SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 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-2023-7028	An issue has been discovered in GitLab CE/EE affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which user account password reset emails could be delivered to an unverified email address.	10.0	More Details
CVE-2024-21669	Hyperledger Aries Cloud Agent Python (ACA-Py) is a foundation for building decentralized identity applications and services running in non-mobile environments. When verifying W3C Format Verifiable Credentials using JSON-LD with Linked Data Proofs (LDP-VCs), the result of verifying the presentation `document.proof` was not factored into the final `verified` value (`true`/`false`) on the presentation record. The flaw enables holders of W3C Format Verifiable Credentials using JSON-LD with Linked Data Proofs (LDPs) to present incorrectly constructed proofs, and allows malicious verifiers to save and replay a presentation from such holders as their own. This vulnerability has been present since version 0.7.0 and fixed in version 0.10.5.	9.9	More Details
CVE-2023-34063	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows.	9.9	More Details
CVE-2023-51987	D-Link DIR-822+ V1.0.2 contains a login bypass in the HNAP1 interface, which allows attackers to log in to administrator accounts with empty passwords.	9.8	More Details
CVE-2024-21591	An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device. This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory. This issue affects Juniper Networks Junos OS SRX Series and EX Series: * Junos OS versions earlier than 20.4R3-S9; * Junos OS 21.2 versions earlier than 21.2R3-S7; * Junos OS 21.3 versions earlier than 21.3R3-S5; * Junos OS 21.4 versions earlier than 21.4R3-S5; * Junos OS 22.1 versions earlier than 22.1R3-S4; * Junos OS 22.2 versions earlier than 22.2R3-S3; * Junos OS 22.3 versions earlier than 22.3R3-S2; * Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30016	SQL Injection vulnerability in oretnom23 Judging Management System v1.0, allows remote attackers to execute arbitrary code and obtain sensitive information via sub_event_id parameter in sub_event_details_edit.php.	9.8	More Details
CVE-2023-30015	SQL Injection vulnerability in oretnom23 Judging Management System v1.0, allows remote attackers to execute arbitrary code and obtain sensitive information via txtsearch parameter in review_search.php.	9.8	More Details
CVE-2023-30014	SQL Injection vulnerability in oretnom23 Judging Management System v1.0, allows remote attackers to execute arbitrary code and obtain sensitive information via sub_event_id parameter in sub_event_stat_update.php.	9.8	More Details
CVE-2023-50919	An issue was discovered on GL.iNet devices before version 4.5.0. There is an NGINX authentication bypass via Lua string pattern matching. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	9.8	More Details
CVE-2023-37117	A heap-use-after-free vulnerability was found in live555 version 2023.05.10 while handling the SETUP.	9.8	More Details
CVE-2022-48620	uev (aka libuev) before 2.4.1 has a buffer overflow in epoll_wait if maxevents is a large number.	9.8	More Details
CVE-2016-20021	In Gentoo Portage before 3.0.47, there is missing PGP validation of executed code: the standalone emerge-webrsync downloads a .gpgsig file but does not perform signature verification. Unless emerge-webrsync is used, Portage is not vulnerable.	9.8	More Details
CVE-2023-51350	A spoofing attack in ujcms v.8.0.2 allows a remote attacker to obtain sensitive information and execute arbitrary code via a crafted script to the X-Forwarded-For function in the header.	9.8	More Details
CVE-2024-22942	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the hostName parameter in the setWanCfg function.	9.8	More Details
CVE-2023-52026	TOTOlink EX1800T V9.1.0cu.2112_B20220316 was discovered to contain a remote command execution (RCE) vulnerability via the telnet_enabled parameter of the setTelnetCfg interface	9.8	More Details
CVE-2024-23061	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the minute parameter in the setScheduleCfg function.	9.8	More Details
CVE-2023-51984	D-Link DIR-822+ V1.0.2 was found to contain a command injection in SetStaticRouteSettings function. allows remote attackers to execute arbitrary commands via shell.	9.8	More Details
CVE-2024-23060	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the ip parameter in the setDmzCfg function.	9.8	More Details
CVE-2024-23059	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the username parameter in the setDdnsCfg function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23058	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the pass parameter in the setTr069Cfg function.	9.8	More Details
CVE-2024-23057	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the tz parameter in the setNtpCfg function.	9.8	More Details
CVE-2023-49569	A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to create and amend files across the filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if they are using the ChrootOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS , which is the default when using "Plain" versions of Open and Clone funcs (e.g. PlainClone). Applications using BoundOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS or in-memory filesystems are not affected by this issue. This is a go-git implementation issue and does not affect the upstream git cli.	9.8	More Details
CVE-2023-31446	In Cassia Gateway firmware XC1000_2.1.1.2303082218 and XC2000_2.1.1.2303090947, the queueUrl parameter in /bypass/config is not sanitized. This leads to injecting Bash code and executing it with root privileges on device startup.	9.8	More Details
CVE-2023-6875	The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a type juggling issue on the connect-app REST endpoint in all versions up to, and including, 2.8.7. This makes it possible for unauthenticated attackers to reset the API key used to authenticate to the mailer and view logs, including password reset emails, allowing site takeover.	9.8	More Details
CVE-2023-49253	Root user password is hardcoded into the device and cannot be changed in the user interface.	9.8	More Details
CVE-2024-22916	In D-LINK Go-RT-AC750 v101b03, the sprintf function in the sub_40E700 function within the cgibin is susceptible to stack overflow.	9.8	More Details
