy version 7.4.0 through 7.4.1, versio attacker to execute code or commands via crafted HTTP or HTTPs requests.
CVE-2025-54643	Out-of-bounds array access issue due to insufficient data verification in the kernel ambient light module. Impact: Successful exploitation of this vulnerability may a
CVE-2025-54644	Out-of-bounds array access issue due to insufficient data verification in the kernel ambient light module. Impact: Successful exploitation of this vulnerability may a
CVE-2025-24921	Improper neutralization for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an unauthenticated user to pot
CVE-2025-50233	A vulnerability in QCMS version 6.0.5 allows authenticated users to read arbitrary files from the server due to insufficient validation of the "Name" parameter in the sensitive files outside the intended template directory, potentially exposing system configuration, PHP source code, or other sensitive information.
CVE-2025-51306	In Gatling Enterprise versions below 1.25.0, a user logging-out can still use his session token to continue using the application without expiration, due to incorrect s
CVE-2024-8244	The filepath.Walk and filepath.WalkDir functions are documented as not following symbolic links, but both functions are susceptible to a TOCTOU (time of check/tim progress.
CVE-2025-50234	MCCMS v2.7.0 has an SSRF vulnerability located in the index() method of the sys\apps\controllers\api\Gf.php file, where the pic parameter is processed. The pic pa (bD2voYwPpNuJ7B8), defined in the db.php file. The decrypted URL is passed to the geturl() method, which uses cURL to make a request to the URL without proper addresses or local file paths (such as http://127.0.0.1 or file:///). By using the file:// protocol, the attacker can access arbitrary files on the local file system (e.g., file: and more, leading to information leakage or system exposure. The danger of this SSRF vulnerability includes accessing internal services and local file systems thro escalation, or full system compromise, severely affecting the system's security and stability.
CVE-2024-55399	4C Strategies Exonaut before v21.6.2.1-1 was discovered to contain a Server-Side Request Forgery (SSRF).

CVE-2025-8419	A vulnerability was found in Keycloak-services. Special characters used during e-mail registration may perform SMTP Injection and unexpectedly send short unwant emails (subject and little data, the example is 60 chars). This flaw's only direct consequence is an unsolicited email being sent from the Keycloak server. However,
CVE-2025-6986	The FileBird – WordPress Media Library Folders & File Manager plugin for WordPress is vulnerable to SQL Injection via the 'search' parameter in all versions up to, a existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing
CVE-2024-55398	4C Strategies Exonaut before v22.4 was discovered to contain insecure permissions.
CVE-2025-46391	CWE-284: Improper Access Control
CVE-2025-50166	Integer overflow or wraparound in Windows Distributed Transaction Coordinator allows an authorized attacker to disclose information over a network.
CVE-2025-50172	Allocation of resources without limits or throttling in Windows DirectX allows an authorized attacker to deny service over a network.
CVE-2025-2028	Lack of TLS validation when downloading a CSV file including mapping from IPs to countries used ONLY for displaying country flags in logs
CVE-2025-51824	libcsp 2.0 is vulnerable to Buffer Overflow in the csp_usart_open() function at drivers/usart/zephyr.c.
CVE-2025-55170	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Prior to version 3.4.8, a reflected cross-site scripting (X allows attackers to inject malicious scripts in the verificacao and redir_config parameter. This issue has been patched in version 3.4.8.
CVE-2025-46389	CWE-620: Unverified Password Change
CVE-2025-6013	Vault and Vault Enterprise's ("Vault") ldap auth method may not have correctly enforced MFA if username_as_alias was set to true and a user had multiple CNs tha 1.19.8, 1.18.13, and 1.16.24.
CVE-2025-53728	Exposure of sensitive information to an unauthorized actor in Microsoft Dynamics 365 (on-premises) allows an unauthorized attacker to disclose information over a
CVE-2025-25005	Improper input validation in Microsoft Exchange Server allows an authorized attacker to perform tampering over a network.
CVE-2025-21465	Information disclosure while processing the hash segment in an MBN file.
CVE-2025-51823	libcsp 2.0 is vulnerable to Buffer Overflow in the csp_eth_init() function due to improper handling of the ifname parameter. The function uses strcpy to copy the int
CVE-2025-21464	Information disclosure while reading data from an image using specified offset and size parameters.
CVE-2025-24835	Protection mechanism failure in the Intel(R) Graphics Driver for the Intel(R) Arc(TM) B-Series graphics before version 32.0.101.6737 may allow an authenticated us
CVE-2025-24515	NULL pointer dereference for some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable denial of service via local access.
CVE-2025-53716	Null pointer dereference in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.
CVE-2025-24323	Improper access control in some firmware package and LED mode toggle tool for some Intel(R) PCIe Switch software before version MR4_1.0b1 may allow a privileg
CVE-2025-8310	Missing authorization in the admin console of Ivanti Virtual Application Delivery Controller before version 22.9 allows a remote authenticated attacker to take over
CVE-2025-21090	Missing reference to active allocated resource for some Intel(R) Xeon(R) processors may allow an authenticated user to potentially enable denial of service via loca
CVE-	

2025-55000	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys. In versions 0.1.0 through 2.3 unexpected normalization in the underlying TOTP library. To work around, ensure that all codes are first normalized before submitting to the OpenBao endpoint. TC
CVE-2025-55001	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys. In versions 2.3.1 and below, auth method. When the username_as_alias=true parameter in the LDAP auth method was in use, the caller-supplied username was used verbatim without normali around this, remove all usage of the username_as_alias=true parameter and update any entity aliases accordingly.
CVE-2024-42048	OpenOrange Business Framework 1.15.5 provides unprivileged users with write access to the installation directory.
CVE-2025-32932	An Improper neutralization of input during web page generation ('cross-site scripting') vulnerability [CWE-79] in FortiSOAR version 7.6.1 and below, version 7.5.1 a authenticated remote attacker to perform an XSS attack via stored malicious service requests
CVE-2023-40992	Hospital Management System 4 is vulnerable to a SQL injection in /Hospital-Management-System-master/func.php via the password2 parameter.
CVE-2025-50468	OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the DocStoreDAO interface. Th
CVE-2025-47188	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit through 6.4 SP4, could allow an unauthentic could allow an attacker to execute arbitrary commands within the context of the phone, leading to disclosure or modification of sensitive configuration data or affe
CVE-2025-53774	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability
CVE-2025-51058	Bottinelli Informatical Vedo Suite 2024.17 is vulnerable to Server-side Request Forgery (SSRF) in the /api_vedo/video/preview endpoint, which allows remote auther
CVE-2025-50952	openjpeg v 2.5.0 was discovered to contain a NULL pointer dereference via the component /openjp2/dwt.c.
CVE-2025-51054	Vedo Suite 2024.17 is vulnerable to Incorrect Access Control, which allows remote attackers to obtain a valid high privilege JWT token without prior authentication
CVE-2025-36023	IBM Cloud Pak for Business Automation 24.0.0 through 24.0.0 IF005 and 24.0.1 through 24.0.1 IF002 could allow an authenticated user to view sensitive user and s
CVE-2024-55401	An issue in 4C Strategies Exonaut before v22.4 allows attackers to execute a directory traversal.
CVE-2025-51052	A path traversal vulnerability in Vedo Suite 2024.17 allows remote authenticated attackers to read arbitrary filesystem files by exploiting an unsanitized 'file_get_c
CVE-2025-51057	A local file inclusion (LFI) vulnerability in Vedo Suite version 2024.17 allows remote authenticated attackers to read arbitrary filesystem files by exploiting an unsan
CVE-2025-50467	OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the TestDefinitionDAO interfac
CVE-2025-8749	Path Traversal vulnerability in API Endpoint in Mobile Industrial Robots (MiR) Software Versions prior to 3.0.0 on MiR Robots allows authenticated users to extract fil
CVE-2025-6259	The esri-map-view plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's esri-map-view shortcode in all versions up to, and including, 1.2 authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-55134	In Agora Foundation Agora fall23-Alpha1 before b087490, there is XSS via tag in client/agora/public/js/editorManager.js.
CVE-2025-8690	The Simple Responsive Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.0 due to insufficient input sanit to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-6690	The WP Tournament Registration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'field' parameter in all versions up to, and including, 1.3.0 Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-55011	Kanboard is project management software that focuses on the Kanban methodology. Prior to version 1.2.47, the createTaskFile method in the API does not validate write a file anywhere on the system the app user controls. The impact is limited due to the filename being hashed and having no extension. This issue has been pa
CVE-	The WPBakery Page Builder for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several shortcodes in all versions up to, and includir

2025-7502	authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-55133	In Agora Foundation Agora fall23-Alpha1 before b087490, there is XSS via topicName in client/agora/public/js/editorManager.js.
CVE-2025-32766	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiWeb CLI version 7.6.0 through 7.6.3 and before 7.4.8 allows a privileged attacker to execute
CVE-2025-55135	In Agora Foundation Agora fall23-Alpha1 before 690ce56, there is XSS via a profile picture to server/controller/userController.js. Formats other than PNG, JPEG, and
CVE-2025-6256	The Flex Guten plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'thumbnailHoverEffect' parameter in all versions up to, and including, 1.2.5 Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8874	The Master Addons – Elementor Addons with White Label, Free Widgets, Hover Effects, Conditions, & Animations plugin for WordPress is vulnerable to Stored Cross output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execu
CVE-2025-8688	The Inline Stock Quotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's stock shortcode in all versions up to, and including, 0.2 du authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-8621	The Mosaic Generator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'c' parameter in all versions up to, and including, 1.0.5 due to insuffi access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8568	The GMap Generator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'h' parameter in all versions up to, and including, 1.1 due to insufficie access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-41986	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S attacker could achieve a man-in-the-middle attack and compromise confidentiality and integrity of data.
CVE-2025-7399	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via an Elementor display setting in all versions up to, and including, 28.1.3 due to in level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-7726	The The7 theme for WordPress is vulnerable to Stored Cross-Site Scripting via its lightbox rendering code in all versions up to, and including, 12.6.0 due to insuffici description' attributes directly via jQuery.attr(), concatenates them into an HTML string, and inserts that string into the DOM using methods such as jQuery.html() v to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8462	The RT Easy Builder – Advanced addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the social URL parameter in all versions authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-48731	Mattermost Confluence Plugin version <1.5.0 fails to check the access of the user to the Confluence space which allows attackers to edit a subscription for a Confl
CVE-2025-7498	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown Widget in all versions up to, and including, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8685	The Wp chart generator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpchart shortcode in all versions up to, and including, 1.0 authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-8314	The Software Issue Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noaccess_msg parameter in all versions up to, and including, Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-7727	The Gutenverse plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Animated Text and Fun Fact blocks in all versions up to, and inclu for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected
CVE-2025-8825	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This affects the function RP_setBasicAuto of the f is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but
CVE-2025-8823	A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this vulnerability is the function setDevic injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosur
CVE-2025-40751	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.3). Affected SIMATIC RTLS Locating Manager Report Clients do not properly extract the credentials and use them to escalate their access rights from the Manager to the Systemadministrator role.
CVE-2025-8701	A vulnerability was found in Wanzhou WOES Intelligent Optimization Energy Saving System 1.0. It has been rated as critical. Affected by this issue is some unknow The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-	A vulnerability classified as critical was found in Wanzhou WOES Intelligent Optimization Energy Saving System 1.0. This vulnerability affects unknown code of the

