SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 31 January 2024

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-2023-52221	Unrestricted Upload of File with Dangerous Type vulnerability in UkrSolution Barcode Scanner and Inventory manager.This issue affects Barcode Scanner and Inventory manager: from n/a through 1.5.1.	10.0	More Details
CVE-2024-23622	A stack-based buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution with SYSTEM privileges.	10.0	More Details
CVE-2024-23621	A buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution.	10.0	More Details
CVE-2024-23616	A buffer overflow vulnerability exists in Symantec Server Management Suite version 7.9 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as SYSTEM.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23615	A buffer overflow vulnerability exists in Symantec Messaging Gateway versions 10.5 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as root.	10.0	More Details
CVE-2024-23614	A buffer overflow vulnerability exists in Symantec Messaging Gateway versions 9.5 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as root.	10.0	More Details
CVE-2024-23613	A buffer overflow vulnerability exists in Symantec Deployment Solution version 7.9 when parsing UpdateComputer tokens. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as SYSTEM.	10.0	More Details
CVE-2024-0402	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.	9.9	More Details
CVE-2024-20253	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.	9.9	More Details
CVE-2024-22862	Integer overflow vulnerability in FFmpeg before n6.1, allows remote attackers to execute arbitrary code via the JJPEG XL Parser.	9.8	More Details
CVE-2023-38317	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the network interface name entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands.	9.8	More Details
CVE-2023-38318	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the gateway FQDN entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands.	9.8	More Details
CVE-2023-38319	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the FAS key entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38323	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the status path script entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands.	9.8	More Details
CVE-2023-52389	UTF32Encoding.cpp in POCO has a Poco::UTF32Encoding integer overflow and resultant stack buffer overflow because Poco::UTF32Encoding::convert() and Poco::UTF32::queryConvert() may return a negative integer if a UTF-32 byte sequence evaluates to a value of 0x80000000 or higher. This is fixed in 1.11.8p2, 1.12.5p2, and 1.13.0.	9.8	More Details
CVE-2024-22860	Integer overflow vulnerability in FFmpeg before n6.1, allows remote attackers to execute arbitrary code via the jpegxl_anim_read_packet component in the JPEG XL Animation decoder.	9.8	More Details
CVE-2024-0808	Integer underflow in WebUI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High)	9.8	More Details
CVE-2024-24329	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setPortForwardRules function.	9.8	More Details
CVE-2024-23739	An issue in Discord for macOS version 0.0.291 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings.	9.8	More Details
CVE-2024-23741	An issue in Hyper on macOS version 3.4.1 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings.	9.8	More Details
CVE-2024-23742	An issue in Loom on macOS version 0.196.1 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. NOTE: the vendor disputes this because it requires local access to a victim's machine.	9.8	More Details
CVE-2024-23740	An issue in Kap for macOS version 3.6.0 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings.	9.8	More Details
CVE-2024-1015	Remote command execution vulnerability in SE-elektronic GmbH E-DDC3.3 affecting versions 03.07.03 and higher. An attacker could send different commands from the operating system to the system via the web configuration functionality of the device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23827	Nginx-UI is a web interface to manage Nginx configurations. The Import Certificate feature allows arbitrary write into the system. The feature does not check if the provided user input is a certification/key and allows to write into arbitrary paths in the system. It's possible to leverage the vulnerability into a remote code execution overwriting the config file app.ini. Version 2.0.0.beta.12 fixed the issue.	9.8	More Details
CVE-2024-24328	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setMacFilterRules function.	9.8	More Details
CVE-2023-51840	DoraCMS 2.1.8 is vulnerable to Use of Hard-coded Cryptographic Key.	9.8	More Details
CVE-2024-24141	Sourcecodester School Task Manager App 1.0 allows SQL Injection via the 'task' parameter.	9.8	More Details
CVE-2023-51837	Ylianst MeshCentral 1.1.16 is vulnerable to Missing SSL Certificate Validation.	9.8	More Details
CVE-2023-51982	CrateDB 5.5.1 is contains an authentication bypass vulnerability in the Admin UI component. After configuring password authentication and_ Local_ In the case of an address, identity authentication can be bypassed by setting the X-Real IP request header to a specific value and accessing the Admin UI directly using the default user identity. (https://github.com/crate/crate/issues/15231)	9.8	More Details
CVE-2023-6943	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Mitsubishi Electric Corporation EZSocket versions 3.0 and later, GT Designer3 Version1(GOT1000) all versions, GT Designer3 Version1(GOT2000) all versions, GX Works2 versions 1.11M and later, GX Works3 versions 1.106L and prior, MELSOFT Navigator versions 1.04E and later, MT Works2 all versions, MX Component versions 4.00A and later and MX OPC Server DA/UA all versions allows a remote unauthenticated attacker to execute a malicious code by RPC with a path to a malicious library while connected to the products.	9.8	More Details
CVE-2024-24324	TOTOLINK A8000RU v7.1cu.643_B20200521 was discovered to contain a hardcoded password for root stored in /etc/shadow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24325	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setParentalRules function.	9.8	More Details
CVE-2024-23738	An issue in Postman version 10.22 and before on macOS allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. NOTE: the vendor states "we dispute the report's accuracy ... the configuration does not enable remote code execution.."	9.8	More Details
CVE-2024-24331	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setWiFiScheduleCfg function.	9.8	More Details
CVE-2023-33759	SpliceCom Maximiser Soft PBX v1.5 and before does not restrict excessive authentication attempts, allowing attackers to bypass authentication via a brute force attack.	9.8	More Details
CVE-2024-24330	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the port or enable parameter in the setRemoteCfg function.	9.8	More Details
CVE-2024-22651	There is a command injection vulnerability in the ssdpcgi_main function of cgibin binary in D-Link DIR-815 router firmware v1.04.	9.8	More Details
CVE-2023-51885	Buffer Overflow vulnerability in Mathtex v.1.05 and before allows a remote attacker to execute arbitrary code via the length of the LaTeX string component.	9.8	More Details
CVE-2023-51887	Command Injection vulnerability in Mathtex v.1.05 and before allows a remote attacker to execute arbitrary code via crafted string in application URL.	9.8	More Details
CVE-2024-24333	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the desc parameter in the setWiFiAclRules function.	9.8	More Details
CVE-2021-42144	Buffer over-read vulnerability in Contiki-NG tinyDTLS through master branch 53a0d97 allows attackers obtain sensitive information via crafted input to dtls_ccm_decrypt_message().	9.8	More Details
CVE-2023-51889	Stack Overflow vulnerability in the validate() function in Mathtex v.1.05 and before allows a remote attacker to execute arbitrary code via crafted string in the application URL.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52038	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_415C80 function.	9.8	More Details
CVE-2023-52039	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_415AA4 function.	9.8	More Details
CVE-2023-52040	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_41284C function.	9.8	More Details
CVE-2024-23897	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.	9.8	More Details
CVE-2024-24332	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the url parameter in the setUrlFilterRules function.	9.8	More Details
CVE-2024-22751	D-Link DIR-882 DIR882A1_FW130B06 was discovered to contain a stack overflow via the sub_477AA0 function.	9.8	More Details
CVE-2024-24326	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the arpEnable parameter in the setStaticDhcpRules function.	9.8	More Details
CVE-2024-22729	NETIS SYSTEMS MW5360 V1.0.1.3031 was discovered to contain a command injection vulnerability via the password parameter on the login page.	9.8	More Details
CVE-2024-22529	TOTOLINK X2000R_V2 V2.0.0-B20230727.10434 has a command injection vulnerability in the sub_449040 (handle function of formUploadFile) of /bin/boa.	9.8	More Details
CVE-2023-7227	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges.	9.8	More Details
CVE-2024-22638	liveSite v2019.1 was discovered to contain a remote code execution (RCE) vulenrabiity via the component /livesite/edit_designer_region.php or /livesite/add_email_campaign.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22922	An issue in Projectworlds Vistor Management Systemin PHP v.1.0 allows a remtoe attacker to escalate privileges via a crafted script to the login page in the POST/index.php	9.8	More Details
CVE-2024-23619	A hardcoded credential vulnerability exists in IBM Merge Healthcare eFilm Workstation. A remote, unauthenticated attacker can exploit this vulnerability to achieve information disclosure or remote code execution.	9.8	More Details
CVE-2024-24327	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the pppoePass parameter in the setIpv6Cfg function.	9.8	More Details
CVE-2024-23617	A buffer overflow vulnerability exists in Symantec Data Loss Prevention version 14.0.2 and before. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a crafted document to achieve code execution.	9.6	More Details
CVE-2024-23618	An arbitrary code execution vulnerability exists in Arris SURFboard SGB6950AC2 devices. An unauthenticated attacker can exploit this vulnerability to achieve code execution as root.	9.6	More Details
CVE-2024-23624	A command injection vulnerability exists in the gena.cgi module of D-Link DAP-1650 devices. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root.	9.6	More Details
CVE-2024-23625	A command injection vulnerability exists in D-Link DAP-1650 devices when handling UPnP SUBSCRIBE messages. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root.	9.6	More Details
CVE-2024-21326	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	9.6	More Details
CVE-2024-23629	An authentication bypass vulnerability exists in the web component of the Motorola MR2600. An attacker can exploit this vulnerability to access protected URLs and retrieve sensitive information.	9.6	More Details
CVE-2023-5389	An attacker could potentially exploit this vulnerability, leading to the ability to modify files on Honeywell Experion ControlEdge VirtualUOC and ControlEdge UOC . This exploit could be used to write a file that may result in unexpected behavior based on configuration changes or updating of files that could result in subsequent execution of a malicious application if triggered. Honeywell recommends updating to the most recent version of the product. See Honeywell Security Notification for recommendations on upgrading and versioning.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51839	DeviceFarmer stf v3.6.6 suffers from Use of a Broken or Risky Cryptographic Algorithm.	9.1	More Details
CVE-2021-42147	Buffer over-read vulnerability in the dtls_sha256_update function in Contiki-NG tinyDTLS through master branch 53a0d97 allows remote attackers to cause a denial of service via crafted data packet.	9.1	More Details
CVE-2021-42143	An issue was discovered in Contiki-NG tinyDTLS through master branch 53a0d97. An infinite loop bug exists during the handling of a ClientHello handshake message. This bug allows remote attackers to cause a denial of service by sending a malformed ClientHello handshake message with an odd length of cipher suites, which triggers an infinite loop (consuming all resources) and a buffer over-read that can disclose sensitive information.	9.1	More Details
CVE-2024-23628	A command injection vulnerability exists in the 'SaveStaticRouteIPv6Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	9.0	More Details
CVE-2024-23627	A command injection vulnerability exists in the 'SaveStaticRouteIPv4Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	9.0	More Details
CVE-2024-23626	A command injection vulnerability exists in the ‘SaveSysLogParams’ parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	9.0	More Details
CVE-2024-23630	An arbitrary firmware upload vulnerability exists in the Motorola MR2600. An attacker can exploit this vulnerability to achieve code execution on the device. Authentication is required, however can be bypassed.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2024-21620	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.	8.8	More Details
CVE-2024-23828	Nginx-UI is a web interface to manage Nginx configurations. It is vulnerable to an authenticated arbitrary command execution via CRLF attack when changing the value of test_config_cmd or start_cmd. This vulnerability exists due to an incomplete fix for CVE-2024-22197 and CVE-2024-22198. This vulnerability has been patched in version 2.0.0.beta.12.	8.8	More Details
CVE-2023-6946	The Autotitle for WordPress plugin through 1.0.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	8.8	More Details
CVE-2024-0919	A vulnerability was found in TRENDnet TEW-815DAP 1.0.2.0. It has been classified as critical. This affects the function do_setNTP of the component POST Request Handler. The manipulation of the argument NtpDstStart/NtpDstEnd leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-43317	An issue in Coign CRM Portal v.06.06 allows a remote attacker to escalate privileges via the userPermissionsList parameter in Session Storage component.	8.8	More Details
CVE-2024-21649	The vantage6 technology enables to manage and deploy privacy enhancing technologies like Federated Learning (FL) and Multi-Party Computation (MPC). Prior to 4.2.0, authenticated users could inject code into algorithm environment variables, resulting in remote code execution. This vulnerability is patched in 4.2.0.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23648	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. The password reset functionality sends to the the user requesting a password change an email containing an URL to reset its password. The URL sent contains a unique token, valid during 24 hours, allowing the user to reset its password. This token is highly sensitive ; as an attacker able to retrieve it would be able to resets the user's password. Prior to version 1.2.3, the reset-password URL is crafted using the "Host" HTTP header of the request sent to request a password reset. This way, an external attacker could send password requests for users, but specify a "Host" header of a website that they control. If the user receiving the mail clicks on the link, the attacker would retrieve the reset token of the victim and perform account takeover. Version 1.2.3 fixes this issue.	8.8	More Details