CVE-2023-52042	An issue discovered in sub_4117F8 function in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the 'lang' parameter.	9.8	More Details
CVE-2023-39691	An issue discovered in kodbox through 1.43 allows attackers to arbitrarily add Administrator accounts via crafted GET request.	9.8	More Details
CVE-2023-52041	An issue discovered in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary code via the sub_410118 function of the shttpd program.	9.8	More Details
CVE-2023-49351	A stack-based buffer overflow vulnerability in /bin/webs binary in Edimax BR6478AC V2 firmware veraion v1.23 allows attackers to overwrite other values located on the stack due to an incorrect use of the strcpy() function.	9.8	More Details
CVE-2023-3211	The WordPress Database Administrator WordPress plugin through 1.0.3 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2023-0224	The GiveWP WordPress plugin before 2.24.1 does not properly escape user input before it reaches SQL queries, which could let unauthenticated attackers perform SQL Injection attacks	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1609	The School Management WordPress plugin before 9.9.7 contains an obfuscated backdoor injected in it's license checking code that registers a REST API handler, allowing an unauthenticated attacker to execute arbitrary PHP code on the site.	9.8	More Details
CVE-2023-52103	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read.	9.8	More Details
CVE-2023-22527	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action. Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin.	9.8	More Details
CVE-2023-6623	The Essential Blocks WordPress plugin before 4.4.3 does not prevent unauthenticated attackers from overwriting local variables when rendering templates over the REST API, which may lead to Local File Inclusion attacks.	9.8	More Details
CVE-2023-6049	The Estatik Real Estate Plugin WordPress plugin before 4.1.1 unserializes user input via some of its cookies, which could allow unauthenticated users to perform PHP Object Injection when a suitable gadget chain is present on the blog	9.8	More Details
CVE-2023-46226	Remote Code Execution vulnerability in Apache IoTDB.This issue affects Apache IoTDB: from 1.0.0 through 1.2.2. Users are recommended to upgrade to version 1.3.0, which fixes the issue.	9.8	More Details
CVE-2020-36770	pkg_postinst in the Gentoo ebuild for Slurm through 22.05.3 unnecessarily calls chown to assign root's ownership on files in the live root filesystem. This could be exploited by the slurm user to become the owner of root-owned files.	9.8	More Details
CVE-2024-0552	Intumit inc. SmartRobot's web framwork has a remote code execution vulnerability. An unauthorized remote attacker can exploit this vulnerability to execute arbitrary commands on the remote server.	9.8	More Details
CVE-2023-49262	The authentication mechanism can be bypassed by overflowing the value of the Cookie "authentication" field, provided there is an active user session.	9.8	More Details
CVE-2023-49255	The router console is accessible without authentication at "data" field, and while a user needs to be logged in in order to modify the configuration, the session state is shared. If any other user is currently logged in, the anonymous user can execute commands in the context of the authenticated one. If the logged in user has administrative privileges, it is possible to use webadmin service configuration commands to create a new admin user with a chosen password.	9.8	More Details
CVE-2023-6979	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ivole_import_upload_csv AJAX action in all versions up to, and including, 5.38.9. This makes it possible for authenticated attackers, with author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2023-51989	D-Link DIR-822+ V1.0.2 contains a login bypass in the HNAP1 interface, which allows attackers to log in to administrator accounts with empty passwords.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6567	The LearnPress plugin for WordPress is vulnerable to time-based SQL Injection via the ‘order_by’ parameter in all versions up to, and including, 4.2.5.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2023-51956	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formSetIptv	9.8	More Details
CVE-2023-47862	A local file inclusion vulnerability exists in the getLanguageFromBrowser functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	9.8	More Details
CVE-2023-6316	The MW WP Form plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the '_single_file_upload' function in versions up to, and including, 5.0.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2023-51964	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo.	9.8	More Details
CVE-2023-51963	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo.	9.8	More Details
CVE-2023-51960	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv.	9.8	More Details
CVE-2023-51959	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv.	9.8	More Details
CVE-2023-51958	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv.	9.8	More Details
CVE-2023-51957	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv.	9.8	More Details
CVE-2023-51955	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formSetIptv.	9.8	More Details
CVE-2023-51962	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo.	9.8	More Details
CVE-2023-51954	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formSetIptv.	9.8	More Details
CVE-2023-51953	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51952	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formSetIptv.	9.8	More Details
CVE-2023-51966	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo.	9.8	More Details
CVE-2023-51961	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formGetIptv.	9.8	More Details
CVE-2023-51972	Tenda AX1803 v1.0.0.1 was discovered to contain a command injection vulnerability via the function fromAdvSetLanIp.	9.8	More Details
CVE-2023-51971	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function getIptvInfo.	9.8	More Details
CVE-2020-26629	A JQuery Unrestricted Arbitrary File Upload vulnerability was discovered in Hospital Management System V4.0 which allows an unauthenticated attacker to upload any file to the server.	9.8	More Details