2025-8703	manipulation of the argument energyId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8821	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This issue affects the function RP_setBasic of the initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any
CVE-2025-21017	Out-of-bounds write in detaching crypto box in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to write out-of-bounds memory.
CVE-2025-8818	A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this issue is the function setDFSSett attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not
CVE-2025-8702	A vulnerability classified as critical has been found in Wanzhou WOES Intelligent Optimization Energy Saving System 1.0. This affects an unknown part of the file /C argument ObjectID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8830	A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this issue is the function sub_3517C be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in a
CVE-2025-8705	A vulnerability, which was classified as critical, was found in Wanzhou WOES Intelligent Optimization Energy Saving System 1.0. Affected is an unknown function of argument BP_ProID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8706	A vulnerability has been found in Wanzhou WOES Intelligent Optimization Energy Saving System 1.0 and classified as critical. Affected by this vulnerability is an un manipulation of the argument MM_MenID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used
CVE-2025-8827	A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This issue affects the function um_inspect_cross_ban The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did
CVE-2025-8828	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected is the function ipv6cmd of the file /gof Ipv6PriDns/Ipv6SecDns/Ipv6StaticGateway/LanIpv6Addr/LanPrefixLen/pppoeUser/pppoePass/pppoeIdleTime/pppoeRedialPeriod/Ipv6in4_PrefixLen/LocalIpv6/Remote leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacte
CVE-2025-8829	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this vulnerability is the function um_r attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not r
CVE-2024-38805	EDK2 contains a vulnerability in BIOS where a user may cause an Integer Overflow or Wraparound by network means. A successful exploitation of this vulnerability
CVE-2025-50927	A reflected cross-site scripting (XSS) vulnerability in the List All FTP User Function in EHCP v20.04.1.b allows authenticated attackers to execute arbitrary JavaScript
CVE-2025-8729	A vulnerability has been found in MigoXLab LMeterX 1.2.0 and classified as critical. Affected by this vulnerability is the function process_cert_files of the file backen launched remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is f1b00597e293d09452aabd4fa57f3185207350e8. It
CVE-2025-8839	A vulnerability was found in jshERP up to 3.5. This issue affects some unknown processing of the file /jshERP-boot/user/addUser of the component Endpoint. The ma public and may be used.
CVE-2025-8841	A vulnerability was identified in zlt2000 microservices-platform up to 6.0.0. Affected by this vulnerability is the function Upload of the file zlt-business/file-center/sr be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8859	A vulnerability was identified in code-projects eBlog Site 1.0. Affected by this vulnerability is an unknown functionality of the file /native/admin/save-slider.php of th The exploit has been disclosed to the public and may be used.
CVE-2025-8697	A vulnerability was found in agentUniverse up to 0.0.18 and classified as critical. This issue affects the function StdioServerParameters of the component MCPSessi The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8704	A vulnerability, which was classified as critical, has been found in Wanzhou WOES Intelligent Optimization Energy Saving System 1.0. This issue affects some unkno Module. The manipulation of the argument resultId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and ma
CVE-2025-8791	A vulnerability was found in LitmusChaos Litmus up to 3.19.0. It has been rated as critical. This issue affects some unknown processing of the file /auth/list_projects exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8807	A vulnerability was found in xujeff tianti 天梯 up to 2.3. It has been declared as critical. This vulnerability affects unknown code of the file /tianti-module-admin/user disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8795	A vulnerability, which was classified as critical, was found in LitmusChaos Litmus up to 3.19.0. This affects an unknown part of the file /auth/login. The manipulation has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-	A vulnerability, which was classified as critical, was found in SkyworkAI DeepResearchAgent up to 08eb7f8eb9505d0094d75bb97ff7dacc3fa3bbf2. Affected is the fu possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this produ

8667	this disclosure but did not respond in any way.
CVE-2025-8756	A vulnerability has been found in TDuckCloud tduck-platform up to 5.1 and classified as critical. Affected by this vulnerability is the function preHandle of the file /n improper authorization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8775	A vulnerability was found in Qiyuesuo Eelectronic Signature Platform up to 4.34 and classified as critical. Affected by this issue is the function execute of the file /ap upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure
CVE-2025-8806	A vulnerability was found in zhilink 智互联(深圳)科技有限公司 ADP Application Developer Platform 应用开发者平台 1.0.0. It has been classified as critical. This affects ar is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but
CVE-2025-8797	A vulnerability was found in LitmusChaos Litmus up to 3.19.0 and classified as critical. This issue affects some unknown processing of the component LocalStorage disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8665	A vulnerability, which was classified as critical, has been found in agno-agi agno up to 1.7.5. This issue affects the function MCPTools/MultiMCPTools in the library li command leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was cor
CVE-2025-8764	A vulnerability classified as critical has been found in linlinjava litemall up to 1.8.0. Affected is the function Upload of the file /wx/storage/upload. The manipulation disclosed to the public and may be used.
CVE-2025-54623	Out-of-bounds read vulnerability in the devicemanager module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54608	Vulnerability that allows setting screen rotation direction without permission verification in the screen management module. Impact: Successful exploitation of this
CVE-2025-49456	Race condition in the installer for certain Zoom Clients for Windows may allow an unauthenticated user to impact application integrity via local access.
CVE-2025-21013	Improper access control in SemSensorManager for Galaxy Watch prior to SMR Aug-2025 Release 1 allows local attackers to access sensitive information related to
CVE-2025-54614	Input verification vulnerability in the home screen module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-40753	A vulnerability has been identified in POWER METER SICAM Q100 (7KG9501-0AA01-0AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0 V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA31-2AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q200 family (All versions >= V2.70 < allow an authenticated local attacker to extract it and use the configured SMTP service for arbitrary purposes.
CVE-2025-40752	A vulnerability has been identified in POWER METER SICAM Q100 (7KG9501-0AA01-0AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0 V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA31-2AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q200 family (All versions >= V2.70 < attacker to extract it and use the configured SMTP service for arbitrary purposes.
CVE-2025-30034	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.3). Affected devices do not properly validate input sent to its listening port
CVE-2025-54615	Vulnerability of insufficient information protection in the media library module. Impact: Successful exploitation of this vulnerability may affect service confidentialit
CVE-2025-54392	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 allows XSS for authentication error data, a different vulnerability than CVE-2
CVE-2025-50740	AutoConnect 1.4.2, an Arduino library, is vulnerable to a cross site scripting (xss) vulnerability. The AutoConnect web interface /_ac/config allows HTML/JS code to b
CVE-2025-54395	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 allows XSS for authentication configuration data.
CVE-2023-41519	Student Attendance Management System v1 was discovered to contain a cross-site scripting (XSS) vulnerability via the sessionName parameter at createSessionTe
CVE-2025-51053	A Cross-site scripting (XSS) vulnerability in /api_vedo/ in Vedo Suite version 2024.17 allows remote attackers to inject arbitrary Javascript or HTML code and potenti
CVE-2025-54784	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. There is a Cross Site Scripting (XSS) vulnerability in the SuiteCRM-instance. By simply viewing emails as the logged-in user, the payload can be triggered. With that, an attacker is able to run arbitrary actions as the l versions 7.14.7.
CVE-2025-	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions 7.14.6 and below have a Reflected Cross-S Referer header to include some arbitrary domain with malicious JavaScript code at the end. The server will attempt to block the arbitrary domain but allow the Java

54783	
CVE-2025-21457	Information disclosure while opening a fastrpc session when domain is not sanitized.
CVE-2025-42945	SAP NetWeaver Application Server ABAP has HTML injection vulnerability. Due to this, an attacker could craft a URL with malicious script as payload and trick a vict data or its manipulation. There is no impact on availability.
CVE-2025-42948	Due to a Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver ABAP Platform, an unauthenticated attacker could generate a malicious link and make it publicly generation, resulting in the creation of malicious content. When this malicious content gets executed, the attacker could gain the ability to access/modify informati
CVE-2023-41529	Hospital Management System v4 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in func2.php via the fname and lname parameters.
CVE-2025-51531	A reflected cross-site scripting (XSS) vulnerability in Sage DPW 2024_12_004 and earlier allows attackers to execute arbitrary JavaScript in the context of a victim's stated that the issue is fixed in 2025_06_000, released in June 2025.
CVE-2024-52680	EyouCMS 1.6.7 is vulnerable to Cross Site Scripting (XSS) in /login.php?m=admin&c=System&a=web&lang=cn.
CVE-2025-42942	SAP NetWeaver Application Server for ABAP has cross-site scripting vulnerability. Due to this, an unauthenticated attacker could craft a URL embedded with malicio attacker could access and modify limited information within the scope of victim's browser. This vulnerability has no impact on availability of the application.
CVE-2025-42975	SAP NetWeaver Application Server ABAP (BIC Document) allows an unauthenticated attacker to craft a URL link which, when accessed on the BIC Document applica the attacker to access and/or modify information related to the web client without affecting availability.
CVE-2025-21010	Improper privilege management in SamsungAccount prior to SMR Aug-2025 Release 1 allows local privileged attackers to deactivate Samsung account.
CVE-2025-24296	Improper input validation in some firmware for the Intel(R) E810 Ethernet before version 4.6 may allow a privileged user to enable denial of service via local access
CVE-2025-20067	Observable timing discrepancy in firmware for some Intel(R) CSME and Intel(R) SPS may allow a privileged user to potentially enable information disclosure via loca
CVE-2025-53514	Mattermost Confluence Plugin version <1.5.0 fails to handle unexpected request body which allows attackers to crash the plugin via constant hit to server webhook
CVE-2025-54463	Mattermost Confluence Plugin version <1.5.0 fails to handle unexpected request body which allows attackers to crash the plugin via constant hit to server webhook
CVE-2025-36020	IBM Guardium Data Protection could allow a remote attacker to obtain sensitive information due to cleartext transmission of sensitive credential information.
CVE-2025-54635	Vulnerability of returning released pointers in the distributed notification service. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54612	Iterator failure vulnerability in the card management module. Impact: Successful exploitation of this vulnerability may affect function stability.
CVE-2025-49558	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race manipulating the timing between the check of a resource's state and its use, allowing unauthorized write access. Exploitation of this issue does not require user int
CVE-2025-6572	The OpenStreetMap for Gutenberg and WPBakery Page Builder (formerly Visual Composer) WordPress plugin through 1.2.0 does not validate and escape some of it contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2025-54613	Iterator failure vulnerability in the card management module. Impact: Successful exploitation of this vulnerability may affect function stability.
CVE-2025-23333	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause an out-of-bounds read by mar
CVE-2025-23334	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause an out-of-bounds read by send
CVE-2025-	Windows Shortcut Following (.LNK) vulnerability in multiple processes of Mitsubishi Electric Iconics Digital Solutions GENESIS64 all versions, Mitsubishi Electric Iconi versions, and Mitsubishi Electric GENESIS version 11.00 allows a local authenticated attacker to make an unauthorized write to arbitrary files, by creating a symbol