CVE-2024-22636	PluXml Blog v5.8.9 was discovered to contain a remote code execution (RCE) vulnerability in the Static Pages feature. This vulnerability is exploited via injecting a crafted payload into the Content field.	8.8	More Details
CVE-2024-23620	An improper privilege management vulnerability exists in IBM Merge Healthcare eFilm Workstation. A local, authenticated attacker can exploit this vulnerability to escalate privileges to SYSTEM.	8.8	More Details
CVE-2023-6391	The Custom User CSS WordPress plugin through 0.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	8.8	More Details
CVE-2023-5378	Improper Input Validation vulnerability in MegaBIP and already unsupported SmodBIP software allows for Stored XSS.This issue affects SmodBIP in all versions and MegaBIP in versions up to 4.36.2. MegaBIP 5.08 was tested and is not vulnerable. A precise range of vulnerable versions remains unknown.	8.8	More Details
CVE-2023-52251	An issue discovered in provectus kafka-ui 0.4.0 through 0.7.1 allows remote attackers to execute arbitrary code via the q parameter of /api/clusters/local/topics/{topic}/messages.	8.8	More Details
CVE-2023-6390	The WordPress Users WordPress plugin through 1.4 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	8.8	More Details
CVE-2024-23646	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. The application allows users to create zip files from available files on the site. In the 1.x branch prior to version 1.3.2, parameter `selectedIds` is susceptible to SQL Injection. Any backend user with very basic permissions can execute arbitrary SQL statements and thus alter any data or escalate their privileges to at least admin level. Version 1.3.2 contains a fix for this issue.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23898	Jenkins 2.217 through 2.441 (both inclusive), LTS 2.222.1 through 2.426.2 (both inclusive) does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller.	8.8	More Details
CVE-2024-0813	Use after free in Reading Mode in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-0812	Inappropriate implementation in Accessibility in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-1059	Use after free in Peer Connection in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-1060	Use after free in Canvas in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-1077	Use after free in Network in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High)	8.8	More Details
CVE-2024-0807	Use after free in Web Audio in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-0806	Use after free in Passwords in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-7074	The WP SOCIAL BOOKMARK MENU WordPress plugin through 1.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	8.8	More Details
CVE-2024-22309	Deserialization of Untrusted Data vulnerability in QuantumCloud ChatBot with AI.This issue affects ChatBot with AI: from n/a through 5.1.0.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22284	Deserialization of Untrusted Data vulnerability in Thomas Belser Asgaros Forum.This issue affects Asgaros Forum: from n/a through 2.7.2.	8.7	More Details
CVE-2024-1061	The 'HTML5 Video Player' WordPress Plugin, version < 2.5.25 is affected by an unauthenticated SQL injection vulnerability in the 'id' parameter in the 'get_view' function.	8.6	More Details
CVE-2024-1019	ModSecurity / libModSecurity 3.0.0 to 3.0.11 is affected by a WAF bypass for path-based payloads submitted via specially crafted request URLs. ModSecurity v3 decodes percent-encoded characters present in request URLs before it separates the URL path component from the optional query string component. This results in an impedance mismatch versus RFC compliant back-end applications. The vulnerability hides an attack payload in the path component of the URL from WAF rules inspecting it. A back-end may be vulnerable if it uses the path component of request URLs to construct queries. Integrators and users are advised to upgrade to 3.0.12. The ModSecurity v2 release line is not affected by this vulnerability.	8.6	More Details
CVE-2023-6267	A flaw was found in the json payload. If annotation based security is used to secure a REST resource, the JSON body that the resource may consume is being processed (deserialized) prior to the security constraints being evaluated and applied. This does not happen with configuration based security.	8.6	More Details
CVE-2023-52076	Atril Document Viewer is the default document reader of the MATE desktop environment for Linux. A path traversal and arbitrary file write vulnerability exists in versions of Atril prior to 1.26.2. This vulnerability is capable of writing arbitrary files anywhere on the filesystem to which the user opening a crafted document has access. The only limitation is that this vulnerability cannot be exploited to overwrite existing files, but that doesn't stop an attacker from achieving Remote Command Execution on the target system. Version 1.26.2 of Atril contains a patch for this vulnerability.	8.5	More Details
CVE-2024-22283	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Delhivery Delhivery Logistics Courier.This issue affects Delhivery Logistics Courier: from n/a through 1.0.107.	8.5	More Details
CVE-2023-1705	Missing Authorization vulnerability in Forcepoint FlOne SmartEdge Agent on Windows (bgAutoinstaller service modules) allows Privilege Escalation, Functionality Bypass.This issue affects FlOne SmartEdge Agent: before 1.7.0.230330-554.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40547	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. This flaw is only exploitable during the early boot phase, an attacker needs to perform a Man-in-the-Middle or compromise the boot server to be able to exploit this vulnerability successfully.	8.3	More Details
CVE-2024-21385	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2024-23876	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurecreate.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23881	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23880	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23877	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencycreate.php, in the currencyid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23879	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statemodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2023-51843	react-dashboard 1.4.0 is vulnerable to Cross Site Scripting (XSS) as httpOnly is not set.	8.2	More Details
CVE-2024-23861	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/unitofmeasurementcreate.php, in the unitofmeasurementid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23878	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnprint.php, in the grnno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23883	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructuremodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23870	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancelist.php, in the delete parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23875	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancedisplay.php, in the issuanceno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23874	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/companymodify.php, in the address1 parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23873	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencymodify.php, in the currencyid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23872	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/locationmodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23871	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/unitofmeasurementmodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23869	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuanceprint.php, in the issuanceno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23855	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodemodify.php, in multiple parameters. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23868	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnlist.php, in the deleted parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23867	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statecreate.php, in the stateid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23866	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrycreate.php, in the countryid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23865	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23862	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grndisplay.php, in the grnno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23863	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructuredisplay.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23860	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencylist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23864	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrylist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23890	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itempopup.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23885	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrymodify.php, in the countryid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23893	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/costcentermodify.php, in the costcenterid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23889	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemgroupcreate.php, in the itemgroupid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-24558	TanStack Query supplies asynchronous state management, server-state utilities and data fetching for the web. The `@tanstack/react-query-next-experimental` NPM package is vulnerable to a cross-site scripting vulnerability. To exploit this, an attacker would need to either inject malicious input or arrange to have malicious input be returned from an endpoint. To fix this issue, please update to version 5.18.0 or later.	8.2	More Details
CVE-2023-46230	In Splunk Add-on Builder versions below 4.1.4, the app writes sensitive information to internal log files.	8.2	More Details
CVE-2024-23894	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancecreate.php, in the issuancedate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23888	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stocktransactionslist.php, in the itemidy parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23887	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grncreate.php, in the grndate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23886	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemmodify.php, in the bincardinfo parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23891	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemcreate.php, in the itemid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23892	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/costcentercreate.php, in the costcenterid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23856	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemlist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23884	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnmodify.php, in the grndate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23896	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stock.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23841	apollo-client-nextjs is the Apollo Client support for the Next.js App Router. The @apollo/experimental-apollo-client-nextjs NPM package is vulnerable to a cross-site scripting vulnerability. To exploit this vulnerability, an attacker would need to either inject malicious input (e.g. by redirecting a user to a specifically-crafted link) or arrange to have malicious input be returned by a GraphQL server (e.g. by persisting it in a database). To fix this issue, please update to version 0.7.0 or later.	8.2	More Details
CVE-2024-23857	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnlinecreate.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23882	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodecreate.php, in the taxcodeid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23858	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancelinecreate.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details
CVE-2024-23859	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurelinecreate.php, in the flatamount parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6258	A security vulnerability has been identified in the pkcs11-provider, which is associated with Public-Key Cryptography Standards (PKCS#11). If exploited successfully, this vulnerability could result in a Bleichenbacher-like security flaw, potentially enabling a side-channel attack on PKCS#1 1.5 decryption.	8.1	More Details
CVE-2024-0212	The Cloudflare Wordpress plugin was found to be vulnerable to improper authentication. The vulnerability enables attackers with a lower privileged account to access data from the Cloudflare API.	8.1	More Details
CVE-2023-51833	A command injection issue in TRENDnet TEW-411BRPplus v.2.07_eu that allows a local attacker to execute arbitrary code via the data1 parameter in the debug.cgi page.	8.1	More Details
CVE-2024-22135	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Order Export & Order Import for WooCommerce.This issue affects Order Export & Order Import for WooCommerce: from n/a through 2.4.3.	8.0	More Details
CVE-2024-22152	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Product Import Export for WooCommerce.This issue affects Product Import Export for WooCommerce: from n/a through 2.3.7.	8.0	More Details
CVE-2024-21840	Incorrect Default Permissions vulnerability in Hitachi Storage Plug-in for VMware vCenter allows local users to read and write specific files. This issue affects Hitachi Storage Plug-in for VMware vCenter: from 04.0.0 through 04.9.2.	7.9	More Details
CVE-2024-22938	Insecure Permissions vulnerability in BossCMS v.1.3.0 allows a local attacker to execute arbitrary code and escalate privileges via the init function in admin.class.php component.	7.8	More Details
CVE-2022-48622	In GNOME GdkPixbuf (aka gdk-pixbuf) through 2.42.10, the ANI (Windows animated cursor) decoder encounters heap memory corruption (in ani_load_chunk in io-ani.c) when parsing chunks in a crafted .ani file. A crafted file could allow an attacker to overwrite heap metadata, leading to a denial of service or code execution attack. This occurs in gdk_pixbuf_set_option() in gdk-pixbuf.c.	7.8	More Details