CVE-2023-49599	An insufficient entropy vulnerability exists in the salt generation functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted series of HTTP requests can lead to privilege escalation. An attacker can gather system information via HTTP requests and brute force the salt offline, leading to forging a legitimate password recovery code for the admin user.	9.8	More Details
CVE-2023-51965	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo.	9.8	More Details
CVE-2023-51967	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function getIptvInfo.	9.8	More Details
CVE-2023-51970	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv.	9.8	More Details
CVE-2023-52032	TOTOlink EX1200T V4.1.2cu.5232_B20210713 was discovered to contain a remote command execution (RCE) vulnerability via the "main" function.	9.8	More Details
CVE-2023-52031	TOTOlink A3700R v9.1.2u.5822_B20200513 was discovered to contain a remote command execution (RCE) vulnerability via the UploadFirmwareFile function.	9.8	More Details
CVE-2023-52030	TOTOlink A3700R v9.1.2u.5822_B20200513 was discovered to contain a remote command execution (RCE) vulnerability via the setOpModeCfg function.	9.8	More Details
CVE-2023-52029	TOTOlink A3700R v9.1.2u.5822_B20200513 was discovered to contain a remote command execution (RCE) vulnerability via the setDiagnosisCfg function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52028	TOTOlink A3700R v9.1.2u.5822_B20200513 was discovered to contain a remote command execution (RCE) vulnerability via the setTracerouteCfg function.	9.8	More Details
CVE-2023-52027	TOTOlink A3700R v9.1.2u.5822_B20200513 was discovered to contain a remote command execution (RCE) vulnerability via the NTPSyncWithHost function.	9.8	More Details
CVE-2023-51123	An issue discovered in D-Link dir815 v.1.01SSb08.bin allows a remote attacker to execute arbitrary code via a crafted POST request to the service parameter in the soapcgi_main function of the cgibin binary component.	9.8	More Details
CVE-2023-40414	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 10, iOS 17 and iPadOS 17, tvOS 17, macOS Sonoma 14, Safari 17. Processing web content may lead to arbitrary code execution.	9.8	More Details
CVE-2023-51126	Command injection vulnerability in /usr/www/res.php in FLIR AX8 up to 1.46.16 allows attackers to run arbitrary commands via the value parameter.	9.8	More Details
CVE-2023-31488	Hyland Perceptive Filters releases before 2023-12-08 (e.g., 11.4.0.2647), as used in Cisco IronPort Email Security Appliance Software, Cisco Secure Email Gateway, and various non-Cisco products, allow attackers to trigger a segmentation fault and execute arbitrary code via a crafted document.	9.8	More Details
CVE-2023-52064	Wuzhicms v4.1.0 was discovered to contain a SQL injection vulnerability via the $keywords parameter at /core/admin/copyfrom.php.	9.8	More Details
CVE-2023-51968	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function getIptvInfo.	9.8	More Details
CVE-2023-51969	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function getIptvInfo.	9.8	More Details
CVE-2023-48728	A cross-site scripting (xss) vulnerability exists in the functiongetOpenGraph videoName functionality of WWBN AVideo 11.6 and dev master commit 3c6bb3ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	9.6	More Details
CVE-2023-51698	Atril is a simple multi-page document viewer. Atril is vulnerable to a critical Command Injection Vulnerability. This vulnerability gives the attacker immediate access to the target system when the target user opens a crafted document or clicks on a crafted link/URL using a maliciously crafted CBT document which is a TAR archive. A patch is available at commit ce41df6.	9.6	More Details
CVE-2024-22406	Shopware is an open headless commerce platform. The Shopware application API contains a search functionality which enables users to search through information stored within their Shopware instance. The searches performed by this function can be aggregated using the parameters in the “aggregations” object. The ‘name’ field in this “aggregations” object is vulnerable SQL-injection and can be exploited using time-based SQL-queries. This issue has been addressed and users are advised to update to Shopware 6.5.7.4. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.	9.3	More Details
CVE-2023-31030	NVIDIA DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22199	This package provides universal methods to use multiple template engines with the Fiber web framework using the Views interface. This vulnerability specifically impacts web applications that render user-supplied data through this template engine, potentially leading to the execution of malicious scripts in users' browsers when visiting affected web pages. The vulnerability has been addressed, the template engine now defaults to having autoescape set to `true`, effectively mitigating the risk of XSS attacks.	9.3	More Details
CVE-2023-31029	NVIDIA DGX A100 baseboard management controller (BMC) contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	9.3	More Details
CVE-2024-21887	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.	9.1	More Details
CVE-2022-46025	Totolink N200RE_V5 V9.3.5u.6255_B20211224 is vulnerable to Incorrect Access Control. The device allows remote attackers to obtain Wi-Fi system information, such as Wi-Fi SSID and Wi-Fi password, without logging into the management page.	9.1	More Details
CVE-2023-46943	An issue was discovered in NPM's package @evershop/evershop before version 1.0.0-rc.8. The HMAC secret used for generating tokens is hardcoded as "secret". A weak HMAC secret poses a risk because attackers can use the predictable secret to create valid JSON Web Tokens (JWTs), allowing them access to important information and actions within the application.	9.1	More Details
CVE-2024-21638	Azure IPAM (IP Address Management) is a lightweight solution developed on top of the Azure platform designed to help Azure customers manage their IP Address space easily and effectively. By design there is no write access to customers' Azure environments as the Service Principal used is only assigned the Reader role at the root Management Group level. Until recently, the solution lacked the validation of the passed in authentication token which may result in attacker impersonating any privileged user to access data stored within the IPAM instance and subsequently from Azure, causing an elevation of privilege. This vulnerability has been patched in version 3.0.0.	9.1	More Details