7376	the attacker to destroy the file on a PC with the affected products installed, resulting in a denial-of-service (DoS) condition on the PC if the destroyed file is necessa
CVE-2025-36124	IBM WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.8 could allow a remote attacker to bypass security restrictions caused by a failure to honor JMS
CVE-2025-24840	Improper access control for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an unauthenticated user to pot
CVE-2025-47872	The public-facing product registration endpoint server responds differently depending on whether the S/N is valid and unregistered, valid but already registered, or attacker to gain information on the product registration status of different S/Ns.
CVE-2025-55136	ERC (aka Emotion Recognition in Conversation) through 0.3 has insecure deserialization via a serialized object because jsonpickle is used.
CVE-2025-50157	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.
CVE-2025-53719	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.
CVE-2025-50156	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.
CVE-2025-48393	The server identity check mechanism for firmware upgrade performed via command shell is insecurely implemented potentially allowing an attacker to perform a M download center.
CVE-2025-54618	Permission control vulnerability in the distributed clipboard module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2024-58257	EnzoH has an OS command injection vulnerability. Successful exploitation of this vulnerability may lead to arbitrary command execution.
CVE-2025-21020	Out-of-bounds write in creating bitmap images in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to write out-of-bounds memory.
CVE-2025-53138	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.
CVE-2025-55003	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys. In versions 2.3.1 and below, (TOTP). Due to normalization applied by the underlying TOTP library, codes were accepted which could contain whitespace; this whitespace could bypass internal r around this, use of rate-limiting quotas can limit an attacker's ability to exploit this: https://openbao.org/api-docs/system/rate-limit-quotas/.
CVE-2025-26472	Uncontrolled resource consumption for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an authenticated us
CVE-2025-53153	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.
CVE-2025-53148	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.
CVE-2025-54624	Unexpected injection event vulnerability in the multimodalinput module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-21021	Out-of-bounds write in drawing pinpad in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to write out-of-bounds memory.
CVE-2025-26398	SolarWinds Database Performance Analyzer was found to contain a hard-coded cryptographic key. If exploited, this vulnerability could lead to a machine-in-the-mid the server and administrator level privileges on the host.
CVE-2025-47806	In GStreamer through 1.26.1, the subparse plugin's parse_subrip_time function may write data past the bounds of a stack buffer, leading to a crash.
CVE-2025-47808	In GStreamer through 1.26.1, the subparse plugin's tmplayer_parse_line function may dereference a NULL pointer while parsing a subtitle file, leading to a crash.
CVE-2024-33607	Out-of-bounds read in some Intel(R) TDX module software before version TDX_1.5.07.00.774 may allow an authenticated user to potentially enable information dis

CVE-2025-54233	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Expl
CVE-2025-53136	Exposure of sensitive information to an unauthorized actor in Windows NT OS Kernel allows an authorized attacker to disclose information locally.
CVE-2025-21011	Improper access control in SemSensorService for Galaxy Watch prior to SMR Aug-2025 Release 1 allows local attackers to access sensitive information related to m
CVE-2025-21012	Improper access control in fall detection for Galaxy Watch prior to SMR Aug-2025 Release 1 allows local attackers to modify fall detection configuration.
CVE-2025-54238	Dimension versions 4.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue
CVE-2025-27537	Improper input validation for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an authenticated user to pote
CVE-2025-54192	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-54228	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-47807	In GStreamer through 1.26.1, the subparse plugin's subrip_unescape_formatting function may dereference a NULL pointer while parsing a subtitle file, leading to a
CVE-2025-54202	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-49567	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker c user interaction in that a victim must open a malicious file.
CVE-2025-49568	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. Exploitation of this iss
CVE-2025-54203	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54204	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54638	Issue of inconsistent read/write serialization in the ad module. Impact: Successful exploitation of this vulnerability may affect the availability of the ad service.
CVE-2025-54639	ParcelMismatch vulnerability in attribute deserialization. Impact: Successful exploitation of this vulnerability may cause playback control screen display exceptions.
CVE-2025-54205	Substance3D - Sampler versions 5.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-54640	ParcelMismatch vulnerability in attribute deserialization. Impact: Successful exploitation of this vulnerability may cause playback control screen display exceptions.
CVE-2025-54214	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54227	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-20090	Untrusted Pointer Dereference for some Intel(R) QuickAssist Technology software before version 2.5.0 may allow an authenticated user to potentially enable denial
CVE-2025-54193	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio

CVE-2024-52964	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiManager version 7.6.0 through 7.6.1, 7.4.0 7.4.5 and before 7.2.9 allows an authenticated remote attacker to overwrite arbitrary files via FGFM crafted requests.
CVE-2025-54235	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-5468	Improper handling of symbolic links in Ivanti Connect Secure before version 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 2 authenticated attacker to read arbitrary files on disk.
CVE-2025-54620	Deserialization vulnerability of untrusted data in the ability module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54201	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54200	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54199	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54198	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54197	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54195	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-40584	A vulnerability has been identified in SIMOTION SCOUT TIA V5.4 (All versions), SIMOTION SCOUT TIA V5.5 (All versions), SIMOTION SCOUT TIA V5.6 (All versions < V SCOUT V5.5 (All versions), SIMOTION SCOUT V5.6 (All versions < V5.6 SP1 HF7), SIMOTION SCOUT V5.7 (All versions < V5.7 SP1 HF1), SINAMICS STARTER V5.5 (All contains a XML External Entity Injection (XXE) vulnerability while parsing specially crafted XML files. This could allow an attacker to read arbitrary files in the syster
CVE-2025-54194	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-40766	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application runs docker containers without
CVE-2025-21472	Information disclosure while capturing logs as eSE debug messages are logged.
CVE-2025-49562	Animate versions 23.0.12, 24.0.9 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. Exploitation of this iss
CVE-2025-54188	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-53769	External control of file name or path in Windows Security App allows an authorized attacker to perform spoofing locally.
CVE-2025-54186	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitati
CVE-2025-54191	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-27072	Information disclosure while processing a packet at EAVB BE side with invalid header length.
CVE-2025-54190	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-21019	Improper authorization in Samsung Health prior to version 6.30.1.003 allows local attackers to access data in Samsung Health. User interaction is required for trigg

CVE-2025-53156	Exposure of sensitive information to an unauthorized actor in Storage Port Driver allows an authorized attacker to disclose information locally.
CVE-2025-54189	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitatio
CVE-2025-8840	A vulnerability was determined in jshERP up to 3.5. Affected is an unknown function of the file /jshERP-boot/user/deleteBatch of the component Endpoint. The mani been disclosed to the public and may be used. Different than CVE-2025-7947.
CVE-2025-54610	Out-of-bounds access vulnerability in the audio codec module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54648	Out-of-bounds read vulnerability in the SSAP module of the NearLink protocol stack. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54647	Out-of-bounds read vulnerability in the SSAP module of the NearLink protocol stack. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-54393	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 allows Static Code Injection. Authenticated users can obtain administrative
CVE-2025-8100	The Element Pack Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'marker_content' parameter in versio authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-8753	A vulnerability, which was classified as critical, has been found in linlinjava litemall up to 1.8.0. Affected by this issue is the function delete of the file /admin/storag be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8796	A vulnerability has been found in LitmusChaos Litmus up to 3.19.0 and classified as problematic. This vulnerability affects unknown code of the file /auth/delete_pr authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this discl
CVE-2025-42936	The SAP NetWeaver Application Server for ABAP does not enable an administrator to assign distinguished authorizations for different user roles, this issue allows au low impact on the confidentiality and integrity of the application, there is no impact on availability.
CVE-2025-20215	A vulnerability in the meeting-join functionality of Cisco Webex Meetings could have allowed an unauthenticated, network-proximate attacker to complete a meetir addressed this vulnerability in the Cisco Webex Meetings service, and no customer action is needed. This vulnerability existed due to client certificate validation iss wireless or adjacent networks for client-join requests and attempting to interrupt and complete the meeting-join flow as another user who was currently joining a m wireless or adjacent network, to monitor and intercept the targeted network traffic flows, and to satisfy timing requirements in order to interrupt the meeting-join f user. However, the Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of the vulnerability that is described in this advisory.
CVE-2025-54396	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 allows SQL Injection. Authenticated users can exploit this.
CVE-2025-20331	A vulnerability in the web-based management interface of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to conduct a stored XSS attac based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A su access sensitive, browser-based information. To exploit this vulnerability, the attacker must have at least a low-privileged account on the affected device.
CVE-2025-25229	Omnissa Workspace ONE UEM contains a Server-Side Request Forgery (SSRF) Vulnerability. A malicious actor with user privileges may be able to access restricted
CVE-2025-49745	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Dynamics 365 (on-premises) allows an unauthorized attacker to per
CVE-2025-54609	Out-of-bounds access vulnerability in the audio codec module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-8851	A vulnerability was determined in LibTIFF up to 4.5.1. Affected by this issue is the function readSeparateStripsetoBuffer of the file tools/tiffcrop.c of the component patch is identified as 8a7a48d7a645992ca83062b3a1873c951661e2b3. It is recommended to apply a patch to fix this issue.
CVE-2025-54619	Iterator failure issue in the multi-mode input module. Impact: Successful exploitation of this vulnerability may cause iterator failures and affect availability.
CVE-2025-8755	A vulnerability was found in macrozheng mall up to 1.0.3 and classified as problematic. This issue affects the function detail of the file UmsMemberController.java bypass. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure
CVE-2025-8842	A vulnerability has been found in NASM Netwide Assember 2.17rc0. Affected by this issue is the function do_directive of the file preproc.c. The manipulation leads t
CVE-2025-	A vulnerability has been found in NASM Netwide Assember 2.17rc0. Affected is the function parse_line of the file parser.c. The manipulation leads to stack-based bu

8846	
CVE-2025-8845	A vulnerability was identified in NASM Netwide Assember 2.17rc0. This issue affects the function assemble_file of the file nasm.c. The manipulation leads to stack-b and may be used.
CVE-2025-51308	In Gatling Enterprise versions below 1.25.0, a low-privileged user that does not hold the role "admin" could perform a REST API call on read-only endpoints, allowin
CVE-2025-8805	A vulnerability was found in Open5GS up to 2.7.5 and classified as problematic. Affected by this issue is the function smf_gsm_state_wait_pfcp_deletion of the file s remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.7.6 is able to address this issue. The patch is identified as c58b8f0
CVE-2025-8738	A vulnerability has been found in zlt2000 microservices-platform up to 6.0.0 and classified as problematic. This vulnerability affects unknown code of the file /actua initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-25006	Improper handling of additional special element in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.
CVE-2025-25007	Improper validation of syntactic correctness of input in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.
CVE-2025-8837	A vulnerability was identified in JasPer up to 4.2.5. This affects the function jpc_dec_dump of the file src/libjasper/jpc/jpc_dec.c of the component JPEG2000 File Han the public and may be used. The patch is named 8308060d3fbc1da10353ac8a95c8ea60eba9c25a. It is recommended to apply a patch to fix this issue.
CVE-2025-54621	Iterator failure issue in the WantAgent module. Impact: Successful exploitation of this vulnerability may cause memory release failures.
CVE-2025-8736	A vulnerability, which was classified as critical, has been found in GNU cflow up to 1.8. Affected by this issue is the function yylex of the file c.c of the component L disclosed to the public and may be used.
CVE-2025-8794	A vulnerability, which was classified as problematic, has been found in LitmusChaos Litmus up to 3.19.0. Affected by this issue is some unknown functionality of th access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but
CVE-2025-8620	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 4.6.0. This r
CVE-2025-25248	An Integer Overflow or Wraparound vulnerability [CWE-190] in FortiOS version 7.6.2 and below, version 7.4.7 and below, version 7.2.10 and below, 7.2 all versions, versions and FortiPAM version 1.5.0, version 1.4.2 and below, 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions SSL-VPN RDP and VNC bookmarks m
CVE-2025-20077	Missing release of memory after effective lifetime in the UEFI OobRasMmbiHandlerDriver module for some Intel(R) reference server platforms may allow a privilege
CVE-2025-8707	A vulnerability was found in Huuge Box App 1.0.3 on Android. It has been classified as problematic. This affects an unknown part of the file AndroidManifest.xml of Local access is required to approach this attack. The exploit has been disclosed to the public and may be used.
CVE-2025-8843	A vulnerability was found in NASM Netwide Assember 2.17rc0. This affects the function macho_no_dead_strip of the file outmacho.c. The manipulation leads to hea and may be used.
CVE-2025-54628	Vulnerability of incomplete verification information in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-6632	A maliciously crafted PSD file, when linked or imported into Autodesk 3ds Max, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this v
CVE-2025-8745	A vulnerability, which was classified as problematic, has been found in Weee RICEPO App 6.17.77 on Android. This issue affects some unknown processing of the fil application components. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early ab
CVE-2025-55152	oak is a middleware framework for Deno's native HTTP server, Deno Deploy, Node.js 16.5 and later, Cloudflare Workers and Bun. In versions 17.1.5 and below, it's headers.
CVE-2025-8804	A vulnerability has been found in Open5GS up to 2.7.5 and classified as problematic. Affected by this vulnerability is the function ngap_build_downlink_nas_transpo exploit has been disclosed to the public and may be used. Upgrading to version 2.7.6 is able to address this issue. The identifier of the patch is bca0a7b6e01d254f
CVE-2025-51533	An Insecure Direct Object Reference (IDOR) in Sage DPW v2024_12_004 and below allows unauthorized attackers to access internal forms via sending a crafted GE
CVE-2025-	The WP Private Content Plus plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.2 via the 'validate_restrict resticted posts on archive and feed pages.