CVE-2024-23940	Trend Micro uiAirSupport, included in the Trend Micro Security 2023 family of consumer products, version 6.0.2092 and below is vulnerable to a DLL hijacking/proxying vulnerability, which if exploited could allow an attacker to impersonate and modify a library to execute code on the system and ultimately escalate privileges on an affected system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51711	An issue was discovered in Regify Regipay Client for Windows version 4.5.1.0 allows DLL hijacking: a user can trigger the execution of arbitrary code every time the product is executed.	7.8	More Details
CVE-2024-22545	An issue was discovered in TRENDnet TEW-824DRU version 1.04b01, allows unauthenticated attackers to execute arbitrary code via the system.ntp.server parameter in the sub_420AE0() function. The attack can be launched remotely.	7.8	More Details
CVE-2024-22432	Networker 19.9 and all prior versions contains a Plain-text Password stored in temporary config file during backup duration in NMDA MySQL Database backups. User has low privilege access to Networker Client system could potentially exploit this vulnerability, leading to the disclosure of configured MySQL Database user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application Database with privileges of the compromised account.	7.8	More Details
CVE-2023-3181	The C:\Program Files (x86)\Splashtop\Splashtop Software Updater\uninst.exe process creates a folder at C:\Windows\Temp~nsu.tmp and copies itself to it as Au_.exe. The C:\Windows\Temp~nsu.tmp\Au_.exe file is automatically launched as SYSTEM when the system reboots or when a standard user runs an MSI repair using Splashtop Streamer's Windows Installer. Since the C:\Windows\Temp~nsu.tmp folder inherits permissions from C:\Windows\Temp and Au_.exe is susceptible to DLL hijacking, standard users can write a malicious DLL to it and elevate their privileges.	7.8	More Details
CVE-2024-22749	GPAC v2.3 was detected to contain a buffer overflow via the function gf_isom_new_generic_sample_description function in the isomedia/isom_write.c:4577	7.8	More Details
CVE-2024-23506	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in InstaWP Team InstaWP Connect – 1-click WP Staging & Migration.This issue affects InstaWP Connect – 1-click WP Staging & Migration: from n/a through 0.1.0.9.	7.7	More Details
CVE-2024-21985	ONTAP 9 versions prior to 9.9.1P18, 9.10.1P16, 9.11.1P13, 9.12.1P10 and 9.13.1P4 are susceptible to a vulnerability which could allow an authenticated user with multiple remote accounts with differing roles to perform actions via REST API beyond their intended privilege. Possible actions include viewing limited configuration details and metrics or modifying limited settings, some of which could result in a Denial of Service (DoS).	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22147	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Overnight PDF Invoices & Packing Slips for WooCommerce.This issue affects PDF Invoices & Packing Slips for WooCommerce: from n/a through 3.7.5.	7.6	More Details
CVE-2023-6919	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C.	7.5	More Details
CVE-2024-23747	The Moderna Sistemas ModernaNet Hospital Management System 2024 is susceptible to an Insecure Direct Object Reference (IDOR) vulnerability. This vulnerability resides in the system's handling of user data access through a /Modernanet/LAUDO/LAU0000100/Laudo?id= URI. By manipulating this id parameter, an attacker can gain access to sensitive medical information.	7.5	More Details
CVE-2023-7204	The WP STAGING WordPress Backup plugin before 3.2.0 allows access to cache files during the cloning process which provides	7.5	More Details
CVE-2024-24736	The POP3 service in YahooPOPs (aka YPOPs!) 1.6 allows a remote denial of service (reboot) via a long string to TCP port 110, a related issue to CVE-2004-1558.	7.5	More Details
CVE-2023-6200	A race condition was found in the Linux Kernel. Under certain conditions, an unauthenticated attacker from an adjacent network could send an ICMPv6 router advertisement packet, causing arbitrary code execution.	7.5	More Details
CVE-2023-46838	Transmit requests in Xen's virtual network protocol can consist of multiple parts. While not really useful, except for the initial part any of them may be of zero length, i.e. carry no data at all. Besides a certain initial portion of the to be transferred data, these parts are directly translated into what Linux calls SKB fragments. Such converted request parts can, when for a particular SKB they are all of length zero, lead to a de-reference of NULL in core networking code.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29055	In Apache Kylin version 2.0.0 to 4.0.3, there is a Server Config web interface that displays the content of file 'kylin.properties', that may contain serverside credentials. When the kylin service runs over HTTP (or other plain text protocol), it is possible for network sniffers to hijack the HTTP payload and get access to the content of kylin.properties and potentially the containing credentials. To avoid this threat, users are recommended to * Always turn on HTTPS so that network payload is encrypted. * Avoid putting credentials in kylin.properties, or at least not in plain text. * Use network firewalls to protect the serverside such that it is not accessible to external attackers. * Upgrade to version Apache Kylin 4.0.4, which filters out the sensitive content that goes to the Server Config web interface.	7.5	More Details
CVE-2024-23656	Dex is an identity service that uses OpenID Connect to drive authentication for other apps. Dex 2.37.0 serves HTTPS with insecure TLS 1.0 and TLS 1.1. `cmd/dex/serve.go` line 425 seemingly sets TLS 1.2 as minimum version, but the whole `tlsConfig` is ignored after `TLS cert reloader` was introduced in v2.37.0. Configured cipher suites are not respected either. This issue is fixed in Dex 2.38.0.	7.5	More Details
CVE-2024-0804	Insufficient policy enforcement in iOS Security UI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2021-42145	An assertion failure discovered in in check_certificate_request() in Contiki-NG tinyDTLS through master branch 53a0d97 allows attackers to cause a denial of service.	7.5	More Details
CVE-2024-23655	Tuta is an encrypted email service. Starting in version 3.118.12 and prior to version 3.119.10, an attacker is able to send a manipulated email so that the user can no longer use the app to get access to received emails. By sending a manipulated email, an attacker could put the app into an unusable state. In this case, a user can no longer access received e-mails. Since the vulnerability affects not only the app, but also the web application, a user in this case has no way to access received emails. This issue was tested with iOS and the web app, but it is possible all clients are affected. Version 3.119.10 fixes this issue.	7.5	More Details
CVE-2023-51890	An infinite loop issue discovered in Mathtex 1.05 and before allows a remote attackers to consume CPU resources via crafted string in the application URL.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23838	TrueLayer.NET is the .Net client for TrueLayer. The vulnerability could potentially allow a malicious actor to gain control over the destination URL of the HttpClient used in the API classes. For applications using the SDK, requests to unexpected resources on local networks or to the internet could be made which could lead to information disclosure. The issue can be mitigated by having strict egress rules limiting the destinations to which requests can be made, and applying strict validation to any user input passed to the `truelayer-dotnet` library. Versions of TrueLayer.Client `v1.6.0` and later are not affected.	7.5	More Details
CVE-2024-22861	Integer overflow vulnerability in FFmpeg before n6.1, allows attackers to cause a denial of service (DoS) via the avcodec/osq module.	7.5	More Details
CVE-2024-22523	Directory Traversal vulnerability in Qiyu iFair version 23.8_ad0 and before, allows remote attackers to obtain sensitive information via uploadimage component.	7.5	More Details
CVE-2023-6942	Missing Authentication for Critical Function vulnerability in Mitsubishi Electric Corporation EZSocket versions 3.0 and later, GT Designer3 Version1(GOT1000) all versions, GT Designer3 Version1(GOT2000) all versions, GX Works2 versions 1.11M and later, GX Works3 versions 1.106L and prior, MELSOFT Navigator versions 1.04E and later, MT Works2 all versions, MX Component versions 4.00A and later and MX OPC Server DA/UA all versions allows a remote unauthenticated attacker to bypass authentication by sending specially crafted packets and connect to the products illegally.	7.5	More Details
CVE-2023-36260	An issue was discovered in the Feed Me plugin 4.6.1 for Craft CMS. It allows remote attackers to cause a denial of service (DoS) via crafted strings to Feed-Me Name and Feed-Me URL fields, due to saving a feed using an Asset element type with no volume selected. NOTE: this is not a report about code provided by the Craft CMS product; it is only a report about the Feed Me plugin. NOTE: a third-party report states that commit b5d6ede51848349bd91bc95fec288b6793f15e28 has "nothing to do with security."	7.5	More Details
CVE-2023-50943	Apache Airflow, versions before 2.8.1, have a vulnerability that allows a potential attacker to poison the XCom data by bypassing the protection of "enable_xcom_pickling=False" configuration setting resulting in poisoned data after XCom deserialization. This vulnerability is considered low since it requires a DAG author to exploit it. Users are recommended to upgrade to version 2.8.1 or later, which fixes this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22154	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in SNP Digital SalesKing.This issue affects SalesKing: from n/a through 1.6.15.	7.5	More Details
CVE-2023-52356	A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service.	7.5	More Details
CVE-2024-23641	SvelteKit is a web development kit. In SvelteKit 2, sending a GET request with a body eg `{}` to a built and previewed/hosted sveltekit app throws `Request with GET/HEAD method cannot have body.` and crashes the preview/hosting. After this happens, one must manually restart the app. `TRACE` requests will also cause the app to crash. Prerendered pages and SvelteKit 1 apps are not affected. `@sveltejs/adapter-node` versions 2.1.2, 3.0.3, and 4.0.1 and `@sveltejs/kit` version 2.4.3 contain a patch for this issue.	7.5	More Details
CVE-2023-51888	Buffer Overflow vulnerability in the nomath() function in Mathtex v.1.05 and before allows a remote attacker to cause a denial of service via a crafted string in the application URL.	7.5	More Details
CVE-2023-51886	Buffer Overflow vulnerability in the main() function in Mathtex 1.05 and before allows a remote attacker to cause a denial of service when using \convertpath.	7.5	More Details
CVE-2024-23904	Jenkins Log Command Plugin 1.0.2 and earlier does not disable a feature of its command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read content from arbitrary files on the Jenkins controller file system.	7.5	More Details
CVE-2021-42146	An issue was discovered in Contiki-NG tinyDTLS through master branch 53a0d97. DTLS servers allow remote attackers to reuse the same epoch number within two times the TCP maximum segment lifetime, which is prohibited in RFC6347. This vulnerability allows remote attackers to obtain sensitive application (data of connected clients).	7.5	More Details
CVE-2023-4550	Improper Input Validation, Files or Directories Accessible to External Parties vulnerability in OpenText AppBuilder on Windows, Linux allows Probe System Files. An unauthenticated or authenticated user can abuse a page of AppBuilder to read arbitrary files on the server on which it is hosted. This issue affects AppBuilder: from 21.2 before 23.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23985	EzServer 6.4.017 allows a denial of service (daemon crash) via a long string, such as one for the RNTO command.	7.5	More Details
CVE-2023-51842	An algorithm-downgrade issue was discovered in Ylianst MeshCentral 1.1.16.	7.5	More Details
CVE-2023-52355	An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFRasterScanlineSize64() API. This flaw allows a remote attacker to cause a denial of service via a crafted input with a size smaller than 379 KB.	7.5	More Details
CVE-2024-23649	Lemmy is a link aggregator and forum for the fediverse. Starting in version 0.17.0 and prior to version 0.19.1, users can report private messages, even when they're neither sender nor recipient of the message. The API response to creating a private message report contains the private message itself, which means any user can just iterate over message ids to (loudly) obtain all private messages of an instance. A user with instance admin privileges can also abuse this if the private message is removed from the response, as they're able to see the resulting reports. Creating a private message report by POSTing to `/api/v3/private_message/report` does not validate whether the reporter is the recipient of the message. lemmy-ui does not allow the sender to report the message; the API method should likely be restricted to accessible to recipients only. The API response when creating a report contains the `private_message_report_view` with all the details of the report, including the private message that has been reported: Any authenticated user can obtain arbitrary (untargeted) private message contents. Privileges required depend on the instance configuration; when registrations are enabled without application system, the privileges required are practically none. When registration applications are required, privileges required could be considered low, but this assessment heavily varies by instance. Version 0.19.1 contains a patch for this issue. A workaround is available. If an update to a fixed Lemmy version is not immediately possible, the API route can be blocked in the reverse proxy. This will prevent anyone from reporting private messages, but it will also prevent exploitation before the update has been applied.	7.5	More Details
CVE-2024-0822	An authentication bypass vulnerability was found in overt-engine. This flaw allows the creation of users in the system without authentication due to a flaw in the CreateUserSession command.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40548	A buffer overflow was found in Shim in the 32-bit system. The overflow happens due to an addition operation involving a user-controlled value parsed from the PE binary being used by Shim. This value is further used for memory allocation operations, leading to a heap-based buffer overflow. This flaw causes memory corruption and can lead to a crash or data integrity issues during the boot phase.	7.4	More Details