CVE-2023-52101	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity.	9.1	More Details
CVE-2023-6699	The WP Compress – Image Optimizer [All-In-One] plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.10.33 via the css parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	9.1	More Details
CVE-2023-31024	NVIDIA DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause stack memory corruption by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	9.0	More Details
CVE-2023-47861	A cross-site scripting (xss) vulnerability exists in the channelBody.php user name functionality of WWBN AVideo 11.6 and dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	9.0	More Details
CVE-2024-22206	Clerk helps developers build user management. Unauthorized access or privilege escalation due to a logic flaw in auth() in the App Router or getAuth() in the Pages Router. This vulnerability was patched in version 4.29.3.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-21672	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives).	8.8	More Details
CVE-2023-51063	QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 was discovered to contain a DOM Based Reflected Cross Site Scripting (XSS) vulnerability within the component qnme-ajax?method=tree_level.	8.8	More Details
CVE-2024-0573	A vulnerability has been found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip 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-250789 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0574	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this issue is the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sTime 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-250790 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0575	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been classified as critical. This affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command 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-250791. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0535	A vulnerability classified as critical was found in Tenda PA6 1.0.1.21. Affected by this vulnerability is the function cgiPortMapAdd of the file /portmap of the component httpd. The manipulation of the argument groupName 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-250705 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2021-24566	The WooCommerce Currency Switcher FOX WordPress plugin before 1.3.7 was vulnerable to LFI attacks via the "woocs" shortcode.	8.8	More Details
CVE-2021-24869	The WP Fastest Cache WordPress plugin before 0.9.5 does not escape user input in the set_urls_with_terms method before using it in a SQL statement, leading to an SQL injection exploitable by low privilege users such as subscriber	8.8	More Details
CVE-2023-44250	An improper privilege management vulnerability [CWE-269] in a Fortinet FortiOS HA cluster version 7.4.0 through 7.4.1 and 7.2.5 and in a FortiProxy HA cluster version 7.4.0 through 7.4.1 allows an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51066	An authenticated remote code execution vulnerability in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows attackers to arbitrarily execute commands.	8.8	More Details
CVE-2023-33472	An issue was discovered in Scada-LTS v2.7.5.2 build 4551883606 and before, allows remote attackers with low-level authentication to escalate privileges, execute arbitrary code, and obtain sensitive information via Event Handlers function.	8.8	More Details
CVE-2024-0578	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File 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-250794 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-49589	An insufficient entropy vulnerability exists in the userRecoverPass.php recoverPass generation functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to an arbitrary user password recovery. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2023-49647	Improper access control in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows before version 5.16.10 may allow an authenticated user to conduct an escalation of privilege via local access.	8.8	More Details
CVE-2023-4536	The My Account Page Editor WordPress plugin before 1.3.2 does not validate the profile picture to be uploaded, allowing any authenticated users, such as subscriber to upload arbitrary files to the server, leading to RCE	8.8	More Details
CVE-2023-50159	In ScaleFusion (Windows Desktop App) agent 10.5.2, Kiosk mode application restrictions can be bypassed allowing arbitrary code to be executed. This is fixed in 10.5.7 by preventing the launching of the file explorer in Agent-based Multi-App and Single App Kiosk mode.	8.8	More Details
CVE-2023-51748	ScaleFusion 10.5.2 does not properly limit users to the Edge application because Ctrl-O and Ctrl-S can be used. This is fixed in 10.5.7 by preventing the launching of the file explorer in Agent-based Multi-App and Single App Kiosk mode.	8.8	More Details
CVE-2023-51749	ScaleFusion 10.5.2 does not properly limit users to the Edge application because a search can be made from a tooltip. NOTE: the vendor's position is "Not vulnerable if the default Windows device profile configuration is used which utilizes modern management with website allow-listing rules."	8.8	More Details
CVE-2023-6373	The ArtPlacer Widget WordPress plugin before 2.20.7 does not sanitize and escape the "id" parameter before submitting the query, leading to a SQLI exploitable by editors and above. Note: Due to the lack of CSRF check, the issue could also be exploited via a CSRF against a logged editor (or above)	8.8	More Details