4390	
CVE-2025-46660	An issue was discovered in 4C Strategies Exonaut 21.6. Passwords, stored in the database, are hashed without a salt.
CVE-2025-8803	A vulnerability, which was classified as problematic, was found in Open5GS up to 2.7.5. Affected is the function gmm_state_de_registered/gmm_state_exception of attack remotely. Upgrading to version 2.7.6 is able to address this issue. The name of the patch is 1f30edac27f69f61cff50162e980fe58fdeb30ca. It is recommende
CVE-2025-54998	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys. In versions 0.1.0 through 2.3 was caused by different aliasing between pre-flight and full login request user entity alias attributions. This is fixed in version 2.3.2. To work around this issue, exist limit-quotas/.
CVE-2025-54879	Mastodon is a free, open-source social network server based on ActivityPub Mastodon which facilitates LDAP configuration for authentication. In versions 3.1.5 thro error where the email-based throttle for confirmation emails incorrectly checks the password reset path instead of the confirmation path, effectively disabling per-e unlimited confirmation emails to any email address, as only a weak IP-based throttle (25 requests per 5 minutes) remains active. The vulnerability enables denial-o is fixed in versions 4.2.24, 4.3.11 and 4.4.3.
CVE-2025-8802	A vulnerability classified as problematic was found in Open5GS up to 2.7.5. This vulnerability affects the function smf_state_operational of the file src/smf/smf-sm.c remotely. The exploit has been disclosed to the public and may be used. Upgrading to version v2.7.6 is able to address this issue. The patch is identified as f168f75
CVE-2024-55402	4C Strategies Exonaut before v22.4 was discovered to contain an access control issue.
CVE-2025-49559	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by an Improper Limitation of a Pathname to a R leverage this vulnerability to modify limited data. Exploitation of this issue does not require user interaction.
CVE-2025-8801	A vulnerability classified as problematic has been found in Open5GS up to 2.7.5. This affects the function gmm_state_exception of the file src/amf/gmm-sm.c of the has been disclosed to the public and may be used. Upgrading to version 2.7.6 is able to address this issue. The identifier of the patch is f47f2bd4f7274295c5fbb19
CVE-2025-54786	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. In versions 7.14.6 and 8.8.0, the broken authenticat user's meeting (calendar event) data given their username, related functionality allows user enumeration. This is fixed in versions 7.14.7 and 8.8.1.
CVE-2025-8799	A vulnerability was found in Open5GS up to 2.7.5. It has been declared as problematic. Affected by this vulnerability is the function amf_npcf_am_policy_control_bu manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version recommended to upgrade the affected component.
CVE-2025-8800	A vulnerability was found in Open5GS up to 2.7.5. It has been rated as problematic. Affected by this issue is the function esm_handle_pdn_connectivity_request of t attack may be launched remotely. Upgrading to version 2.7.6 is able to address this issue. The name of the patch is 701505102f514cbde2856cd2ebc9bedb7efc820
CVE-2025-54394	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 has Insufficiently Protected Credentials for requests to remote Excel resourc
CVE-2025-7195	Early versions of Operator-SDK provided an insecure method to allow operator containers to run in environments that used a random UID. Operator-SDK before 0.1 Developers who used Operator-SDK before 0.15.2 to scaffold their operator may still be impacted by this if the insecure user_setup script is still being used to build permissions and a group ownership of root (gid=0). An attacker who can execute commands within an affected container, even as a non-root user, may be able to user with any arbitrary UID, including UID 0, leading to full root privileges within the container.
CVE-2025-54646	Vulnerability of inadequate packet length check in the BLE module. Impact: Successful exploitation of this vulnerability may affect performance.
CVE-2025-7677	Missing Authentication for Critical Function vulnerability in ABB Aspect.This issue affects Aspect: All versions.
CVE-2024-52885	The Mobile Access Portal's File Share application is vulnerable to a directory traversal attack, allowing an authenticated, malicious end-user (authorized to at least
CVE-2025-8708	A vulnerability was found in Antabot White-Jotter 0.22. It has been declared as critical. This vulnerability affects the function CookieRememberMeManager of the fil EVANNIGHTLY_WAOU leads to deserialization. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be diffic
CVE-2024-58255	EnzoH has an OS command injection vulnerability. Successful exploitation of this vulnerability may lead to arbitrary command execution.
CVE-2025-54458	Mattermost Confluence Plugin version <1.5.0 fails to check the access of the user to the Confluence space which allows attackers to create a subscription for a Cor
CVE-2025-54645	Out-of-bounds array access issue due to insufficient data verification in the location service module. Impact: Successful exploitation of this vulnerability may affect
CVE-2025-42949	Due to a missing authorization check in the ABAP Platform, an authenticated user with elevated privileges could bypass authorization restrictions for common trans without proper authorization, leading to a significant compromise of data confidentiality. However, the integrity and availability of the system remain unaffected.
CVE-	

2025-8081	The Elementor plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 3.30.2 via the Import_Images::import() function due to i access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.
CVE-2025-5466	XEE in Ivanti Connect Secure before 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secu to trigger a denial of service
CVE-2024-41982	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S information. This could allow an authenticated attacker to gain access of sensitive information.
CVE-2025-54651	Race condition vulnerability in the kernel hufs module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2025-8767	The AnWP Football Leagues plugin for WordPress is vulnerable to CSV Injection in all versions up to, and including, 0.16.17 via the 'download_csv_players' and 'dow above, to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a
CVE-2025-50928	Easy Hosting Control Panel EHCP v20.04.1.b was discovered to contain a SQL injection vulnerability via the id parameter in the Change Settings function.
CVE-2025-48394	An attacker with authenticated and privileged access could modify the contents of a non-sensitive file by traversing the path in the limited shell of the CLI. This sec
CVE-2025-54649	Vulnerability of using incompatible types to access resources in the location service. Impact: Successful exploitation of this vulnerability may cause some location i
CVE-2025-42943	SAP GUI for Windows may allow the leak of NTML hashes when specific ABAP frontend services are called with UNC paths. For a successful attack, the attacker nee execute by using SAP GUI for Windows. This could trigger automatic NTLM authentication, potentially exposing hashed credentials to an attacker. As a result, it has
CVE-2024-58256	EnzoH has an OS command injection vulnerability. Successful exploitation of this vulnerability may lead to arbitrary command execution.
CVE-2025-54626	Pointer dangling vulnerability in the cjwindow module. Impact: Successful exploitation of this vulnerability may affect function stability.
CVE-2025-23335	NVIDIA Triton Inference Server for Windows and Linux and the Tensor RT backend contain a vulnerability where an attacker could cause an underflow by a specific
CVE-2025-20025	Uncontrolled recursion for some TinyCBOR libraries maintained by Intel(R) before version 0.6.1 may allow an authenticated user to potentially enable denial of serv
CVE-2025-21018	Out-of-bounds read in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to read out-of-bounds memory.
CVE-2025-54636	Issue of buffer overflow caused by insufficient data verification in the kernel drop detection module. Impact: Successful exploitation of this vulnerability may affect
CVE-2025-53765	Exposure of private personal information to an unauthorized actor in Azure Stack allows an authorized attacker to disclose information locally.
CVE-2025-24313	Improper access control for some Device Plugins for Kubernetes software maintained by Intel before version 0.32.0 may allow a privileged user to potentially enabl
CVE-2025-36000	IBM WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.8 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed disclosure within a trusted session.
CVE-2025-22392	Out-of-bounds read in firmware for some Intel(R) AMT and Intel(R) Standard Manageability may allow a privileged user to potentially enable information disclosure
CVE-2024-40588	Multiple relative path traversal vulnerabilities [CWE-23] in Fortinet FortiMail version 7.6.0 through 7.6.1 and before 7.4.3, FortiVoice version 7.0.0 through 7.0.5 and before 7.4.6 may allow a privileged attacker to read files from the underlying filesystem via crafted CLI requests.
CVE-2025-54637	Out-of-bounds array access issue due to insufficient data verification in the kernel ambient light module. Impact: Successful exploitation of this vulnerability may a
CVE-2025-8790	A vulnerability was found in Portabilis i-Educar up to 2.9.0. It has been declared as critical. This vulnerability affects unknown code of the file /module/Api/pessoa of initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any
CVE-	

2025-8793	A vulnerability classified as problematic was found in LitmusChaos Litmus up to 3.19.0. Affected by this vulnerability is an unknown functionality. The manipulation exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-20332	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to modify parts of the configuration on an affect exploit this vulnerability by submitting a crafted HTTP request to an affected system. A successful exploit could allow the attacker to modify descriptions of files on
CVE-2025-8582	Insufficient validation of untrusted input in Core in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to spoof the contents of the Omnibox (URL ba
CVE-2025-8792	A vulnerability classified as problematic has been found in LitmusChaos Litmus up to 3.19.0. Affected is an unknown function. The manipulation leads to client-side public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8739	A vulnerability was found in zhenfeng13 My-Blog up to 1.0.0 and classified as problematic. This issue affects some unknown processing of the file /admin/tags/save The exploit has been disclosed to the public and may be used.
CVE-2025-8583	Inappropriate implementation in Permissions in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (
CVE-2025-8814	A vulnerability was found in atjiu pybbs up to 6.0.0 and classified as problematic. This issue affects the function setCookie of the file src/main/java/co/yiiu/pybbs/uti has been disclosed to the public and may be used. The patch is named 8aa2bb1aef3346e49aec6358edf5e47ce905ae7b. It is recommended to apply a patch to fix
CVE-2025-8808	A vulnerability was found in xujeff tianti 天梯 up to 2.3. It has been rated as problematic. This issue affects the function exportOrder of the file /tianti-module-admin initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any
CVE-2025-8789	A vulnerability was found in Portabilis i-Educar up to 2.9.0. It has been classified as problematic. This affects an unknown part of the file /module/Api/Diario of the c exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8580	Inappropriate implementation in Filesystems in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (
CVE-2025-8595	The Zakra theme for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the welcome_notice_import_handler() functior access and above, to import demo settings.
CVE-2025-55006	Frappe Learning is a learning system that helps users structure their content. In versions 2.33.0 and below, the image upload functionality did not adequately sanit malicious content. Malicious SVG files could be used to execute arbitrary scripts in the context of other users. A fix for this issue is planned for version 2.34.0.
CVE-2025-8852	A vulnerability was identified in WuKongOpenSource WukongCRM 11.0. This affects an unknown part of the file /adminFile/upload of the component API Response H remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-21014	Improper export of android application component in Emergency SoS prior to SMR Aug-2025 Release 1 allows local attackers to access sensitive information.
CVE-2025-21016	Improper access control in PkgPredictorService prior to SMR Aug-2025 Release 1 in Chinese Android 13, 14, 15 and 16 allows local attackers to use the privileged A
CVE-2025-8577	Inappropriate implementation in Picture In Picture in Google Chrome prior to 139.0.7258.66 allowed a remote attacker who convinced a user to engage in specific U
CVE-2025-8482	The Simple Local Avatars plugin for WordPress is vulnerable to unauthorized modification of data in version 2.8.4. This is due to a missing capability check on the m and above, to migrate avatar metadata for all users.
CVE-2025-8579	Inappropriate implementation in Picture In Picture in Google Chrome prior to 139.0.7258.66 allowed a remote attacker who convinced a user to engage in specific U
CVE-2025-8581	Inappropriate implementation in Extensions in Google Chrome prior to 139.0.7258.66 allowed a remote attacker who convinced a user to engage in specific UI gest
CVE-2025-8452	By using the "uscan" protocol provided by the eSCL specification, an attacker can discover the serial number of multi-function printers that implement the Brother- calculate the default administrator password. This flaw is similar to CVE-2024-51977, with the only difference being the protocol by which an attacker can use to le discovery service that implements the eSCL specification can be used to exploit this vulnerability, and one such implementation is the runZero Explorer. Changing administrator password would no longer be the correct password.
CVE-2025-46388	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
CVE-2025-42934	SAP S/4HANA Supplier invoice is vulnerable to CRLF Injection. An attacker with user-level privileges can bypass the allowlist and insert untrusted sites into the 'Trus on the application's integrity and no impact on confidentiality or availability.