CVE-2024-1035	A vulnerability has been found in openBI up to 1.0.8 and classified as critical. This vulnerability affects the function uploadIcon of the file /application/index/controller/Icon.php. The manipulation of the argument image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252310 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-0945	A vulnerability classified as critical has been found in 60IndexPage up to 1.8.5. This affects an unknown part of the file /include/file.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252189 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-0946	A vulnerability classified as critical was found in 60IndexPage up to 1.8.5. This vulnerability affects unknown code of the file /apply/index.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252190 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-1036	A vulnerability was found in openBI up to 1.0.8 and classified as critical. This issue affects the function uploadIcon of the file /application/index/controller/Screen.php of the component Icon Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252311.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1006	A vulnerability was found in Shanxi Diankeyun Technology NODERP up to 6.0.2 and classified as critical. This issue affects some unknown processing of the file application/index/common.php of the component Cookie Handler. The manipulation of the argument Nod_User_Id/Nod_User_Token leads to improper authentication. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252275. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-1009	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Admin/login.php. The manipulation of the argument txtusername leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252278 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-1034	A vulnerability, which was classified as critical, was found in openBI up to 1.0.8. This affects the function uploadFile of the file /application/index/controller/File.php. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252309 was assigned to this vulnerability.	7.3	More Details
CVE-2024-1032	A vulnerability classified as critical was found in openBI up to 1.0.8. Affected by this vulnerability is the function testConnection of the file /application/index/controller/Databasesource.php of the component Test Connection Handler. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252307.	7.3	More Details
CVE-2024-21488	Versions of the package network before 0.7.0 are vulnerable to Arbitrary Command Injection due to use of the child_process exec function without input sanitization. If (attacker-controlled) user input is given to the mac_address_for function of the package, it is possible for the attacker to execute arbitrary commands on the operating system that this package is being run on.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0918	A vulnerability was found in TRENDnet TEW-800MB 1.0.1.0 and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument DeviceURL leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252122 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0920	A vulnerability was found in TRENDnet TEW-822DRE 1.03B02. It has been declared as critical. This vulnerability affects unknown code of the file /admin_ping.htm of the component POST Request Handler. The manipulation of the argument ipv4_ping/ipv6_ping leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0991	A vulnerability has been found in Tenda i6 1.0.0.9(3857) and classified as critical. This vulnerability affects the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 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 identifier of this vulnerability is VDB-252256. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0990	A vulnerability, which was classified as critical, was found in Tenda i6 1.0.0.9(3857). This affects the function formSetAutoPing of the file /goform/setAutoPing of the component httpd. The manipulation of the argument ping1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252255. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-1004	A vulnerability, which was classified as critical, was found in Totolink N200RE 9.3.5u.6139_B20201216. This affects the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252273 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0992	A vulnerability was found in Tenda i6 1.0.0.9(3857) and classified as critical. This issue affects the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252257 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-1000	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been rated as critical. This issue affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252269 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-24139	Sourcecodester Login System with Email Verification 1.0 allows SQL Injection via the 'user' parameter.	7.2	More Details
CVE-2023-4551	Improper Input Validation vulnerability in OpenText AppBuilder on Windows, Linux allows OS Command Injection. The AppBuilder's Scheduler functionality that facilitates creation of scheduled tasks is vulnerable to command injection. This allows authenticated users to inject arbitrary operating system commands into the executing process. This issue affects AppBuilder: from 21.2 before 23.2.	7.2	More Details
CVE-2023-24676	An issue found in ProcessWire 3.0.210 allows attackers to execute arbitrary code and install a reverse shell via the download_zip_url parameter when installing a new module. NOTE: this is disputed because exploitation requires that the attacker is able to enter requests as an admin; however, a ProcessWire admin is intentionally allowed to install any module that contains any arbitrary code.	7.2	More Details
CVE-2024-0993	A vulnerability was found in Tenda i6 1.0.0.9(3857). It has been classified as critical. Affected is the function formWifiMacFilterGet of the file /goform/WifiMacFilterGet of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-252258 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31037	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS.	7.2	More Details
CVE-2024-1003	A vulnerability, which was classified as critical, has been found in Totolink N200RE 9.3.5u.6139_B20201216. Affected by this issue is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument lang leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252272. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-24399	An arbitrary file upload vulnerability in LEPTON v7.0.0 allows authenticated attackers to execute arbitrary PHP code by uploading this code to the backend/languages/index.php languages area.	7.2	More Details
CVE-2024-1002	A vulnerability classified as critical was found in Totolink N200RE 9.3.5u.6139_B20201216. Affected by this vulnerability is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ePort leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252271. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2023-49038	Command injection in the ping utility on Buffalo LS210D 1.78-0.03 allows a remote authenticated attacker to inject arbitrary commands onto the NAS as root.	7.2	More Details
CVE-2024-1001	A vulnerability classified as critical has been found in Totolink N200RE 9.3.5u.6139_B20201216. Affected is the function main of the file /cgi-bin/cstecgi.cgi. The manipulation leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-252270 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0999	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument eTime 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 identifier of this vulnerability is VDB-252268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0998	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. This affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252267. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0997	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. Affected by this issue is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252266 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2023-5372	The post-authentication command injection vulnerability in Zyxel NAS326 firmware versions through V5.21(AAZF.15)C0 and NAS542 firmware versions through V5.21(ABAG.12)C0 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands by sending a crafted query parameter attached to the URL of an affected device’s web management interface.	7.2	More Details
CVE-2024-0996	A vulnerability classified as critical has been found in Tenda i9 1.0.0.9(4122). This affects the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252261 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0995	A vulnerability was found in Tenda W6 1.0.0.9(4122). It has been rated as critical. Affected by this issue is the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252260. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0994	A vulnerability was found in Tenda W6 1.0.0.9(4122). It has been declared as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252259. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-24556	urql is a GraphQL client that exposes a set of helpers for several frameworks. The `@urql/next` package is vulnerable to XSS. To exploit this an attacker would need to ensure that the response returns `html` tags and that the web-application is using streamed responses (non-RSC). This vulnerability is due to improper escaping of html-like characters in the response-stream. To fix this vulnerability upgrade to version 1.1.1	7.2	More Details
CVE-2024-24140	Sourcecodester Daily Habit Tracker App 1.0 allows SQL Injection via the parameter 'tracker.'	7.2	More Details
CVE-2023-6279	The Woostify Sites Library WordPress plugin before 1.4.8 does not have authorisation in an AJAX action, allowing any authenticated users, such as subscriber to update arbitrary blog options and set them to 'activated' which could lead to DoS when using a specific option name	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23817	Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. Version 18.0.4 has a HTML Injection vulnerability in the Home page of the Dolibarr Application. This vulnerability allows an attacker to inject arbitrary HTML tags and manipulate the rendered content in the application's response. Specifically, I was able to successfully inject a new HTML tag into the returned document and, as a result, was able to comment out some part of the Dolibarr App Home page HTML code. This behavior can be exploited to perform various attacks like Cross-Site Scripting (XSS). To remediate the issue, validate and sanitize all user-supplied input, especially within HTML attributes, to prevent HTML injection attacks; and implement proper output encoding when rendering user-provided data to ensure it is treated as plain text rather than executable HTML.	7.1	More Details
CVE-2023-6291	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users.	7.1	More Details
CVE-2023-46231	In Splunk Add-on Builder versions below 4.1.4, the application writes user session tokens to its internal log files when you visit the Splunk Add-on Builder or when you build or edit a custom app or add-on.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23644	Trillium is a composable toolkit for building internet applications with async rust. In `trillium-http` prior to 0.3.12 and `trillium-client` prior to 0.5.4, insufficient validation of outbound header values may lead to request splitting or response splitting attacks in scenarios where attackers have sufficient control over headers. This only affects use cases where attackers have control of request headers, and can insert "\r\n" sequences. Specifically, if untrusted and unvalidated input is inserted into header names or values. Outbound `trillium_http::HeaderValue` and `trillium_http::HeaderName` can be constructed infallibly and were not checked for illegal bytes when sending requests from the client or responses from the server. Thus, if an attacker has sufficient control over header values (or names) in a request or response that they could inject `\r\n` sequences, they could get the client and server out of sync, and then pivot to gain control over other parts of requests or responses. (i.e. exfiltrating data from other requests, SSRF, etc.) In `trillium-http` versions 0.3.12 and later, if a header name is invalid in server response headers, the specific header and any associated values are omitted from network transmission. Additionally, if a header value is invalid in server response headers, the individual header value is omitted from network transmission. Other headers values with the same header name will still be sent. In `trillium-client` versions 0.5.4 and later, if any header name or header value is invalid in the client request headers, awaiting the client Conn returns an `Error::MalformedHeader` prior to any network access. As a workaround, Trillium services and client applications should sanitize or validate untrusted input that is included in header values and header names. Carriage return, newline, and null characters are not allowed.	6.8	More Details
CVE-2024-22894	An issue fixed in AIT-Deutschland Alpha Innotec Heatpumps V2.88.3 or later, V3.89.0 or later, V4.81.3 or later and Novelan Heatpumps V2.88.3 or later, V3.89.0 or later, V4.81.3 or later, allows remote attackers to execute arbitrary code via the password component in the shadow file.	6.8	More Details
CVE-2024-22366	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22372	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product.	6.8	More Details
CVE-2024-23826	spbu_se_site is the website of the Department of System Programming of St. Petersburg State University. Before 2024.01.29, when uploading an avatar image, an authenticated user may intentionally use a large Unicode filename which would lead to a server-side denial of service under Windows. This is due to no limitation of the length of the filename and the costly use of the Unicode normalization with the form NFKD on Windows OS. This vulnerability was fixed in the 2024.01.29 release.	6.8	More Details
CVE-2024-0841	A null pointer dereference flaw was found in the hugetlbfs_fill_super function in the Linux kernel hugetlbfs (HugeTLB pages) functionality. This issue may allow a local user to crash the system or potentially escalate their privileges on the system.	6.6	More Details
CVE-2023-44281	Dell Pair Installer version prior to 1.2.1 contains an elevation of privilege vulnerability. A low privilege user with local access to the system could potentially exploit this vulnerability to delete arbitrary files and result in Denial of Service.	6.6	More Details
CVE-2024-0697	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.2.3 via the node_id parameter in the backuply_get_jstree function. This makes it possible for attackers with administrator privileges or higher to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2024-23647	Authentik is an open-source Identity Provider. There is a bug in our implementation of PKCE that allows an attacker to circumvent the protection that PKCE offers. PKCE adds the code_challenge parameter to the authorization request and adds the code_verifier parameter to the token request. Prior to 2023.8.7 and 2023.10.7, a downgrade scenario is possible: if the attacker removes the code_challenge parameter from the authorization request, authentik will not do the PKCE check. Because of this bug, an attacker can circumvent the protection PKCE offers, such as CSRF attacks and code injection attacks. Versions 2023.8.7 and 2023.10.7 fix the issue.	6.5	More Details