CVE-2024-0576	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been declared as critical. This vulnerability affects the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sPort 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-250792. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0536	A vulnerability, which was classified as critical, has been found in Tenda W9 1.0.0.7(4456). Affected by this issue is the function setWrlAccessList of the component httpd. The manipulation of the argument ssidIndex 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-250706 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0572	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser 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-250788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0571	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. This issue affects the function setSmsCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument text 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-250787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0537	A vulnerability, which was classified as critical, was found in Tenda W9 1.0.0.7(4456). This affects the function setWrlBasicInfo of the component httpd. The manipulation of the argument ssidIndex 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-250707. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-21773	Multiple TP-LINK products allow a network-adjacent unauthenticated attacker with access to the product from the LAN port or Wi-Fi to execute arbitrary OS commands on the product that has pre-specified target devices and blocked URLs in parental control settings.	8.8	More Details
CVE-2023-22526	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program	8.8	More Details
CVE-2024-21833	Multiple TP-LINK products allow a network-adjacent unauthenticated attacker with access to the product to execute arbitrary OS commands. The affected device, with the initial configuration, allows login only from the LAN port or Wi-Fi.	8.8	More Details
CVE-2024-21673	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42866	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.5, iOS 16.6 and iPadOS 16.6, tvOS 16.6, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-51059	An issue in MOKO TECHNOLOGY LTD MOKOSmart MKGW1 BLE Gateway v.1.1.1 and before allows a remote attacker to escalate privileges via the session management component of the administrative web interface.	8.8	More Details
CVE-2023-43449	An issue in HummerRisk HummerRisk v.1.10 thru 1.4.1 allows an authenticated attacker to execute arbitrary code via a crafted request to the service/LicenseService component.	8.8	More Details
CVE-2023-42833	A correctness issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14, Safari 17, iOS 17 and iPadOS 17. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-47460	SQL injection vulnerability in Knovos Discovery v.22.67.0 allows a remote attacker to execute arbitrary code via the /DiscoveryProcess/Service/Admin.svc/getGridColumnStructure component.	8.8	More Details
CVE-2023-41060	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. A remote user may be able to cause kernel code execution.	8.8	More Details
CVE-2023-6991	The JSM file_get_contents() Shortcode WordPress plugin before 2.7.1 does not validate one of its shortcode's parameters before making a request to it, which could allow users with contributor role and above to perform SSRF attacks.	8.8	More Details
CVE-2023-5448	The WP Register Profile With Shortcode plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.5.9. This is due to missing or incorrect nonce validation on the update_password_validate function. This makes it possible for unauthenticated attackers to reset a user's password via a forged request granted they can trick the user into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-0252	ManageEngine ADSelfService Plus versions 6401 and below are vulnerable to the remote code execution due to the improper handling in the load balancer component. Authentication is required in order to exploit this vulnerability.	8.8	More Details
CVE-2024-0542	A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been rated as critical. Affected by this issue is the function formWifiMacFilterGet 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-250712. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0541	A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been declared as critical. Affected by this vulnerability is the function formAddSysLogRule of the component httpd. The manipulation of the argument sysRulenEn 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-250711. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0539	A vulnerability was found in Tenda W9 1.0.0.7(4456) and classified as critical. This issue affects the function formQosManage_user of the component httpd. The manipulation of the argument ssidIndex 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-250709 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0538	A vulnerability has been found in Tenda W9 1.0.0.7(4456) and classified as critical. This vulnerability affects the function formQosManage_auto of the component httpd. The manipulation of the argument ssidIndex 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-250708. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-0577	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects 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 initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250793 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-6878	The Slick Social Share Buttons plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'dcssb_ajax_update' function in versions up to, and including, 2.4.11. This makes it possible for authenticated attackers, with subscriber-level permissions or above to update the site options arbitrarily.	8.8	More Details
CVE-2023-49257	An authenticated user is able to upload an arbitrary CGI-compatible file using the certificate upload utility and execute it with the root user privileges.	8.8	More Details
CVE-2023-6735	Privilege escalation in mk_tsm agent plugin in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows local user to escalate privileges	8.8	More Details
CVE-2023-49471	Blind Server-Side Request Forgery (SSRF) vulnerability in karlomikus Bar Assistant before version 3.2.0 does not validate a parameter before making a request through Image::make(), which could allow authenticated remote attackers to execute arbitrary code.	8.8	More Details
CVE-2023-40250	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Hancom HCell on Windows allows Overflow Buffers.This issue affects HCell: 12.0.0.893.	8.8	More Details
CVE-2023-48252	The vulnerability allows an authenticated remote attacker to perform actions exceeding their authorized access via crafted HTTP requests.	8.8	More Details