CVE-2025-8772	A vulnerability, which was classified as problematic, has been found in Vinades NukeViet up to 4.5.06. This issue affects some unknown processing of the file /admi forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure
CVE-2025-7965	The CBX Restaurant Booking WordPress plugin through 1.2.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a
CVE-2025-49755	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.
CVE-2025-49736	The ui performs the wrong action in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.
CVE-2025-54397	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 inserts Sensitive Information Into Sent Data to authenticated users.
CVE-2025-22834	AMI APTIOV contains a vulnerability in BIOS where a user may cause “Improper Initialization” by local accessing. Successful exploitation of this vulnerability may le
CVE-2025-54650	Improper array index verification vulnerability in the audio codec module. Impact: Successful exploitation of this vulnerability may affect the audio decoding functi
CVE-2025-55013	The Assemblyline 4 Service Client interfaces with the API to fetch tasks and publish the result for a service in Assemblyline 4. In versions below 4.6.1.dev138, the A directly as a local file name.A malicious or compromised server (or any MITM that can speak to client) can return a path-traversal payload such as `../../../etc/cron.d 4.6.1.dev138.
CVE-2025-42935	The SAP NetWeaver Application Server ABAP and ABAP Platform Internet Communication Manager (ICM) permits authorized users with admin privileges and local a confidentiality of the application, with no impact on integrity or availability.
CVE-2025-33023	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions), RUGGEDCOM ROX MX5000RE (All versions), RUGGEDCOM ROX RX1400 (All versions versions), RUGGEDCOM ROX RX1511 (All versions), RUGGEDCOM ROX RX1512 (All versions), RUGGEDCOM ROX RX1524 (All versions), RUGGEDCOM ROX RX1536 (files that can be uploaded from the web interface. This could allow an authenticated remote attacker with high privileges in the web interface to upload arbitrary fi
CVE-2025-20044	Improper locking for some Intel(R) TDX Module firmware before version 1.5.13 may allow a privileged user to potentially enable escalation of privilege via local acc
CVE-2025-44001	Mattermost Confluence Plugin version <1.5.0 fails to check the access of the user to the channel which allows attackers to get channel subscription details without
CVE-2025-54616	Out-of-bounds array access vulnerability in the ArkUI framework. Impact: Successful exploitation of this vulnerability may affect availability.
CVE-2025-20990	Improper access control in accessing system device node prior to SMR Aug-2025 Release 1 allows local attackers to access device identifier.
CVE-2025-32094	An issue was discovered in Akamai Ghost, as used for the Akamai CDN platform before 2025-03-26. Under certain circumstances, a client making an HTTP/1.x OPTI two in-path Akamai servers interpret the request, allowing an attacker to smuggle a second request in the original request body.
CVE-2025-53910	Mattermost Confluence Plugin version <1.5.0 fails to check the access of the user to the channel which allows attackers to create a channel subscription without pr
CVE-2025-8285	Mattermost Confluence Plugin version <1.5.0 fails to check the access of the user to the channel which allows attackers to create channel subscription without pro
CVE-2025-21015	Path Traversal in Document scanner prior to SMR Aug-2025 Release 1 allows local attackers to delete file with Document scanner's privilege.
CVE-2025-32004	Improper input validation in the Intel Edger8r Tool for some Intel(R) SGX SDK may allow an authenticated user to potentially enable escalation of privilege via local
CVE-2025-26863	Uncontrolled resource consumption in the Linux kernel-mode driver for some Intel(R) 700 Series Ethernet before version 2.28.5 may allow an authenticated user to
CVE-2025-8742	A vulnerability was found in macrozheng mall 1.0.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Admi launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The vendor was contacted early about this disclosure but di
CVE-2025-8759	A vulnerability was found in TRENDnet TN-200 1.02b02. It has been declared as problematic. This vulnerability affects unknown code of the component Lighttpd. Th cryptographic key . The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been d way.
CVE-	

2024-56339	IBM WebSphere Application Server 9.0 and WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.7 could allow a remote attacker to bypass security restri
CVE-2025-8763	A vulnerability was found in Ruijie EG306MG 3.0(1)B11P309. It has been rated as problematic. This issue affects some unknown processing of the file /etc/strongsw i_dont_care_about_security_and_use_aggressive_mode_psk leads to missing encryption of sensitive data. The attack may be initiated remotely. The complexity of a but did not respond in any way.
CVE-2025-8741	A vulnerability was found in macrozheng mall up to 1.0.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file / remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The ver
CVE-2025-54999	OpenBao exists to provide a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys. In versions 0.1.0 through 2.3 existent users and users with stored credentials. This is independent of whether the supplied credentials were valid for the given user. This issue was fixed in versi of requests in a period of time: https://openbao.org/api-docs/system/rate-limit-quotas/.
CVE-2025-54787	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. There is a vulnerability in SuiteCRM version 7.14.6 v attachments). An unauthenticated attacker could download internal files when he discovers a valid file-ID. Valid IDs could be brute-forced, but this is quite time-cor
CVE-2025-8556	A flaw was found in CIRCL's implementation of the FourQ elliptic curve. This vulnerability allows an attacker to compromise session security via low-order point inje
CVE-2025-53857	Mattermost Confluence Plugin version <1.5.0 fails to check the access of the user to the channel which allows attackers to get channel subscription details without
CVE-2025-49221	Mattermost Confluence Plugin version <1.5.0 fails to enforce authentication of the user to the Mattermost instance which allows unauthenticated attackers to acce
CVE-2025-55188	7-Zip before 25.01 does not always properly handle symbolic links during extraction.
CVE-2025-8765	A vulnerability classified as problematic was found in Datacom DM955 5GT 1200 825.8010.00. Affected by this vulnerability is an unknown functionality of the com launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8847	A vulnerability was found in yangzongzhuan RuoYi up to 4.8.1. Affected by this vulnerability is the function Edit of the file /system/notice/edit. The manipulation of t has been disclosed to the public and may be used.
CVE-2025-8784	A vulnerability classified as problematic was found in Portabilis i-Educar up to 2.9. This vulnerability affects unknown code of the file /intranet/funcionario_vinculo_c The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did n
CVE-2025-8785	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar up to 2.9. This issue affects some unknown processing of the file /intranet scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosur
CVE-2025-8786	A vulnerability, which was classified as problematic, was found in Portabilis i-Diario up to 1.5.0. Affected is an unknown function of the file /registros-de-conteudos-p atividades/Conteúdos leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The v
CVE-2025-38746	Dell SupportAssist OS Recovery, versions prior to 5.5.14.0, contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability. An unauthenticate
CVE-2025-8787	A vulnerability has been found in Portabilis i-Diario up to 1.5.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /re Registro de atividades/Conteúdos leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used
CVE-2025-8788	A vulnerability was found in Portabilis i-Diario up to 1.5.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /planos-de-a Parecer/Conteúdos/Objetivos leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The
CVE-2024-41983	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S encountered during the generation of reports using Cockpit tool.
CVE-2025-8743	A vulnerability classified as problematic has been found in Scada-LTS up to 2.7.8.1. This affects an unknown part of the file /data_source_edit.shtm of the compone possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8737	A vulnerability, which was classified as problematic, was found in zlt2000 microservices-platform up to 6.0.0. This affects the function onLogoutSuccess of the file s redirect_url leads to open redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-24523	Protection mechanism failure for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an authenticated user to
CVE-2025-8813	A vulnerability has been found in atjiu pybbs up to 6.0.0 and classified as problematic. This vulnerability affects the function changeLanguage of the file src/main/ja The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is identified as edb14ff13e9e05394960ba46c3d31d8
CVE-	Due to a missing authorization check in SAP Cloud Connector, an attacker on an adjacent network with low privileges could send a crafted request to the endpoint

2025-42955	availability of the service. Confidentiality and integrity of the data are not affected.
CVE-2025-42941	SAP Fiori (Launchpad) is vulnerable to Reverse Tabnabbing vulnerability due to inadequate external navigation protections for its link (<a>) elements. An attacker administrative access is necessary for certain configurations, the attacker does not need the administrative privileges to execute the attack. This could result in un integrity of the system, but the availability remains unaffected.
CVE-2025-27250	Uncontrolled resource consumption for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an authenticated us
CVE-2025-8835	A vulnerability was found in JasPer up to 4.2.5. Affected by this vulnerability is the function jas_image_chclrspc of the file src/libjasper/base/jas_image.c of the comp the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier of the patch is bb7d62bd0a2a8e0e1fdb4d603f3305f9551
CVE-2025-8746	A vulnerability, which was classified as problematic, was found in GNU libopts up to 27.6. Affected is the function __strstr_sse2. The manipulation leads to memory used. This issue was initially reported to the tcpreplay project, but the code maintainer explains, that this "bug appears to be in libopts which is an external library.
CVE-2025-8733	A vulnerability was found in GNU Bison up to 3.8.2. It has been rated as problematic. This issue affects the function __obstack_vprintf_internal of the file obprintf.c. disclosed to the public and may be used.
CVE-2025-8734	A vulnerability classified as problematic has been found in GNU Bison up to 3.8.2. Affected is the function code_free of the file src/scan-code.c. The manipulation le used.
CVE-2025-8732	A vulnerability was found in libxml2 up to 2.14.5. It has been declared as problematic. This vulnerability affects the function xmlParseSGMLCatalog of the compone disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The code maintainer explains, that "[t]he issue can that anyone is still using SGML catalogs at all."
CVE-2025-21024	Use of Implicit Intent for Sensitive Communication in Smart View prior to Android 16 allows local attackers to access sensitive information.
CVE-2025-21023	Improper access control in WcsExtension for Galaxy Watch prior to Android Watch 16 allows local attackers to access sensitive information.
CVE-2025-21022	Improper access control in Galaxy Wearable prior to version 2.2.63.25042861 allows local attackers to access sensitive information.
CVE-2025-8844	A vulnerability was determined in NASM Netwide Assember 2.17rc0. This vulnerability affects the function parse_smacro_template of the file preproc.c. The manipu and may be used.
CVE-2025-8836	A vulnerability was determined in JasPer up to 4.2.5. Affected by this issue is the function jpc_floorlog2 of the file src/libjasper/jpc/jpc_enc.c of the component JPEG2 been disclosed to the public and may be used. The patch is identified as 79185d32d7a444abae441935b20ae4676b3513d4. It is recommended to apply a patch to
CVE-2025-25212	in OpenHarmony v5.0.3 and prior versions allow a local attacker case DOS through improper input.
CVE-2025-24511	Improper initialization in the Linux kernel-mode driver for some Intel(R) I350 Series Ethernet before version 5.19.2 may allow an authenticated user to potentially e
CVE-2025-20613	Predictable Seed in Pseudo-Random Number Generator (PRNG) in the firmware for some Intel(R) TDX may allow an authenticated user to potentially enable inform
CVE-2025-24844	in OpenHarmony v5.0.3 and prior versions allow a local attacker case DOS through missing release of memory.
CVE-2025-8735	A vulnerability classified as problematic was found in GNU cflow up to 1.8. Affected by this vulnerability is the function yylex of the file c.c of the component Lexer. disclosed to the public and may be used.
CVE-2025-8698	A vulnerability was found in Open5GS up to 2.7.5. It has been classified as problematic. Affected is the function amf_nsmf_pdusession_handle_release_sm_context Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The name of the patch is 66bc558e417e70ae216ec155e4e81c14
CVE-2025-26690	in OpenHarmony v5.0.3 and prior versions allow a local attacker case DOS through NULL pointer dereference.
CVE-2025-24925	in OpenHarmony v5.0.3 and prior versions allow a local attacker case DOS through missing release of memory.
CVE-2025-27536	in OpenHarmony v5.0.3 and prior versions allow a local attacker cause DOS through type confusion.
CVE-2025-	Insertion of sensitive information into log file for some Intel(R) Local Manageability Service software before version 2514.7.16.0 may allow an authenticated user to