CVE-2023-50944	Apache Airflow, versions before 2.8.1, have a vulnerability that allows an authenticated user to access the source code of a DAG to which they don't have access. This vulnerability is considered low since it requires an authenticated user to exploit it. Users are recommended to upgrade to version 2.8.1, which fixes this issue.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21388	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.5	More Details
CVE-2024-23638	Squid is a caching proxy for the Web. Due to an expired pointer reference bug, Squid prior to version 6.6 is vulnerable to a Denial of Service attack against Cache Manager error responses. This problem allows a trusted client to perform Denial of Service when generating error pages for Client Manager reports. Squid older than 5.0.5 have not been tested and should be assumed to be vulnerable. All Squid-5.x up to and including 5.9 are vulnerable. All Squid-6.x up to and including 6.5 are vulnerable. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. As a workaround, prevent access to Cache Manager using Squid's main access control: `http_access deny manager`.	6.5	More Details
CVE-2024-21653	The vantage6 technology enables to manage and deploy privacy enhancing technologies like Federated Learning (FL) and Multi-Party Computation (MPC). Nodes and servers get a ssh config by default that permits root login with password authentication. In a proper deployment, the SSH service is not exposed so there is no risk, but not all deployments are ideal. The default should therefore be less permissive. The vulnerability can be mitigated by removing the ssh part from the docker file and rebuilding the docker image. Version 4.2.0 patches the vulnerability.	6.5	More Details
CVE-2024-0814	Incorrect security UI in Payments in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-22643	A Cross-Site Request Forgery (CSRF) vulnerability in SEO Panel version 4.10.0 allows remote attackers to perform unauthorized user password resets.	6.5	More Details
CVE-2023-51813	Cross Site Request Forgery (CSRF) vulnerability in Free Open-Source Inventory Management System v.1.0 allows a remote attacker to execute arbitrary code via the staff_list parameter in the index.php component.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51702	Since version 5.2.0, when using deferrable mode with the path of a Kubernetes configuration file for authentication, the Airflow worker serializes this configuration file as a dictionary and sends it to the triggerer by storing it in metadata without any encryption. Additionally, if used with an Airflow version between 2.3.0 and 2.6.0, the configuration dictionary will be logged as plain text in the triggerer service without masking. This allows anyone with access to the metadata or triggerer log to obtain the configuration file and use it to access the Kubernetes cluster. This behavior was changed in version 7.0.0, which stopped serializing the file contents and started providing the file path instead to read the contents into the trigger. Users are recommended to upgrade to version 7.0.0, which fixes this issue.	6.5	More Details
CVE-2024-23901	Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier unconditionally discovers projects that are shared with the configured owner group, allowing attackers to configure and share a project, resulting in a crafted Pipeline being built by Jenkins during the next scan of the group.	6.5	More Details
CVE-2023-6159	An issue has been discovered in GitLab CE/EE affecting all versions from 12.7 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 It was possible for an attacker to trigger a Regular Expression Denial of Service via a `Cargo.toml` containing maliciously crafted input.	6.5	More Details
CVE-2023-41474	Directory Traversal vulnerability in Ivanti Avalanche 6.3.4.153 allows a remote authenticated attacker to obtain sensitive information via the javax.faces.resource component.	6.5	More Details
CVE-2024-0879	Authentication bypass in vector-admin allows a user to register to a vector-admin server while “domain restriction” is active, even when not owning an authorized email address.	6.5	More Details
CVE-2024-22141	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Cozmoslabs Profile Builder Pro.This issue affects Profile Builder Pro: from n/a through 3.10.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23829	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Security-sensitive parts of the Python HTTP parser retained minor differences in allowable character sets, that must trigger error handling to robustly match frame boundaries of proxies in order to protect against injection of additional requests. Additionally, validation could trigger exceptions that were not handled consistently with processing of other malformed input. Being more lenient than internet standards require could, depending on deployment environment, assist in request smuggling. The unhandled exception could cause excessive resource consumption on the application server and/or its logging facilities. This vulnerability exists due to an incomplete fix for CVE-2023-47627. Version 3.9.2 fixes this vulnerability.	6.5	More Details
CVE-2023-30970	Gotham Table service and Forward App were found to be vulnerable to a Path traversal issue allowing an authenticated user to read arbitrary files on the file system.	6.5	More Details
CVE-2024-23899	Jenkins Git server Plugin 99.va_0826a_b_cdfa_d and earlier does not disable a feature of its command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing attackers with Overall/Read permission to read content from arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2023-5933	An issue has been discovered in GitLab CE/EE affecting all versions after 13.7 before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. Improper input sanitization of user name allows arbitrary API PUT requests.	6.4	More Details
CVE-2024-0824	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Link Anything functionality in all versions up to, and including, 2.6.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-7225	The MapPress Maps for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the width and height parameters in all versions up to, and including, 2.88.16 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-37518	HCL BigFix ServiceNow is vulnerable to arbitrary code injection. A malicious authorized attacker could inject arbitrary code and execute within the context of the running user.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0988	A vulnerability classified as critical was found in Sichuan Yougou Technology KuERP up to 1.0.4. Affected by this vulnerability is the function checklogin of the file /application/index/common.php. The manipulation of the argument App_User_id/App_user_Token leads to improper authentication. The exploit has been disclosed to the public and may be used. The identifier VDB-252253 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0937	A vulnerability, which was classified as critical, has been found in van_der_Schaar LAB synthcity 0.2.9. Affected by this issue is the function load_from_file of the component PKL File Handler. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252182 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early and confirmed immediately the existence of the issue. A patch is planned to be released in February 2024.	6.3	More Details
CVE-2024-0939	A vulnerability has been found in Byzoro Smart S210 Management Platform up to 20240117 and classified as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252184. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0987	A vulnerability classified as critical has been found in Sichuan Yougou Technology KuERP up to 1.0.4. Affected is an unknown function of the file /runtime/log. The manipulation leads to improper output neutralization for logs. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252252. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-1027	A vulnerability, which was classified as critical, was found in SourceCodester Facebook News Feed Like 1.0. Affected is an unknown function of the component Post Handler. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-252300.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0933	A vulnerability was found in Niushop B2B2C V5 and classified as critical. Affected by this issue is some unknown functionality of the file \app\model\Upload.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-1007	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been classified as critical. Affected is an unknown function of the file edit_profile.php. The manipulation of the argument txtfullname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252276.	6.3	More Details
CVE-2024-0674	Privilege escalation vulnerability in Lamassu Bitcoin ATM Douro machines, in its 7.1 version, which could allow a local user to acquire root permissions by modifying the updatescript.js, inserting special code inside the script and creating the done.txt file. This would cause the watchdog process to run as root and execute the payload stored in the updatescript.js.	6.3	More Details
CVE-2024-0675	Vulnerability of improper checking for unusual or exceptional conditions in Lamassu Bitcoin ATM Douro machines, in its 7.1 version, the exploitation of which could allow an attacker with physical access to the ATM to escape kiosk mode, access the underlying Xwindow interface and execute arbitrary commands as an unprivileged user.	6.3	More Details
CVE-2024-0962	A vulnerability was found in obgm libcoap 4.3.4. It has been rated as critical. Affected by this issue is the function get_split_entry of the file src/coap_oscore.c of the component Configuration File Handler. The manipulation leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-252206 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-1021	A vulnerability, which was classified as critical, has been found in Rebuild up to 3.5.5. Affected by this issue is the function readRawText of the component HTTP Request Handler. The manipulation of the argument url leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252290 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0936	A vulnerability classified as critical was found in van_der_Schaar LAB TemporAI 0.0.3. Affected by this vulnerability is the function load_from_file of the component PKL File Handler. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252181 was assigned to this vulnerability. NOTE: The vendor was contacted early and confirmed immediately the existence of the issue. A patch is planned to be released in February 2024.	6.3	More Details
CVE-2024-23834	Discourse is an open-source discussion platform. Improperly sanitized user input could lead to an XSS vulnerability in some situations. This vulnerability only affects Discourse instances which have disabled the default Content Security Policy. The vulnerability is patched in 3.1.5 and 3.2.0.beta5. As a workaround, ensure Content Security Policy is enabled and does not include `unsafe-inline`.	6.3	More Details
CVE-2024-22099	NULL Pointer Dereference vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (net, bluetooth modules) allows Overflow Buffers. This vulnerability is associated with program files /net/bluetooth/rfcomm/core.C. This issue affects Linux kernel: v2.6.12-rc2.	6.3	More Details
CVE-2024-0890	A vulnerability was found in hongmaple octopus 1.0. It has been classified as critical. Affected is an unknown function of the file /system/dept/edit. The manipulation of the argument ancestors leads to sql injection. It is 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 product. Therefore, no version details of affected nor updated releases are available. VDB-252042 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0883	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been declared as critical. This vulnerability affects the function prepare of the file admin/pay.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252034 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-1014	Uncontrolled resource consumption vulnerability in SE-elektronic GmbH E-DDC3.3 affecting versions 03.07.03 and higher. An attacker could interrupt the availability of the administration panel by sending multiple ICMP packets.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40546	A flaw was found in Shim when an error happened while creating a new ESL variable. If Shim fails to create the new variable, it tries to print an error message to the user; however, the number of parameters used by the logging function doesn't match the format string used by it, leading to a crash under certain circumstances.	6.2	More Details
CVE-2023-40549	An out-of-bounds read flaw was found in Shim due to the lack of proper boundary verification during the load of a PE binary. This flaw allows an attacker to load a crafted PE binary, triggering the issue and crashing Shim, resulting in a denial of service.	6.2	More Details
CVE-2023-6389	The WordPress Toolbar WordPress plugin through 2.2.6 redirects to any URL via the "wptbto" parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	6.1	More Details
CVE-2023-6278	The Biteship: Plugin Ongkos Kirim Kurir Instant, Reguler, Kargo WordPress plugin before 2.2.25 does not sanitise and escape the biteship_error and biteship_message parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-6697	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the map id parameter in all versions up to, and including, 9.0.28 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-0665	The WP Customer Area plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 8.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-22639	iGalerie v3.0.22 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Titre (Title) field in the editing interface.	6.1	More Details
CVE-2024-23055	An issue in Plone Docker Official Image 5.2.13 (5221) open-source software allows for remote code execution via improper validation of input by the HOST headers.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22637	Form Tools v3.1.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /form_builder/preview.php?form_id=2.	6.1	More Details
CVE-2024-22635	WebCalendar v1.3.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /WebCalendarvqsmnseug2/edit_entry.php.	6.1	More Details
CVE-2023-37571	Softing TH SCOPE through 3.70 allows XSS.	6.1	More Details
CVE-2023-33758	Splicecom Maximiser Soft PBX v1.5 and before was discovered to contain a cross-site scripting (XSS) vulnerability via the CLIENT_NAME and DEVICE_GUID fields in the login component.	6.1	More Details
CVE-2024-23388	Improper authorization in handler for custom URL scheme issue in "Mercari" App for Android prior to version 5.78.0 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack.	6.1	More Details
CVE-2024-24135	Product Name and Product Code in the 'Add Product' section of Sourcecodester Product Inventory with Export to Excel 1.0 are vulnerable to XSS attacks.	6.1	More Details