CVE-2023-48253	The vulnerability allows a remote authenticated attacker to read or update arbitrary content of the authentication database via a crafted HTTP request. By abusing this vulnerability it is possible to exfiltrate other users' password hashes or update them with arbitrary values and access their accounts.	8.8	More Details
CVE-2023-51949	Verydows v2.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /protected/controller/backend/role_controller	8.8	More Details
CVE-2023-6740	Privilege escalation in jar_signature agent plugin in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows local user to escalate privileges	8.8	More Details
CVE-2023-49254	Authenticated user can execute arbitrary commands in the context of the root user by providing payload in the "destination" field of the network test tools. This is similar to the vulnerability CVE-2021-28151 mitigated on the user interface level by blacklisting characters with JavaScript, however, it can still be exploited by sending POST requests directly.	8.8	More Details
CVE-2024-0519	Out of bounds memory access in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0518	Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-31211	Insufficient authentication flow in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows attacker to use locked credentials	8.8	More Details
CVE-2024-0517	Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-48909	An issue was discovered in Jave2 version 3.3.1, allows attackers to execute arbitrary code via the FFmpeg function.	8.8	More Details
CVE-2023-5504	The BackWPup plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.0.1 via the Log File Folder. This allows authenticated attackers to store backups in arbitrary folders on the server provided they can be written to by the server. Additionally, default settings will place an index.php and a .htaccess file into the chosen directory (unless already present) when the first backup job is run that are intended to prevent directory listing and file access. This means that an attacker could set the backup directory to the root of another site in a shared environment and thus disable that site.	8.7	More Details
CVE-2023-48297	Discourse is a platform for community discussion. The message serializer uses the full list of expanded chat mentions (@all and @here) which can lead to a very long array of users. This issue was patched in versions 3.1.4 and beta 3.2.0.beta5.	8.6	More Details
CVE-2022-45794	An attacker with network access to the affected PLC (CJ-series and CS-series PLCs, all versions) may use a network protocol to read and write files on the PLC internal memory and memory card.	8.6	More Details
CVE-2023-48730	A cross-site scripting (xss) vulnerability exists in the navbarMenuAndLogo.php user name functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	8.5	More Details
CVE-2023-50729	Traccar is an open source GPS tracking system. Prior to 5.11, Traccar is affected by an unrestricted file upload vulnerability in File feature allows attackers to execute arbitrary code on the server. This vulnerability is more prevalent because Traccar is recommended to run web servers as root user. It is also more dangerous because it can write or overwrite files in arbitrary locations. Version 5.11 was published to fix this vulnerability.	8.4	More Details
CVE-2023-31003	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254658.	8.4	More Details
CVE-2023-45234	EDK2's Network Package is susceptible to a buffer overflow vulnerability when processing DNS Servers option from a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.	8.3	More Details
CVE-2023-45235	EDK2's Network Package is susceptible to a buffer overflow vulnerability when handling Server ID option from a DHCPv6 proxy Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.	8.3	More Details
CVE-2023-45230	EDK2's Network Package is susceptible to a buffer overflow vulnerability via a long server ID option in DHCPv6 client. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20916	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). The supported version that is affected is 13.5.0.0. Easily exploitable vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L).	8.3	More Details
CVE-2023-46805	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.	8.2	More Details
CVE-2023-48266	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	8.1	More Details
CVE-2023-48262	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	8.1	More Details
CVE-2023-5905	The DeMomentSomTres WordPress Export Posts With Images WordPress plugin through 20220825 does not check authorization of requests to export the blog data, allowing any logged in user, such as subscribers to export the contents of the blog, including restricted and unpublished posts, as well as passwords of protected posts.	8.1	More Details
CVE-2023-48263	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	8.1	More Details
CVE-2023-6634	The LearnPress plugin for WordPress is vulnerable to Command Injection in all versions up to, and including, 4.2.5.7 via the get_content function. This is due to the plugin making use of the call_user_func function with user input. This makes it possible for unauthenticated attackers to execute any public function with one parameter, which could result in remote code execution.	8.1	More Details
CVE-2023-48264	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	8.1	More Details
CVE-2023-51073	An issue in Buffalo LS210D v.1.78-0.03 allows a remote attacker to execute arbitrary code via the Firmware Update Script at /etc/init.d/update_notifications.sh.	8.1	More Details
CVE-2023-48265	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	8.1	More Details
CVE-2023-41056	Redis is an in-memory database that persists on disk. Redis incorrectly handles resizing of memory buffers which can result in integer overflow that leads to heap overflow and potential remote code execution. This issue has been patched in version 7.0.15 and 7.2.4.	8.1	More Details
CVE-2022-3899	The 3dprint WordPress plugin before 3.5.6.9 does not protect against CSRF attacks in the modified version of Tiny File Manager included with the plugin, allowing an attacker to craft a malicious request that will delete any number of files or directories on the target server by tricking a logged in admin into submitting a form.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6220	The Piotnet Forms plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'piotnetforms_ajax_form_builder' function in versions up to, and including, 1.0.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.1	More Details