24520	
CVE-2025-26697	Uncontrolled resource consumption in the Linux kernel-mode driver for some Intel(R) 700 Series Ethernet before version 2.28.5 may allow an authenticated user to
CVE-2025-27562	in OpenHarmony v5.0.3 and prior versions allow a local attacker case DOS through missing release of memory.
CVE-2025-45764	jsrsasign v11.1.0 was discovered to contain weak encryption. NOTE: this issue has been disputed by a third party who believes that CVE IDs can be assigned for ke This dispute is subject to review under CNA rules 4.1.4, 4.1.14, and other rules; the dispute tagging is not meant to recommend an outcome for this CVE Record.
CVE-2024-41980	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S interface by default. This could allow an authenticated attacker to gain unauthorized access to sensitive information.
CVE-2025-8751	A vulnerability was found in Protected Total WebShield Extension up to 3.2.0 on Chrome. It has been classified as problematic. This affects an unknown part of the the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be use
CVE-2025-52136	In EMQX before 5.8.6, administrators can install arbitrary novel plugins via the Dashboard web interface. NOTE: the Supplier's position is that this is the intended b installation) is set by the "emqx ctl plugins allow" CLI command.
CVE-2025-27576	Uncontrolled resource consumption for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may allow an unauthenticated
CVE-2025-24324	Integer overflow or wraparound in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user to pot
CVE-2025-27707	Exposure of sensitive information to an unauthorized actor for some Edge Orchestrator software before version 24.11.1 for Intel(R) Tiber(TM) Edge Platform may al
CVE-2024-41984	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S inaccessible resource leading to exposing the system applications.
CVE-2024-41985	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), S could allow an attacker to get unauthorized access if the session is left idle.
CVE-2025-54798	tmp is a temporary file and directory creator for node.js. In versions 0.2.3 and below, tmp is vulnerable to an arbitrary temporary file / directory write via symbolic
CVE-2025-8774	A vulnerability has been found in riscv-boom SonicBOOM up to 2.2.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the approach this attack. The complexity of an attack is rather high. The exploitation appears to be difficult. The vendor was contacted early about this disclosure but d
CVE-2025-8834	A vulnerability has been found in JCG Link-net LW-N915R 17s.20.001.908. Affected is an unknown function of the file /wireless/basic.asp of the component Wireless launch the attack remotely.
CVE-2025-40570	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V10.0), SIPROTEC 5 6MD85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 5 6MU85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7KE85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SA82 (CP150) (All versions < V10.0), V10.0), SIPROTEC 5 7SD82 (CP150) (All versions < V10.0), SIPROTEC 5 7SD86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SD87 (CP300) (All versions > SIPROTEC 5 7SJ85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SJ86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SK82 (CP150) (All versions < SIPROTEC 5 7SL86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SL87 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SS85 (CP300) (All versions SIPROTEC 5 7SX82 (CP150) (All versions < V10.0), SIPROTEC 5 7SX85 (CP300) (All versions < V10.0), SIPROTEC 5 7SY82 (CP150) (All versions < V10.0), SIPROTEC (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7UT86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7UT87 (CP300) (All versions >= V7.80 < V10.0) V10.0), SIPROTEC 5 7VU85 (CP300) (All versions < V10.0), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V10.0). Affected devices do not properly limit the l send specially crafted packets with high bandwidth to the affected devices thus forcing them to exhaust their memory and stop responding to any network traffic v is not affected of this vulnerability.
CVE-2025-8740	A vulnerability was found in zhenfeng13 My-Blog up to 1.0.0. It has been classified as problematic. Affected is an unknown function of the file /admin/categories/sa is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8812	A vulnerability, which was classified as problematic, was found in atjiu pybbs up to 6.0.0. This affects an unknown part of the file /api/settings of the component Ad been disclosed to the public and may be used. The identifier of the patch is 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to
CVE-2025-8750	A vulnerability has been found in macrozheng mall up to 1.0.3 and classified as problematic. Affected by this vulnerability is the function Upload of the file /minio/u can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond
CVE-2025-22853	Improper synchronization in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.
CVE-2025-21096	Improper buffer restrictions in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.

CVE-2025-55169	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Prior to version 3.4.8, a path traversal vulnerability wa an attacker to gain unauthorized access to local files in the server and sensitive information stored in config.php. config.php contains information that could allow c
CVE-2025-55168	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Prior to version 3.4.8, a SQL Injection vulnerability was vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This issue has been
CVE-2025-43734	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.10, 2024.Q4.0 through through update 92 allows a remote authenticated attacker to inject JavaScript code in the “first display label” field in the configuration of a custom sort widget. Thi
CVE-2025-32430	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions 4.2-milestone-3 through 16.4.7, 16.5.0-rc-1 through execute malicious JavaScript code in the context of the victim's session by getting the victim to visit an attacker-controlled URL. This permits the attacker to perfor workaround the issue, manually patch the WAR with the same changes as the original patch.
CVE-2025-55167	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Prior to version 3.4.8, a SQL Injection vulnerability was vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This issue has been
CVE-2025-7202	A Cross-Site Request Forgery (CSRF) in Elgato's Key Lights and related light products allows an attacker to host a malicious webpage that remotely controlles the v
CVE-2025-8653	Kenwood DMX958XR JKRadioService Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to exe vulnerability. The specific flaw exists within the JKRadioService. The issue results from the lack of proper validation of the length of user-supplied data prior to copy root. Was ZDI-CAN-26312.
CVE-2025-8654	Kenwood DMX958XR ReadMVGImage Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arb vulnerability. The specific flaw exists within the ReadMVGImage function. The issue results from the lack of proper validation of a user-supplied string before using CAN-26313.
CVE-2025-8655	Kenwood DMX958XR libSystemLib Command injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitr vulnerability. The specific flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using CAN-26314.
CVE-2025-8656	Kenwood DMX958XR Protection Mechanism Failure Software Downgrade Vulnerability. This vulnerability allows physically present attackers to downgrade software specific flaw exists within the libSystemLib library. The issue results from the lack of proper validation of version information before performing an update. An attac CAN-26355.
CVE-2025-55019	Rejected reason: Not used
CVE-2025-55020	Rejected reason: Not used
CVE-2025-55021	Rejected reason: Not used
CVE-2025-55022	Rejected reason: Not used
CVE-2025-55023	Rejected reason: Not used
CVE-2025-55024	Rejected reason: Not used
CVE-2025-55025	Rejected reason: Not used
CVE-2025-55026	Rejected reason: Not used
CVE-2025-55027	Rejected reason: Not used
CVE-2025-7954	A race condition vulnerability has been identified in Shopware's voucher system of Shopware v6.6.10.4 that allows attackers to bypass intended voucher restrictio
CVE-2025-22469	OS command injection vulnerability exists in CL4/6NX Plus and CL4/6NX-J Plus (Japan model) with the firmware versions prior to 1.15.5-r1. An arbitrary OS comman
CVE-2025-8651	Kenwood DMX958XR JKWifiService Command Injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitı vulnerability. The specific flaw exists within the JKWifiService. The issue results from the lack of proper validation of a user-supplied string before using it to execut
CVE-	

2025-22470	CL4/6NX Plus and CL4/6NX-J Plus (Japan model) with the firmware versions prior to 1.15.5-r1 allow crafted dangerous files to be uploaded. An arbitrary Lua script m
CVE-2025-7771	ThrottleStop.sys, a legitimate driver, exposes two IOCTL interfaces that allow arbitrary read and write access to physical memory via the MmMapIoSpace function. kernel and invoke arbitrary kernel functions with ring-0 privileges. The vulnerability enables local attackers to execute arbitrary code in kernel context, resulting in protections. ThrottleStop.sys version 3.0.0.0 and possibly others are affected. Apply updates per vendor instructions.
CVE-2025-5197	A Regular Expression Denial of Service (ReDoS) vulnerability exists in the Hugging Face Transformers library, specifically in the `convert_tf_weight_name_to_pt_we regex pattern `/[^/]*___([^/]*)/` that can be exploited to cause excessive CPU consumption through crafted input strings due to catastrophic backtracking. The vul exhaustion, and potential API service vulnerabilities, impacting model conversion processes between TensorFlow and PyTorch formats.
CVE-2025-8616	A weakness identified in OpenText Advanced Authentication where a Malicious browser plugin can record and replay the user authentication process to bypass Aut
CVE-2025-8130	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-7768	Tigo Energy's Cloud Connect Advanced (CCA) device contains hard-coded credentials that allow unauthorized users to gain administrative access. This vulnerability disrupting solar energy production, and interfering with safety mechanisms.
CVE-2025-7769	Tigo Energy's CCA is vulnerable to a command injection vulnerability in the /cgi-bin/mobile_api endpoint when the DEVICE_PING command is called, allowing remot execute arbitrary commands on the device that could cause potential unauthorized access, service disruption, and data exposure.
CVE-2025-7770	Tigo Energy's CCA device is vulnerable to insecure session ID generation in their remote API. The session IDs are generated using a predictable method based on t session ID requirements for certain commands, this enables unauthorized access to sensitive device functions on connected solar optimization systems.
CVE-2023-3194	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-8086	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-54799	Let's Encrypt client and ACME library written in Go (Lego). In versions 4.25.1 and below, the github.com/go-acme/lego/v4/acme/api package (thus the lego library a solves an ACME challenge over unencrypted HTTP, the ACME protocol requires HTTPS when a client communicates with the CA to performs ACME functions. Howev subsequent addresses returned by the CAs in the directory and order objects. If users input HTTP URLs or CAs misconfigure endpoints, protocol operations occur ov identifiers to network attackers. This was fixed in version 4.25.2.
CVE-2025-54885	Thinbus Javascript Secure Remote Password is a browser SRP6a implementation for zero-knowledge password authentication. In versions 2.0.0 and below, a protoc prime (defaulted to 2048 bits). The client public value is being generated from a private value that is 4 bits below the specification. This reduces the protocol's des the shared session key and password proof. This is fixed in version 2.0.1.
CVE-2025-29865	: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TAGFREE X-Free Uploader XFU allows Path Traversal.This issue affec
CVE-2025-29866	: External Control of File Name or Path vulnerability in TAGFREE X-Free Uploader XFU allows : Parameter Injection.This issue affects X-Free Uploader: from 1.0.1.00
CVE-2025-8652	Kenwood DMX958XR JKWifiService Command Injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitr vulnerability. The specific flaw exists within the JKWifiService. The issue results from the lack of proper validation of a user-supplied string before using it to execut
CVE-2025-8650	Kenwood DMX958XR libSystemLib Command Injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitr vulnerability. The specific flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using CAN-26306.
CVE-2025-7054	Cloudflare quiche was discovered to be vulnerable to an infinite loop when sending packets containing RETIRE_CONNECTION_ID frames. QUIC connections possess 5.1 . Once the QUIC handshake completes, a local endpoint is responsible for issuing and retiring Connection IDs that are used by the remote peer to populate the ensure synchronization between peers. An unauthenticated remote attacker can exploit this vulnerability by first completing a handshake and then sending a spec packet containing RETIRE_CONNECTION_ID frames, Section 19.16 of RFC 9000 https://datatracker.ietf.org/doc/html/rfc9000#section-19.6 requires that the sequenc packet. In other words, a packet cannot contain a frame that retires itself. In scenarios such as path migration, it is possible for there to be multiple active paths wi behaviour of a quiche design feature that supports retirement across paths while maintaining full connection ID synchronization, leading to an infinite loop.This issu
CVE-2025-8633	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-54125	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki Platform Legacy Old Core and XWiki Platform Old Core ve that can be triggered by any user with view rights on a page by appending ?xpage=xml to the URL includes password and email properties stored on a document t the file templates/xml.vm in the deployed WAR can be deleted if the XML isn't needed. There isn't any feature in XWiki itself that depends on the XML export.
CVE-2025-54571	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. In versions 2.9.11 and below, an attacker can overr we have demonstrated the potential for XSS and arbitrary script source code disclosure in the latest version of mod_security2. This issue is fixed in version 2.9.12.
CVE-2025-54801	Fiber is an Express inspired web framework written in Go. In versions 2.52.8 and below, when using Fiber's Ctx.BodyParser to parse form data containing a large nu slice allocation in the underlying schema decoder. The root cause is that the decoder attempts to allocate a slice of length idx + 1 without validating whether the i exhaustion, causing a panic or crash. This is fixed in version 2.52.9.
CVE-	