CVE-2024-22725	Orthanc versions before 1.12.2 are affected by a reflected cross-site scripting (XSS) vulnerability. The vulnerability was present in the server's error reporting.	6.1	More Details
CVE-2023-7200	The EventON WordPress plugin before 4.4.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2024-22550	An arbitrary file upload vulnerability in the component /alsdemo/ss/mediam.cgi of ShopSite v14.0 allows attackers to execute arbitrary code via uploading a crafted SVG file.	6.1	More Details
CVE-2024-24136	The 'Your Name' field in the Submit Score section of Sourcecodester Math Game with Leaderboard v1.0 is vulnerable to Cross-Site Scripting (XSS) attacks.	6.1	More Details
CVE-2024-22551	WhatACart v2.0.7 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /site/default/search.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23334	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. When using aiohttp as a web server and configuring static routes, it is necessary to specify the root path for static files. Additionally, the option 'follow_symlinks' can be used to determine whether to follow symbolic links outside the static root directory. When 'follow_symlinks' is set to True, there is no validation to check if reading a file is within the root directory. This can lead to directory traversal vulnerabilities, resulting in unauthorized access to arbitrary files on the system, even when symlinks are not present. Disabling follow_symlinks and using a reverse proxy are encouraged mitigations. Version 3.9.2 fixes this issue.	5.9	More Details
CVE-2023-33757	A lack of SSL certificate validation in Splicecom iPCS (iOS App) v1.3.4, iPCS2 (iOS App) v2.8 and before, and iPCS (Android App) v1.8.5 and before allows attackers to eavesdrop on communications via a man-in-the-middle attack.	5.9	More Details
CVE-2023-6374	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric Corporation MELSEC WS Series WS0-GETH00200 all serial numbers allows a remote unauthenticated attacker to bypass authentication by capture-replay attack and illegally login to the affected module. As a result, the remote attacker who has logged in illegally may be able to disclose or tamper with the programs and parameters in the modules.	5.9	More Details
CVE-2024-0788	SUPERAntiSpyware Pro X v10.0.1260 is vulnerable to kernel-level API parameters manipulation and Denial of Service vulnerabilities by triggering the 0x9C402140 IOCTL code of the saskutil64.sys driver.	5.8	More Details
CVE-2024-20263	A vulnerability with the access control list (ACL) management within a stacked switch configuration of Cisco Business 250 Series Smart Switches and Business 350 Series Managed Switches could allow an unauthenticated, remote attacker to bypass protection offered by a configured ACL on an affected device. This vulnerability is due to incorrect processing of ACLs on a stacked configuration when either the primary or backup switches experience a full stack reload or power cycle. An attacker could exploit this vulnerability by sending crafted traffic through an affected device. A successful exploit could allow the attacker to bypass configured ACLs, causing traffic to be dropped or forwarded in an unexpected manner. The attacker does not have control over the conditions that result in the device being in the vulnerable state. Note: In the vulnerable state, the ACL would be correctly applied on the primary devices but could be incorrectly applied to the backup devices.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24565	CrateDB is a distributed SQL database that makes it simple to store and analyze massive amounts of data in real-time. There is a COPY FROM function in the CrateDB database that is used to import file data into database tables. This function has a flaw, and authenticated attackers can use the COPY FROM function to import arbitrary file content into database tables, resulting in information leakage. This vulnerability is patched in 5.3.9, 5.4.8, 5.5.4, and 5.6.1.	5.7	More Details
CVE-2024-0676	Weak password requirement vulnerability in Lamassu Bitcoin ATM Douro machines, in its 7.1 version , which allows a local user to interact with the machine where the application is installed, retrieve stored hashes from the machine and crack long 4-character passwords using a dictionary attack.	5.6	More Details
CVE-2023-40550	An out-of-bounds read flaw was found in Shim when it tried to validate the SBAT information. This issue may expose sensitive data during the system's boot phase.	5.5	More Details
CVE-2024-21796	Electronic Deliverables Creation Support Tool (Construction Edition) prior to Ver1.0.4 and Electronic Deliverables Creation Support Tool (Design & Survey Edition) prior to Ver1.0.4 improperly restrict XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2024-0727	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21765	Electronic Delivery Check System (Doboku) Ver.18.1.0 and earlier, Electronic Delivery Check System (Dentsu) Ver.12.1.0 and earlier, Electronic Delivery Check System (Kikai) Ver.10.1.0 and earlier, and Electronic delivery item Inspection Support SystemVer.4.0.31 and earlier improperly restrict XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2022-4964	Ubuntu's pipewire-pulse in snap grants microphone access even when the snap interface for audio-record is not set.	5.5	More Details
CVE-2023-29081	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders.	5.5	More Details
CVE-2024-23840	GoReleaser builds Go binaries for several platforms, creates a GitHub release and then pushes a Homebrew formula to a tap repository. `goreleaser release --debug` log shows secret values used in the in the custom publisher. This vulnerability is fixed in 1.24.0.	5.5	More Details
CVE-2024-0941	A vulnerability was found in Novel-Plus 4.3.0-RC1 and classified as critical. This issue affects some unknown processing of the file /novel/bookComment/list. The manipulation of the argument sort leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-252185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2024-23441	Vba32 Antivirus v3.36.0 is vulnerable to a Denial of Service vulnerability by triggering the 0x2220A7 IOCTL code of the Vba32m64.sys driver.	5.5	More Details
CVE-2024-23453	Android Spoon application version 7.11.1 to 8.6.0 uses hard-coded credentials, which may allow a local attacker to retrieve the hard-coded API key when the application binary is reverse-engineered. This API key may be used for unexpected access of the associated service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0938	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file /general/email/inbox/delete_webmail.php. The manipulation of the argument WEBBODY_ID_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-252183. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-4552	Improper Input Validation vulnerability in OpenText AppBuilder on Windows, Linux allows Probe System Files. An authenticated AppBuilder user with the ability to create or manage existing databases can leverage them to exploit the AppBuilder server - including access to its local file system. This issue affects AppBuilder: from 21.2 before 23.2.	5.5	More Details
CVE-2024-22380	Electronic Delivery Check System (Ministry of Agriculture, Forestry and Fisheries The Agriculture and Rural Development Project Version) March, Heisei 31 era edition Ver.14.0.001.002 and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2023-43988	An issue in nature fitness saijo mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-6282	IceHrm 23.0.0.OS does not sufficiently encode user-controlled input, which creates a Cross-Site Scripting (XSS) vulnerability via /icehrm/app/fileupload_page.php, in multiple parameters. An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload and partially hijacking the victim's browser.	5.4	More Details
CVE-2024-23822	Thruk is a multibackend monitoring webinterface. Prior to 3.12, the Thruk web monitoring application presents a vulnerability in a file upload form that allows a threat actor to arbitrarily upload files to the server to any path they desire and have permissions for. This vulnerability is known as Path Traversal or Directory Traversal. Version 3.12 fixes the issue.	5.4	More Details
CVE-2024-22559	LightCMS v2.0 is vulnerable to Cross Site Scripting (XSS) in the Content Management - Articles field.	5.4	More Details
CVE-2024-22570	A stored cross-site scripting (XSS) vulnerability in /install.php?m=install&c=index&a=step3 of GreenCMS v2.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36259	Cross Site Scripting (XSS) vulnerability in Craft CMS Audit Plugin before version 3.0.2 allows attackers to execute arbitrary code during user creation.	5.4	More Details
CVE-2023-6503	The WP Plugin Lister WordPress plugin through 2.1.0 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	5.4	More Details
CVE-2023-6530	The TJ Shortcodes WordPress plugin through 0.1.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2024-0854	URL redirection to untrusted site ('Open Redirect') vulnerability in file access component in Synology DiskStation Manager (DSM) before 6.2.4-25556-8, 7.0.1-42218-7, 7.1.1-42962-7 and 7.2.1-69057-2 allows remote authenticated users to conduct phishing attacks via unspecified vectors.	5.4	More Details
CVE-2023-7089	The Easy SVG Allow WordPress plugin through 1.0 does not sanitize uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.	5.4	More Details
CVE-2023-44001	An issue in Ailand clinic mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2024-23905	Jenkins Red Hat Dependency Analytics Plugin 0.7.1 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	5.4	More Details
CVE-2023-44000	An issue in Otakara lapis totuka mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48129	An issue in kimono-oldnew mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43989	An issue in mokumoku chohu mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43990	An issue in cherub-hair mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2024-0667	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.15.21. This is due to missing or incorrect nonce validation on the 'execute' function. This makes it possible for unauthenticated attackers to execute arbitrary methods in the 'BoosterController' class via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-43991	An issue in PRIMA CLINIC mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43992	An issue in STOCKMAN GROUP mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48201	Cross Site Scripting (XSS) vulnerability in Sunlight CMS v.8.0.1, allows remote authenticated attackers to execute arbitrary code and escalate privileges via a crafted script to the Content text editor component.	5.4	More Details
CVE-2023-48202	Cross-Site Scripting (XSS) vulnerability in Sunlight CMS 8.0.1 allows an authenticated low-privileged user to escalate privileges via a crafted SVG file in the File Manager component.	5.4	More Details
CVE-2023-43993	An issue in smaregi_app_market mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43994	An issue in Cleaning_makotoya mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43995	An issue in picot.golf mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43996	An issue in Q co ltd mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23782	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier versions. If this vulnerability is exploited, a user with a contributor or higher privilege may execute an arbitrary script on the web browser of the user who accessed the website using the product.	5.4	More Details
CVE-2023-43997	An issue in Yoruichi hobby base mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2024-0989	A vulnerability, which was classified as problematic, has been found in Sichuan Yougou Technology KuERP up to 1.0.4. Affected by this issue is the function del_sn_db of the file /application/index/controller/Service.php. The manipulation of the argument file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-252254 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2023-48130	An issue in GINZA CAFE mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43999	An issue in COLORFUL_laundry mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-43998	An issue in Books-futaba mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48126	An issue in Luxe Beauty Clinic mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48127	An issue in myGAKUYA mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48135	An issue in mimasaka_farm mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48128	An issue in UNITED BOXING GYM mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48133	An issue in angel coffee mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48131	An issue in CHIGASAKI BAKERY mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2023-48132	An issue in kosei entertainment esportsstudioLegends mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	5.4	More Details
CVE-2024-22646	An email address enumeration vulnerability exists in the password reset function of SEO Panel version 4.10.0. This allows an attacker to guess which emails exist on the system.	5.3	More Details
CVE-2024-23903	Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2024-1017	A vulnerability was found in Gabriels FTP Server 1.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument USERNAME leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-252287.	5.3	More Details
CVE-2023-4553	Improper Input Validation vulnerability in OpenText AppBuilder on Windows, Linux allows Probe System Files. AppBuilder configuration files are viewable by unauthenticated users. This issue affects AppBuilder: from 21.2 before 23.2.	5.3	More Details
CVE-2024-22648	A Blind SSRF vulnerability exists in the "Crawl Meta Data" functionality of SEO Panel version 4.10.0. This makes it possible for remote attackers to scan ports in the local environment.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1005	A vulnerability has been found in Shanxi Diankeyun Technology NODERP up to 6.0.2 and classified as critical. This vulnerability affects unknown code of the file /runtime/log. The manipulation leads to files or directories accessible. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252274 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-1016	A vulnerability was found in Solar FTP Server 2.1.1/2.1.2. It has been declared as problematic. This vulnerability affects unknown code of the component PASV Command Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-252286 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2024-22647	An user enumeration vulnerability was found in SEO Panel 4.10.0. This issue occurs during user authentication, where a difference in error messages could allow an attacker to determine if a username is valid or not, enabling a brute-force attack with valid usernames.	5.3	More Details
CVE-2023-33760	SpliceCom Maximiser Soft PBX v1.5 and before was discovered to utilize a default SSL certificate. This issue can allow attackers to eavesdrop on communications via a man-in-the-middle attack.	5.3	More Details