CVE-2023-50123	The number of attempts to bring the Hozard Alarm system (alarmsystemen) v1.0 to a disarmed state is not limited. This could allow an attacker to perform a brute force on the SMS authentication, to bring the alarm system to a disarmed state.	8.1	More Details
CVE-2023-48251	The vulnerability allows a remote attacker to authenticate to the SSH service with root privileges through a hidden hard-coded account.	8.1	More Details
CVE-2023-48250	The vulnerability allows a remote attacker to authenticate to the web application with high privileges through multiple hidden hard-coded accounts.	8.1	More Details
CVE-2023-48243	The vulnerability allows a remote attacker to upload arbitrary files in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request. By abusing this vulnerability, it is possible to obtain remote code execution (RCE) with root privileges on the device.	8.1	More Details
CVE-2024-21821	Multiple TP-LINK products allow a network-adjacent authenticated attacker with access to the product from the LAN port or Wi-Fi to execute arbitrary OS commands.	8.0	More Details
CVE-2023-42136	PAX Android based POS devices with PayDroid_8.1.0_Sagittarius_V11.1.50_20230614 or earlier can allow the execution of arbitrary commands with system account privilege by shell injection starting with a specific word. The attacker must have shell access to the device in order to exploit this vulnerability.	7.8	More Details
CVE-2023-42137	PAX Android based POS devices with PayDroid_8.1.0_Sagittarius_V11.1.50_20230614 or earlier can allow for command execution with high privileges by using malicious symlinks. The attacker must have shell access to the device in order to exploit this vulnerability.	7.8	More Details
CVE-2023-42826	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to arbitrary code execution.	7.8	More Details
CVE-2023-6040	An out-of-bounds access vulnerability involving netfilter was reported and fixed as: f1082dd31fe4 (netfilter: nf_tables: Reject tables of unsupported family); While creating a new netfilter table, lack of a safeguard against invalid nf_tables family (pf) values within `nf_tables_newtable` function enables an attacker to achieve out-of-bounds access.	7.8	More Details
CVE-2023-41075	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-41974	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2024-0562	A use-after-free flaw was found in the Linux Kernel. When a disk is removed, bdi_unregister is called to stop further write-back and waits for associated delayed work to complete. However, wb_inode_writeback_end() may schedule bandwidth estimation work after this has completed, which can result in the timer attempting to access the recently freed bdi_writeback.	7.8	More Details
CVE-2023-7206	In Horner Automation Cscape versions 9.90 SP10 and prior, local attackers are able to exploit this vulnerability if a user opens a malicious CSP file, which would result in execution of arbitrary code on affected installations of Cscape.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32383	This issue was addressed by forcing hardened runtime on the affected binaries at the system level. This issue is fixed in macOS Monterey 12.6.6, macOS Big Sur 11.7.7, macOS Ventura 13.4. An app may be able to inject code into sensitive binaries bundled with Xcode.	7.8	More Details
CVE-2023-42828	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.5. An app may be able to gain root privileges.	7.8	More Details
CVE-2024-22190	GitPython is a python library used to interact with Git repositories. There is an incomplete fix for CVE-2023-40590. On Windows, GitPython uses an untrusted search path if it uses a shell to run `git`, as well as when it runs `bash.exe` to interpret hooks. If either of those features are used on Windows, a malicious `git.exe` or `bash.exe` may be run from an untrusted repository. This issue has been patched in version 3.1.41.	7.8	More Details
CVE-2023-51257	An invalid memory write issue in Jasper-Software Jasper v.4.1.1 and before allows a local attacker to execute arbitrary code.	7.8	More Details
CVE-2023-42870	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-42871	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-42933	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2023-32401	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.6.6, macOS Big Sur 11.7.7, macOS Ventura 13.4. Parsing an office document may lead to an unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2022-47965	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-32378	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-46721	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-3604	The Contact Form Entries WordPress plugin before 1.3.0 does not validate data when its output in a CSV file, which could lead to CSV injection.	7.8	More Details
CVE-2023-32366	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4. Processing a font file may lead to arbitrary code execution.	7.8	More Details
CVE-2023-29445	An uncontrolled search path element vulnerability (DLL hijacking) has been discovered that could allow a locally authenticated adversary to escalate privileges to SYSTEM.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48257	The vulnerability allows a remote attacker to access sensitive data inside exported packages or obtain up to Remote Code Execution (RCE) with root privileges on the device. The vulnerability can be exploited directly by authenticated users, via crafted HTTP requests, or indirectly by unauthenticated users, by accessing already-exported backup packages, or crafting an import package and inducing an authenticated victim into sending the HTTP upload request.	7.8	More Details
CVE-2024-0582	A memory leak flaw was found in the Linux kernel's io_uring functionality in how a user registers a buffer ring with IORING_REGISTER_PBUF_RING, mmap() it, and then frees it. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2024-23347	Prior to v176, when opening a new project Meta Spark Studio would execute scripts defined inside of a package.json file included as part of that project. Those scripts would have the ability to execute arbitrary code on the system as the application.	7.8	More Details