2025-54869	FPDI is a collection of PHP classes that facilitate reading pages from existing PDF documents and using them as templates in FPDF. In versions 2.6.2 and below, any An attacker can upload a small, malicious PDF file that will cause the server-side script to crash due to memory exhaustion. Repeated attacks can lead to sustained
CVE-2025-54872	onion-site-template is a complete, scalable tor hidden service self-hosting sample. Versions which include commit 3196bd89 contain a baked-in tor image if the see or if someone were able to acquire access to the user's device outside of a containerized environment. This is fixed by commit bc9ba0fd.
CVE-2025-54873	RISC Zero is a zero-knowledge verifiable general computing platform based on zk-STARKs and the RISC-V microarchitecture. RISC packages risc0-zkvm versions 2.0 where signed integer division allows multiple outputs for certain inputs with only one being valid, and division by zero results are underconstrained. This issue is fix
CVE-2025-54876	The Janssen Project is an open-source identity and access management (IAM) platform. In versions 1.9.0 and below, Janssen stores passwords in plaintext in the log
CVE-2025-54883	Vision UI is a collection of enterprise-grade, dependency-free modules for modern web projects. In versions 1.4.0 and below, the getSecureRandomInt function in s silent 32-bit integer overflow in its internal masking logic, the function fails to produce a uniform distribution of random numbers when the requested range betwee bitmask for the rejection sampling algorithm. This causes the mask to be incorrect for any range requiring 32 or more bits of entropy. This issue is fixed in version
CVE-2025-54884	Vision UI is a collection of enterprise-grade, dependency-free modules for modern web projects. In versions 1.4.0 and below, the generateSecureId and getSecureR of Service (DoS) attacks. The generateSecureId(length) function directly used the length parameter to size a Uint8Array buffer, allowing attackers to exhaust serve getSecureRandomInt(min, max) function calculated buffer size based on the range between min and max, where large ranges caused excessive memory allocation
CVE-2025-8628	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8629	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8630	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8631	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8632	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8634	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8649	Kenwood DMX958XR JKWifiService Command Injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitr vulnerability. The specific flaw exists within the JKWifiService. The issue results from the lack of proper validation of a user-supplied string before using it to execut
CVE-2025-8635	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8636	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8637	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8638	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8639	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can
CVE-2025-8640	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8641	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8642	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8643	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-	

2025-8644	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8645	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8646	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8647	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8648	Kenwood DMX958XR Firmware Update Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected flaw exists within the firmware update process. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system cal
CVE-2025-8533	A vulnerability was identified in the XPC services of Fantastical. The services failed to implement proper client authorization checks in its listener:shouldAcceptNew process could connect to the XPC service and access its methods. This issue has been resolved in version 4.0.16.
CVE-2025-34148	An unauthenticated OS command injection vulnerability exists in the Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02). When configuring the device i Fi range to inject arbitrary shell commands that execute as root, resulting in full device compromise.
CVE-2025-55166	savg-sanitizer is a PHP SVG/XML sanitizer. Prior to version 0.22.0, the sanitization logic in the cleanXlinkHrefs method only searches for lower-case attribute name, domains. This issue has been patched in version 0.22.0.
CVE-2025-38499	In the Linux kernel, the following vulnerability has been resolved: clone_private_mnt(): make sure that caller has CAP_SYS_ADMIN in the right userns What we want able to undo" may be a result of MNT_LOCKED on a child, but it may also come from lacking admin rights in the userns of the namespace mount belongs to. clone_ various userns during the mount, especially with the new mount API; they serve different purposes and in case of clone_private_mnt() they usually, but not always
CVE-2025-54124	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki Platform Legacy Old Core and XWiki Platform Old Core ve can create an XClass with a database list property that references a password property. When adding an object of that XClass, the content of that password proper password hashes of all users, and possibly other password properties (with hashed or plain storage) that are on pages that the user can view. This issue is fixed in
CVE-2025-8854	Stack-based buffer overflow in LoadOFF in bulletphysics bullet3 before 3.26 on all platforms allows remote attackers to execute arbitrary code via a crafted OFF file function.
CVE-2025-8660	Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed.
CVE-2025-8661	A stored Cross-Site Scripting vulnerability (XSS) occurs when the server does not properly validate or encode the data entered by the user.
CVE-2025-8747	A safe mode bypass vulnerability in the `Model.load_model` method in Keras versions 3.0.0 through 3.10.0 allows an attacker to achieve arbitrary code execution
CVE-2025-8672	MacOS version of GIMP bundles a Python interpreter that inherits the Transparency, Consent, and Control (TCC) permissions granted by the user to the main applic leveraging the application's previously granted TCC permissions to access user's files in privacy-protected folders without triggering user prompts. Accessing other disguising attacker's malicious intent. This issue has been fixed in 3.1.4.2 version of GIMP.
CVE-2025-8862	YugabyteDB has been collecting diagnostics information from YugabyteDB servers, which may include sensitive gflag configurations. To mitigate this, we recomme
CVE-2025-8863	YugabyteDB diagnostic information was transmitted over HTTP, which could expose sensitive data during transmission
CVE-2025-8864	Shared Access Signature token is not masked in the backup configuration response and is also exposed in the yb_backup logs
CVE-2012-10037	PhpTax version 0.8 contains a remote code execution vulnerability in drawimage.php. The pfilez GET parameter is unsafely passed to the exec() function without s context. No authentication is required.
CVE-2012-10038	Auxilium RateMyPet contains an unauthenticated arbitrary file upload vulnerability in upload_banners.php. The banner upload feature fails to validate file types or accessible /banners/ directory and can be executed directly, resulting in remote code execution.
CVE-2012-10039	ZEN Load Balancer versions 2.0 and 3.0-rc1 contain a command injection vulnerability in content2-2.cgi. The filelog parameter is passed directly into a backtick-de code execution as the root user. ZEN Load Balancer is the predecessor of ZEVENET and SKUDONET. The affected versions (2.0 and 3.0-rc1) are no longer supporte
CVE-2012-10040	Openfiler v2.x contains a command injection vulnerability in the system.html page. The device parameter is used to instantiate a NetworkCard object, whose const commands as the openfiler user. Due to misconfigured sudoers, the openfiler user can escalate privileges to root via sudo /bin/bash without a password.
CVE-	