CVE-2024-0624	The Paid Memberships Pro – Content Restriction, User Registration, & Paid Subscriptions plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.12.7. This is due to missing or incorrect nonce validation on the pmpro_update_level_order() function. This makes it possible for unauthenticated attackers to update the order of levels via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2024-23792	When adding attachments to ticket comments, another user can add attachments as well impersonating the orginal user. The attack requires a logged-in other user to know the UUID. While the legitimate user completes the comment, the malicious user can add more files to the comment. This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023.X through 2023.1.1.	5.3	More Details
CVE-2024-0888	A vulnerability, which was classified as problematic, was found in BORGChat 1.0.0 Build 438. This affects an unknown part of the component Service Port 7551. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252039.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5612	An issue has been discovered in GitLab affecting all versions before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. It was possible to read the user email address via tags feed although the visibility in the user profile has been disabled.	5.3	More Details
CVE-2023-7199	The Relevanssi WordPress plugin before 4.22.0, Relevanssi Premium WordPress plugin before 2.25.0 allows any unauthenticated user to read draft and private posts via a crafted request	5.3	More Details
CVE-2024-21387	Microsoft Edge for Android Spoofing Vulnerability	5.3	More Details
CVE-2024-0617	The Category Discount Woocommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpcd_save_discount() function in all versions up to, and including, 4.12. This makes it possible for unauthenticated attackers to modify product category discounts that could lead to loss of revenue.	5.3	More Details
CVE-2024-21619	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.	5.3	More Details
CVE-2024-22294	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in IP2Location IP2Location Country Blocker.This issue affects IP2Location Country Blocker: from n/a through 2.33.3.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0564	A flaw was found in the Linux kernel's memory deduplication mechanism. The max page sharing of Kernel Samepage Merging (KSM), added in Linux kernel version 4.4.0-96.119, can create a side channel. When the attacker and the victim share the same host and the default setting of KSM is "max page sharing=256", it is possible for the attacker to time the unmap to merge with the victim's page. The unmapping time depends on whether it merges with the victim's page and additional physical pages are created beyond the KSM's "max page share". Through these operations, the attacker can leak the victim's page.	5.3	More Details
CVE-2024-0889	A vulnerability was found in Kmint21 Golden FTP Server 2.02b and classified as problematic. This issue affects some unknown processing of the component PASV Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252041 was assigned to this vulnerability.	5.3	More Details
CVE-2024-0887	A vulnerability, which was classified as problematic, has been found in Mafiatic Blue Server 1.1. Affected by this issue is some unknown functionality of the component Connection Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252038 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-52187	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Thomas Maier Image Source Control Lite – Show Image Credits and Captions.This issue affects Image Source Control Lite – Show Image Credits and Captions: from n/a through 2.17.0.	5.3	More Details
CVE-2024-23820	OpenFGA, an authorization/permission engine, is vulnerable to a denial of service attack in versions prior to 1.4.3. In some scenarios that depend on the model and tuples used, a call to `ListObjects` may not release memory properly. So when a sufficiently high number of those calls are executed, the OpenFGA server can create an `out of memory` error and terminate. Version 1.4.3 contains a patch for this issue.	5.3	More Details
CVE-2024-22301	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ignazio Scimone Albo Pretorio On line.This issue affects Albo Pretorio On line: from n/a through 4.6.6.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0885	A vulnerability classified as problematic has been found in SpyCamLizard 1.230. Affected is an unknown function of the component HTTP GET Request Handler. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252036.	5.3	More Details
CVE-2024-1063	Appwrite <= v1.4.13 is affected by a Server-Side Request Forgery (SSRF) via the '/v1/avatars/favicon' endpoint due to an incomplete fix of CVE-2023-27159.	5.3	More Details
CVE-2023-6482	Use of encryption key derived from static information in Synaptics Fingerprint Driver allows an attacker to set up a TLS session with the fingerprint sensor and send restricted commands to the fingerprint sensor. This may allow an attacker, who has physical access to the sensor, to enroll a fingerprint into the template database.	5.2	More Details
CVE-2023-40551	A flaw was found in the MZ binary format in Shim. An out-of-bounds read may occur, leading to a crash or possible exposure of sensitive data during the system's boot phase.	5.1	More Details
CVE-2024-0959	A vulnerability was found in StanfordVL GibsonEnv 0.3.1. It has been classified as critical. Affected is the function cloudpickle.load of the file gibson\utils\pposgd_fuse.py. The manipulation leads to deserialization. It is possible to launch 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 used. The identifier of this vulnerability is VDB-252204.	5.0	More Details
CVE-2024-0960	A vulnerability was found in flink-extended ai-flow 0.3.1. It has been declared as critical. Affected by this vulnerability is the function cloudpickle.loads of the file \ai_flow\cli\commands\workflow_command.py. The manipulation leads to deserialization. The attack can be launched 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 identifier VDB-252205 was assigned to this vulnerability.	5.0	More Details
CVE-2023-4554	Improper Restriction of XML External Entity Reference vulnerability in OpenText AppBuilder on Windows, Linux allows Server Side Request Forgery, Probe System Files. AppBuilder's XML processor is vulnerable to XML External Entity Processing (XXE), allowing an authenticated user to upload specially crafted XML files to induce server-side request forgery, disclose files local to the server that processes them. This issue affects AppBuilder: from 21.2 before 23.2.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22134	Server-Side Request Forgery (SSRF) vulnerability in Renzo Johnson Contact Form 7 Extension For Mailchimp.This issue affects Contact Form 7 Extension For Mailchimp: from n/a through 0.5.70.	4.9	More Details
CVE-2024-23791	Insertion of debug information into log file during building the elastic search index allows reading of sensitive information from articles.This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023.X through 2023.1.1.	4.9	More Details
CVE-2024-22720	Kanboard 1.2.34 is vulnerable to Html Injection in the group management feature.	4.8	More Details
CVE-2024-24134	Sourcecodester Online Food Menu 1.0 is vulnerable to Cross Site Scripting (XSS) via the 'Menu Name' and 'Description' fields in the Update Menu section.	4.8	More Details
CVE-2023-5124	The Page Builder: Pagelayer WordPress plugin before 1.8.0 doesn't prevent attackers with administrator privileges from inserting malicious JavaScript inside a post's header or footer code, even when unfiltered_html is disallowed, such as in multi-site WordPress configurations.	4.8	More Details
CVE-2023-5943	The Wp-Adv-Quiz WordPress plugin before 1.0.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2021-43584	DOM-based Cross Site Scripting (XSS vulnerability in 'Tail Event Logs' functionality in Nagios Nagios Cross-Platform Agent (NCPA) before 2.4.0 allows attackers to run arbitrary code via the name element when filtering for a log.	4.8	More Details
CVE-2024-20305	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5956	The Wp-Adv-Quiz WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-24567	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. Vyper compiler allows passing a value in builtin raw_call even if the call is a delegatecall or a staticcall. But in the context of delegatecall and staticcall the handling of value is not possible due to the semantics of the respective opcodes, and vyper will silently ignore the value= argument. If the semantics of the EVM are unknown to the developer, he could suspect that by specifying the `value` kwarg, exactly the given amount will be sent along to the target. This vulnerability affects 0.3.10 and earlier versions.	4.8	More Details
CVE-2023-6165	The Restrict Usernames Emails Characters WordPress plugin before 3.1.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2023-52046	Cross Site Scripting vulnerability (XSS) in webmin v.2.105 and earlier allows a remote attacker to execute arbitrary code via a crafted payload to the "Execute cron job as" tab Input field.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23633	Label Studio, an open source data labeling tool had a remote import feature allowed users to import data from a remote web source, that was downloaded and could be viewed on the website. Prior to version 1.10.1, this feature could had been abused to download a HTML file that executed malicious JavaScript code in the context of the Label Studio website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. `data_import/uploader.py` lines 125C5 through 146 showed that if a URL passed the server side request forgery verification checks, the contents of the file would be downloaded using the filename in the URL. The downloaded file path could then be retrieved by sending a request to `/api/projects/{project_id}/file-uploads?ids=[{download_id}]` where `{project_id}` was the ID of the project and `{download_id}` was the ID of the downloaded file. Once the downloaded file path was retrieved by the previous API endpoint, `data_import/api.py`lines 595C1 through 616C62 demonstrated that the `Content-Type` of the response was determined by the file extension, since `mimetypes.guess_type` guesses the `Content-Type` based on the file extension. Since the `Content-Type` was determined by the file extension of the downloaded file, an attacker could import in a `.html` file that would execute JavaScript when visited. Version 1.10.1 contains a patch for this issue. Other remediation strategies are also available. For all user provided files that are downloaded by Label Studio, set the `Content-Security-Policy: sandbox;` response header when viewed on the site. The `sandbox` directive restricts a page's actions to prevent popups, execution of plugins and scripts and enforces a `same-origin` policy. Alternatively, restrict the allowed file extensions that may be downloaded.	4.7	More Details
CVE-2024-0932	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This issue affects the function setSmartPowerManagement. The manipulation of the argument time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252137 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0931	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. This vulnerability affects the function saveParentControlInfo. The manipulation of the argument deviceId/time/urls 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 identifier of this vulnerability is VDB-252136. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-1008	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file edit-photo.php of the component Profile Page. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252277 was assigned to this vulnerability.	4.7	More Details
CVE-2024-0986	A vulnerability was found in Issabel PBX 4.0.0. It has been rated as critical. This issue affects some unknown processing of the file /index.php?menu=asterisk_cli of the component Asterisk-Cli. The manipulation of the argument 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 associated identifier of this vulnerability is VDB-252251. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0921	A vulnerability has been found in D-Link DIR-816 A2 1.10CNB04 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setDeviceSettings of the component Web Interface. The manipulation of the argument statuscheckpppoeuser leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252139.	4.7	More Details
CVE-2024-0922	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this vulnerability is the function formQuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252127. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0923	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this issue is the function formSetDeviceName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0924	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function formSetPPTPServer. The manipulation of the argument startIp leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252129 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0925	A vulnerability has been found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This vulnerability affects the function formSetVirtualSer. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252130 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0926	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This issue affects the function formWifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252131. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0927	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been classified as critical. Affected is the function fromAddressNat. The manipulation of the argument entrys/mitInterface/page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252132. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0928	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been declared as critical. Affected by this vulnerability is the function fromDhcpListClient. The manipulation of the argument page/listN leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252133 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0929	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been rated as critical. Affected by this issue is the function fromNatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252134 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0930	A vulnerability classified as critical has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function fromSetWirelessRepeat. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252135. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-0884	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects the function exec of the file payment.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252035.	4.7	More Details