2025-8865	The YugabyteDB tablet server contains a flaw in its YCQL query handling that can trigger a null pointer dereference when processing certain malformed inputs. An
CVE-2025-8866	YugabyteDB Anywhere web server does not properly enforce authentication for the /metamaster/universe API endpoint. An unauthenticated attacker could exploit
CVE-2022-50233	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: eir: Fix using strlen with hdev->{dev_name,short_name} Both dev_name and short_na string needs to be truncated or not.
CVE-2025-54992	OpenKilda is an open-source OpenFlow controller. Prior to version 1.164.0, an XML external entity (XXE) injection vulnerability was found in OpenKilda which in com OpenKilda UI is running. This issue may lead to Information disclosure. This issue has been patched in version 1.164.0.
CVE-2025-55012	Zed is a multiplayer code editor. Prior to version 0.197.3, in the Zed Agent Panel allowed for an AI agent to achieve Remote Code Execution (RCE) by bypassing use specific configuration file, leading to the execution of arbitrary commands on a victim's machine without the explicit approval that would otherwise be required. Th the Agent Panel, or to limit the AI Agent's file system access.
CVE-2025-55156	pyLoad is the free and open-source Download Manager written in pure Python. Prior to version 0.5.0b3.dev91, the parameter add_links in API /json/add_package is has been patched in version 0.5.0b3.dev91.
CVE-2025-55159	slab is a pre-allocated storage for a uniform data type. In version 0.4.10, the get_disjoint_mut method incorrectly checked if indices were within the slab's capacity This has been fixed in slab 0.4.11. A workaround for this issue involves to avoid using get_disjoint_mut with indices that might be beyond the slab's actual length.
CVE-2025-7622	During an internal security assessment, a Server-Side Request Forgery (SSRF) vulnerability that allowed an authenticated attacker to access internal resources on
CVE-2025-8885	Allocation of Resources Without Limits or Throttling vulnerability in Legion of the Bouncy Castle Inc. Bouncy Castle for Java on All (API modules) allows Excessive Al java/blob/main/core/src/main/java/org/bouncycastle/asn1/ASN1ObjectIdentifier.Java. This issue affects Bouncy Castle for Java: from BC 1.0 through 1.77, from BC-FJ
CVE-2025-43736	A Denial Of Service via File Upload (DOS) vulnerability in the Liferay Portal 7.4.3.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.8, 2024.Q4.0 thr 7.4 GA through update 92 allows a user to upload more than 300kb profile picture into the user profile. This size more than the noted max 300kb size. This extra ar
CVE-2025-43735	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2 remote non-authenticated attacker to inject JavaScript into the google_gadget.
CVE-2025-22830	APTIOV contains a vulnerability in BIOS where a skilled user may cause “Race Condition” by local access. A successful exploitation of this vulnerability may lead to
CVE-2025-38500	In the Linux kernel, the following vulnerability has been resolved: xfrm: interface: fix use-after-free after changing collect_md xfrm interface collect_md property or The check to enforce this was done only in the case where the xi was returned from xfrmi_locate() which doesn't look for the collect_md interface, and thus the val >xfrmi hash, but since it also exists in the xfrmi_net->collect_md_xfrmi pointer it would lead to a double free when the net namespace was taken down [1]. Change interfaces. [1] resulting oops: [8.516540] kernel BUG at net/core/dev.c:12029! [8.516552] Oops: invalid opcode: 0000 [#1] SMP NOPTI [8.516559] CPU: 0 UID: 0 I Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [8.516569] Workqueue: netns cleanup_net [8.516579] RIP: 0010:unregister_netd 48 89 32 4c 89 80 78 01 00 00 48 89 b8 80 01 00 00 eb ac 90 <0f> 0b 48 8b 45 00 4c 8d a0 88 fe ff ff 48 39 c5 74 5c 41 80 bc 24 [8.516593] RSP: 0018:ffffa93b8 8.516601] RDX: 0000000000000004 RSI: 0000000000000000 RDI: dead000000000122 [8.516603] RBP: ffffa93b8006bdd8 R08: dead000000000100 R09: ffff98fe ffffffff96c1a510 R14: ffffffff96c1a510 R15: ffffa93b8006be00 [8.516615] FS: 0000000000000000(0000) GS:ffff98fee73b7000(0000) knlGS:0000000000000000 [8. 000000003aa40000 CR4: 0000000000752ef0 [8.516625] PKRU: 55555554 [8.516627] Call Trace: [8.516632] <TASK> [8.516635] ? rtnl_is_locked+0x15/0x20 [cleanup_net+0x1ad/0x2e0 [8.516664] process_one_work+0x160/0x380 [8.516673] worker_thread+0x2aa/0x3c0 [8.516679] ? __pfx_worker_thread+0x10/0x10 [8.516697] ret_from_fork+0x82/0xf0 [8.516705] ? __pfx_kthread+0x10/0x10 [8.516709] ret_from_fork_asm+0x1a/0x30 [8.516718] </TASK>
CVE-2025-3089	ServiceNow has addressed a Broken Access Control vulnerability that was identified in the ServiceNow AI Platform. This vulnerability could allow a low privileged us potentially leading to unauthorized data modifications. This issue is addressed in the listed patches and family releases, which have been made available to hosted
CVE-2025-54800	Hydra is a continuous integration service for Nix based projects. Prior to commit dea1e16, a malicious package can introduce arbitrary JavaScript code into the Hyd by a third-party project as part of its build process. This also happens in other places like with hydra-release-name. This issue has been patched by commit dea1e1
CVE-2025-54864	Hydra is a continuous integration service for Nix based projects. Prior to commit f7bda02, /api/push-github and /api/push-gitea are called by the corresponding forg evaluation can be very taxing on the infrastructure when large evaluations are done, introducing potential denial of service attacks on the host running the evaluat gitea via a reverse proxy.
CVE-2025-55164	content-security-policy-parser parses content security policy directives. A prototype pollution vulnerability exists in versions 0.5.0 and earlier, wherein if a policy na workaround involves disabling prototype method in NodeJS, neutralizing all possible prototype pollution attacks. Provide either --disable-proto=delete (recommend
CVE-2024-58238	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btnxpuart: Resolve TX timeout error in power save stress test This fixes the tx timeout commands coincide with the power save timeout value of 2 seconds. Test procedure using bash script: <load btnxpuart.ko> hciconfig hci0 up //Enable Power Save done Error log, after adding few more debug prints: Bluetooth: btnxpuart_queue_skb(): 01 0A 20 01 00 Bluetooth: hci0: Set UART break: on, status=0 Bluetooth: hc advertise mode on hci0: Connection timed out (110) Bluetooth: hci0: command 0x200a tx timeout When the power save mechanism turns on UART break, and btn >work from being scheduled, which is responsible to turn OFF UART break. This issue is fixed by adding a ps_lock mutex around UART break on/off as well as arour first schedule psdata->work, and then it will reschedule itself once UART break has been turned off and ps_state is PS_STATE_AWAKE. Tested above script for 50,0
CVE-2025-7020	An incorrect encryption implementation vulnerability exists in the system log dump feature of BYD's DiLink 3.0 OS (e.g. in the model ATTO3). An attacker with phys allows the attacker to access and read system logs containing sensitive data, including personally identifiable information (PII) and location data. This vulnerability
CVE-2025-	A command injection vulnerability affects the Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02) during WPA2 configuration. The 'key' parameter is int authentication and can be triggered during wireless setup.

34149	
CVE-2012-10043	A stack-based buffer overflow vulnerability exists in ActFax Server version 4.32, specifically in the "Import Users from File" functionality of the client interface. The during CSV parsing. An attacker can exploit this vulnerability by crafting a malicious .exp file and importing it using the default character set "ECMA-94 / Latin 1 (IS interaction is required to trigger the vulnerability.
CVE-2025-34150	The PPPoE configuration interface of the Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02) is vulnerable to command injection via the 'user' paramete privileges.
CVE-2025-34151	A command injection vulnerability exists in the 'passwd' parameter of the PPPoE setup process on the Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT0 achieve root-level code execution.
CVE-2025-34152	An unauthenticated OS command injection vulnerability exists in the Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02) via the 'time' parameter of the service. Unlike other injection points, this vector allows remote compromise without triggering visible configuration changes.
CVE-2025-54368	uv is a Python package and project manager written in Rust. In versions 0.8.5 and earlier, remote ZIP archives were handled in a streamwise fashion, and file entrie with legitimate contents on some package installers, and malicious contents on others due to multiple local file entries. An attacker could also contrive a "stacked" could choose which installer to target in both scenarios. This issue is fixed in version 0.8.6. To work around this issue, users may choose to set UV_INSECURE_NO_Z
CVE-2025-54793	Astro is a web framework for content-driven websites. In versions 5.2.0 through 5.12.7, there is an Open Redirect vulnerability in the trailing slash redirection logic crafting URLs such as https://mydomain.com//malicious-site.com/. This increases the risk of phishing and other social engineering attacks. This affects sites that us Netlify or Vercel. This issue is fixed in version 5.12.8. To work around this issue at the network level, block outgoing redirect responses with a Location header valu
CVE-2025-54940	An HTML injection vulnerability exists in WordPress plugin "Advanced Custom Fields" prior to 6.4.3. If this vulnerability is exploited, crafted HTML code may be renc
CVE-2025-54958	Powered BLUE 870 versions 0.20130927 and prior contain an OS command injection vulnerability. If this vulnerability is exploited, arbitrary OS commands may be
CVE-2025-54959	Powered BLUE Server versions 0.20130927 and prior contain a path traversal vulnerability. If this vulnerability is exploited, an arbitrary file in the affected product
CVE-2025-8088	A path traversal vulnerability affecting the Windows version of WinRAR allows the attackers to execute arbitrary code by crafting malicious archive files. This vulne
CVE-2025-4576	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.133, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 through 2 through update 92 allows an remote non-authenticated attacker to inject JavaScript into the modules/apps/blogs/blogs-web/src/main/resources/META-INF/resources
CVE-2010-10013	An unauthenticated remote command execution vulnerability exists in AjaXplorer (now known as Pydio Cells) versions prior to 2.6. The flaw resides in the checkIns parameter. By injecting shell metacharacters, remote attackers can execute arbitrary system commands on the server with the privileges of the web server proces
CVE-2012-10036	Project Pier 0.8.8 and earlier contains an unauthenticated arbitrary file upload vulnerability in tools/upload_file.php. The upload handler fails to validate the file type directory. The uploaded file is stored with a predictable suffix and can be executed by requesting its URL, resulting in remote code execution.
CVE-2012-10041	WAN Emulator v2.3 contains two unauthenticated command execution vulnerabilities. The result.php script calls shell_exec() with unsanitized input from the pc PO includes a SUID-root binary named dosu, which is vulnerable to command injection via its first argument. An attacker can exploit both flaws in sequence to achieve
CVE-2012-10042	Sflog! CMS 1.0 contains an authenticated arbitrary file upload vulnerability in the blog management interface. The application ships with default credentials (admir types, enabling attackers to upload a PHP backdoor into a web-accessible directory (blogs/download/uploads/). Once uploaded, the file can be executed remotely, r
CVE-2012-10044	MobileCartly version 1.0 contains an arbitrary file creation vulnerability in the savepage.php script. The application fails to perform authentication or authorization by sending crafted HTTP GET requests to savepage.php, specifying both the filename and content. This allows arbitrary file creation within the pages/ directory or a
CVE-2025-8771	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation sl database configuration established by the user.
CVE-2012-10045	XODA version 0.4.5 contains an unauthenticated file upload vulnerability that allows remote attackers to execute arbitrary PHP code on the server. The flaw resides data POST request, an attacker can upload a .php file directly into the web-accessible files/ directory and trigger its execution via a subsequent GET request.
CVE-2012-10046	The E-Mail Security Virtual Appliance (ESVA) (tested on version ESVA_2057) contains an unauthenticated command injection vulnerability in the learn-msg.cgi scrip shell commands. Exploitation requires no authentication and results in full command execution on the underlying system.
CVE-2012-10047	Cyclope Employee Surveillance Solution versions 6.x is vulnerable to a SQL injection flaw in its login mechanism. The username parameter in the auth-login POST r execute a malicious PHP file on disk, resulting in remote code execution under the SYSTEM user context.
CVE-2012-10048	Zenoss Core 3.x contains a command injection vulnerability in the showDaemonXMLConfig endpoint. The daemon parameter is passed directly to a Popen() call in the zenoss user.
CVE-2012-	WebPageTest version 2.6 and earlier contains an arbitrary file upload vulnerability in the resultimage.php script. The application fails to validate or sanitize user-su

10049	and execute arbitrary PHP code, resulting in full remote code execution under the web server context.
CVE-2012-10050	CuteFlow version 2.11.2 and earlier contains an arbitrary file upload vulnerability in the restart_circulation_values_write.php script. The application fails to validate directory. These files are then accessible via the web server, enabling remote code execution.
CVE-2012-10051	Photodex ProShow Producer version 5.0.3256 contains a stack-based buffer overflow vulnerability in the handling of plugin load list files. When a specially crafted l overflow when the file is parsed during startup. Exploitation requires local access to place the file and user interaction to launch the application.
CVE-2012-10052	EGallery version 1.2 contains an unauthenticated arbitrary file upload vulnerability in the uploadify.php script. The application fails to validate file types or enforce directory. This results in full remote code execution under the web server context.
CVE-2012-10053	Simple Web Server 2.2 rc2 contains a stack-based buffer overflow vulnerability in its handling of the Connection HTTP header. When a remote attacker sends an ov the stack. This flaw allows remote attackers to execute arbitrary code with the privileges of the web server process. The vulnerability is triggered before authentica
CVE-2025-54417	Craft is a platform for creating digital experiences. Versions 4.13.8 through 4.16.2 and 5.5.8 through 5.8.3 contain a vulnerability that can bypass CVE-2025-23209 these requirements: have a compromised security key and create an arbitrary file in Craft's /storage/backups folder. With those criteria in place, attackers could cr fixed in versions 4.16.3 and 5.8.4.
CVE-2025-54888	Fedify is a TypeScript library for building federated server apps powered by ActivityPub. In versions below 1.3.20, 1.4.0-dev.585 through 1.4.12, 1.5.0-dev.636 thro authentication bypass vulnerability allows any unauthenticated attacker to impersonate any ActivityPub actor by sending forged activities signed with their own ke impersonation across all Fedify instances. This is fixed in versions 1.3.20, 1.4.13, 1.5.5, 1.6.8, 1.7.9 and 1.8.5.
CVE-2025-55149	Tiny-Scientist is a lightweight framework for automating the entire lifecycle of scientific research—from ideation to implementation, writing, and review. In versions backend/app.py. The vulnerability allows malicious users to access arbitrary PDF files on the server by providing crafted file paths that bypass the intended securit sensitive documents outside the intended directory and perform reconnaissance on the server's file system structure. This issue does not currently have a fix.
CVE-2025-4581	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 th vulnerability in the portal-settings-authentication-opensso-web due to improper validation of user-supplied URLs. An attacker can exploit this issue to force the serv exploitation.
CVE-2025-4655	SSRF vulnerability in FreeMarker templates in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.5, 2024.Q4.0 through 2024.Q4.7, 92 allows template editors to bypass access validations via crafted URLs.
CVE-2025-8395	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.