CVE-2024-0664	The Meks Smart Social Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Meks Smart Social Widget in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6497	The WordPress Simple Shopping Cart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the automatic redirect URL setting in all versions up to and including 4.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-0618	The Contact Form Plugin – Fastest Contact Form Builder Plugin for WordPress by Fluent Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via imported form titles in all versions up to, and including, 5.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-0625	The WPFront Notification Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘wpfront-notification-bar-options[custom_class]’ parameter in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-0688	The "WebSub (FKA. PubSubHubbub)" plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2024-23307	Integer Overflow or Wraparound vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (md, raid, raid5 modules) allows Forced Integer Overflow.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21630	Zulip is an open-source team collaboration tool. A vulnerability in version 8.0 is similar to CVE-2023-32677, but applies to multi-use invitations, not single-use invitation links as in the prior CVE. Specifically, it applies when the installation has configured non-admins to be able to invite users and create multi-use invitations, and has also configured only admins to be able to invite users to streams. As in CVE-2023-32677, this does not let users invite new users to arbitrary streams, only to streams that the inviter can already see. Version 8.1 fixes this issue. As a workaround, administrators can limit sending of invitations down to users who also have the permission to add users to streams.	4.3	More Details
CVE-2024-23900	Jenkins Matrix Project Plugin 822.v01b_8c85d16d2 and earlier does not sanitize user-defined axis names of multi-configuration projects, allowing attackers with Item/Configure permission to create or replace any config.xml files on the Jenkins controller file system with content not controllable by the attackers.	4.3	More Details
CVE-2024-1011	A vulnerability classified as problematic was found in SourceCodester Employee Management System 1.0. This vulnerability affects unknown code of the file delete-leave.php of the component Leave Handler. The manipulation of the argument id leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252280.	4.3	More Details
CVE-2024-21382	Microsoft Edge for Android Information Disclosure Vulnerability	4.3	More Details
CVE-2024-0456	An authorization vulnerability exists in GitLab versions 14.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. An unauthorized attacker is able to assign arbitrary users to MRs that they created within the project	4.3	More Details
CVE-2024-1033	A vulnerability, which was classified as problematic, has been found in openBI up to 1.0.8. Affected by this issue is the function agent of the file /application/index/controller/Datament.php. The manipulation of the argument api leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252308.	4.3	More Details
CVE-2023-6633	The Site Notes WordPress plugin through 2.0.0 does not have CSRF checks in some of its functionalities, which could allow attackers to make logged in users perform unwanted actions, such as deleting administration notes, via CSRF attacks	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23902	A cross-site request forgery (CSRF) vulnerability in Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier allows attackers to connect to an attacker-specified URL.	4.3	More Details
CVE-2024-0880	A vulnerability was found in Qidianbang qdbcrm 1.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /user/edit?id=2 of the component Password Reset. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252032. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-0882	A vulnerability was found in qwdigital LinkWechat 5.1.0. It has been classified as problematic. This affects an unknown part of the file /linkwechat-api/common/download/resource of the component Universal Download Interface. The manipulation of the argument name with the input /profile/../../../../../etc/passwd leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252033 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-0805	Inappropriate implementation in Downloads in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-0811	Inappropriate implementation in Extensions API in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Details
CVE-2024-0810	Insufficient policy enforcement in DevTools in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-0809	Inappropriate implementation in Autofill in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0943	A vulnerability was found in Totolink N350RT 9.3.5u.6255. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. The attack can be launched 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 associated identifier of this vulnerability is VDB-252187. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-0944	A vulnerability was found in Totolink T8 4.1.5cu.833_20220905. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252188. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-0942	A vulnerability was found in Totolink N200RE V5 9.3.5u.6255_B20211224. It has been classified as problematic. Affected is an unknown function of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. It is possible to launch 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 used. VDB-252186 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-21671	The vantage6 technology enables to manage and deploy privacy enhancing technologies like Federated Learning (FL) and Multi-Party Computation (MPC). It is possible to find out usernames from the response time of login requests. This could aid attackers in credential attacks. Version 4.2.0 patches this vulnerability.	3.7	More Details
CVE-2024-0958	A vulnerability was found in CodeAstro Stock Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /index.php of the component Add Category Handler. The manipulation of the argument Category Name/Category Description leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252203.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1028	A vulnerability has been found in SourceCodester Facebook News Feed Like 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Post Handler. The manipulation of the argument Description with the input <marquee>HACKED</marquee> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252301 was assigned to this vulnerability.	3.5	More Details
CVE-2024-1010	A vulnerability classified as problematic has been found in SourceCodester Employee Management System 1.0. This affects an unknown part of the file edit-profile.php. The manipulation of the argument fullname/phone/date of birth/address/date of appointment leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-252279.	3.5	More Details
CVE-2024-22193	The vantage6 technology enables to manage and deploy privacy enhancing technologies like Federated Learning (FL) and Multi-Party Computation (MPC). There are no checks on whether the input is encrypted if a task is created in an encrypted collaboration. Therefore, a user may accidentally create a task with sensitive input data that will then be stored unencrypted in a database. Users should ensure they set the encryption setting correctly. This vulnerability is patched in 4.2.0.	3.5	More Details
CVE-2023-22836	In cases where a multi-tenant stack user is operating Foundry's Linter service, and the user changes a group name from the default value, the renamed value may be visible to the rest of the stack's tenants.	3.5	More Details
CVE-2024-1020	A vulnerability classified as problematic was found in Rebuild up to 3.5.5. Affected by this vulnerability is the function getStorageFile of the file /filex/proxy-download. The manipulation of the argument url leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252289 was assigned to this vulnerability.	3.5	More Details
CVE-2024-1026	A vulnerability was found in Cogites eReserv 7.7.58 and classified as problematic. This issue affects some unknown processing of the file front/admin/config.php. The manipulation of the argument id with the input %22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-252293 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1024	A vulnerability has been found in SourceCodester Facebook News Feed Like 1.0 and classified as problematic. This vulnerability affects unknown code of the component New Account Handler. The manipulation of the argument First Name/Last Name with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252292.	3.5	More Details
CVE-2024-0891	A vulnerability was found in hongmaple octopus 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument description with the input <script>alert(document.cookie)</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-252043.	3.5	More Details
CVE-2024-1031	A vulnerability was found in CodeAstro Expense Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file templates/5-Add-Expenses.php of the component Add Expenses Page. The manipulation of the argument item leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252304.	3.5	More Details
CVE-2024-1029	A vulnerability was found in Cogites eReserv 7.7.58 and classified as problematic. Affected by this issue is some unknown functionality of the file /front/admin/tenancyDetail.php. The manipulation of the argument Nom with the input Dreux"><script>alert('XSS')</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252302 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-21803	Use After Free vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (bluetooth modules) allows Local Execution of Code. This vulnerability is associated with program files https://gitee.Com/anolis/cloud-kernel/blob/devel-5.10/net/bluetooth/af_bluetooth.C. This issue affects Linux kernel: from v2.6.12-rc2 before v6.8-rc1.	3.5	More Details
CVE-2024-1030	A vulnerability was found in Cogites eReserv 7.7.58. It has been classified as problematic. This affects an unknown part of the file /front/admin/tenancyDetail.php. The manipulation of the argument id leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-252303.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23790	Improper Input Validation vulnerability in the upload functionality for user avatars allows functionality misuse due to missing check of filetypes. This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023 through 2023.1.1.	3.5	More Details
CVE-2024-22308	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in smp7, wp.Insider Simple Membership.This issue affects Simple Membership: from n/a through 4.4.1.	3.4	More Details
CVE-2024-0886	A vulnerability classified as problematic was found in Poikosoft EZ CD Audio Converter 8.0.7. Affected by this vulnerability is an unknown functionality of the component Activation Handler. The manipulation of the argument Key leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-252037 was assigned to this vulnerability.	3.3	More Details
CVE-2024-23743	Notion through 3.1.0 on macOS might allow code execution because of RunAsNode and enableNodeCliInspectArguments. NOTE: the vendor states "the attacker must launch the Notion Desktop application with nonstandard flags that turn the Electron-based application into a Node.js execution environment."	3.3	More Details
CVE-2024-22200	vantage6-UI is the User Interface for vantage6. The docker image used to run the UI leaks the nginx version. To mitigate the vulnerability, users can run the UI as an angular application. This vulnerability was patched in 4.2.0.	3.3	More Details
CVE-2024-21383	Microsoft Edge (Chromium-based) Spoofing Vulnerability	3.3	More Details
CVE-2024-22229	Dell Unity, versions prior to 5.4, contain a vulnerability whereby log messages can be spoofed by an authenticated attacker. An attacker could exploit this vulnerability to forge log entries, create false alarms, and inject malicious content into logs that compromise logs integrity. A malicious attacker could also prevent the product from logging information while malicious actions are performed or implicate an arbitrary user for malicious activities.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23825	TablePress is a table plugin for Wordpress. For importing tables, TablePress makes external HTTP requests based on a URL that is provided by the user. That user input is filtered insufficiently, which makes it is possible to send requests to unintended network locations and receive responses. On sites in a cloud environment like AWS, an attacker can potentially make GET requests to the instance's metadata REST API. If the instance's configuration is insecure, this can lead to the exposure of internal data, including credentials. This vulnerability is fixed in 2.2.5.	3.0	More Details
CVE-2023-50785	Zoho ManageEngine ADAudit Plus before 7270 allows admin users to view names of arbitrary directories via path traversal.	2.7	More Details
CVE-2024-21336	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2.5	More Details
CVE-2024-1022	A vulnerability, which was classified as problematic, was found in CodeAstro Simple Student Result Management System 5.6. This affects an unknown part of the file /add_classes.php of the component Add Class Page. The manipulation of the argument Class Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252291.	2.4	More Details
CVE-2024-1018	A vulnerability classified as problematic has been found in PbootCMS 3.2.5-20230421. Affected is an unknown function of the file /admin.php?p=/Area/index#tab=t2. The manipulation of the argument name 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 identifier of this vulnerability is VDB-252288.	2.4	More Details
CVE-2024-0948	** DISPUTED ** A vulnerability, which was classified as problematic, has been found in NetBox up to 3.7.0. This issue affects some unknown processing of the file /core/config-revisions of the component Home Page Configuration. The manipulation with the input <<h1 onload=alert(1)>>test</h1> leads to cross site scripting. The attack may be initiated 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 associated identifier of this vulnerability is VDB-252191. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51197	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2023-51204	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2023-51202	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2023-45930	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-45928	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-51198	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2023-45926	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-22682	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-52071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-6470	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45932	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-45921	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-45916	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-45923	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-46050	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details