CVE-2022-47915	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-50671	In exiftags 1.01, nikon_prop1 in nikon.c has a heap-based buffer overflow (write of size 28) because snprintf can write to an unexpected address.	7.8	More Details
CVE-2024-22197	Nginx-ui is online statistics for Server Indicators Monitor CPU usage, memory usage, load average, and disk usage in real-time. The `Home > Preference` page exposes a small list of nginx settings such as `Nginx Access Log Path` and `Nginx Error Log Path`. However, the API also exposes `test_config_cmd`, `reload_cmd` and `restart_cmd`. While the UI doesn't allow users to modify any of these settings, it is possible to do so by sending a request to the API. This issue may lead to authenticated Remote Code Execution, Privilege Escalation, and Information Disclosure. This issue has been patched in version 2.0.0.beta.9.	7.7	More Details
CVE-2023-4812	An issue has been discovered in GitLab EE affecting all versions starting from 15.3 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2. The required CODEOWNERS approval could be bypassed by adding changes to a previously approved merge request.	7.6	More Details
CVE-2024-21637	Authentik is an open-source Identity Provider. Authentik is a vulnerable to a reflected Cross-Site Scripting vulnerability via JavaScript-URIs in OpenID Connect flows with `response_mode=form_post`. This relatively user could use the described attacks to perform a privilege escalation. This vulnerability has been patched in versions 2023.10.6 and 2023.8.6.	7.6	More Details
CVE-2024-22408	Shopware is an open headless commerce platform. The implemented Flow Builder functionality in the Shopware application does not adequately validate the URL used when creating the "call webhook" action. This enables malicious users to perform web requests to internal hosts. This issue has been fixed in the Commercial Plugin release 6.5.7.4 or with the Security Plugin. For installations with Shopware 6.4 the Security plugin is recommended to be installed and up to date. For older versions of 6.4 and 6.5 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.	7.6	More Details
CVE-2024-20924	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Audit Vault and Database Firewall. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H).	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4818	PAX A920 device allows to downgrade bootloader due to a bug in its version check. The signature is correctly checked and only bootloader signed by PAX can be used. The attacker must have physical USB access to the device in order to exploit this vulnerability.	7.6	More Details
CVE-2024-21614	An Improper Check for Unusual or Exceptional Conditions vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to cause rpd to crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when NETCONF and gRPC are enabled, and a specific query is executed via Dynamic Rendering (DREND), rpd will crash and restart. Continuous execution of this specific query will cause a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS * 22.2 versions earlier than 22.2R2-S2, 22.2R3; * 22.3 versions earlier than 22.3R2, 22.3R3. Juniper Networks Junos OS Evolved * 22.2 versions earlier than 22.2R2-S2-EVO, 22.2R3-EVO; * 22.3 versions earlier than 22.3R2-EVO, 22.3R3-EVO. This issue does not affect Juniper Networks: Junos OS versions earlier than 22.2R1; Junos OS Evolved versions earlier than 22.2R1-EVO.	7.5	More Details
CVE-2024-21612	An Improper Handling of Syntactically Invalid Structure vulnerability in Object Flooding Protocol (OFP) service of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS Evolved platforms, when specific TCP packets are received on an open OFP port, the OFP crashes leading to a restart of Routine Engine (RE). Continuous receipt of these specific TCP packets will lead to a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS Evolved * All versions earlier than 21.2R3-S7-EVO; * 21.3 versions earlier than 21.3R3-S5-EVO ; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO ; * 22.3 versions earlier than 22.3R3-EVO; * 22.4 versions earlier than 22.4R2-EVO, 22.4R3-EVO.	7.5	More Details
CVE-2024-21611	A Missing Release of Memory after Effective Lifetime vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). In a Juniper Flow Monitoring (jflow) scenario route churn that causes BGP next hops to be updated will cause a slow memory leak and eventually a crash and restart of rpd. Thread level memory utilization for the areas where the leak occurs can be checked using the below command: user@host> show task memory detail l match so_in so_in6 28 32 344450 11022400 344760 11032320 so_in 8 16 1841629 29466064 1841734 29467744 This issue affects: Junos OS * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Junos OS Evolved * 21.4-EVO versions earlier than 21.4R3-EVO; * 22.1-EVO versions earlier than 22.1R3-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO. This issue does not affect: Juniper Networks Junos OS versions earlier than 21.4R1. Juniper Networks Junos OS Evolved versions earlier than 21.4R1.	7.5	More Details
CVE-2023-48166	A directory traversal vulnerability in the SOAP Server integrated in Atos Unify OpenScape Voice V10 before V10R3.26.1 allows a remote attacker to view the contents of arbitrary files in the local file system. An unauthenticated attacker might obtain sensitive files that allow for the compromise of the underlying system.	7.5	More Details
CVE-2023-31035	NVIDIA DGX A100 SBIOS contains a vulnerability where an attacker may cause an SMI callout vulnerability that could be used to execute arbitrary code at the SMM level. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, and information disclosure.	7.5	More Details
CVE-2023-31036	NVIDIA Triton Inference Server for Linux and Windows contains a vulnerability where, when it is launched with the non-default command line option --model-control explicit, an attacker may use the model load API to cause a relative path traversal. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21606	A Double Free vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). In a remote access VPN scenario, if a "tcp-encap-profile" is configured and a sequence of specific packets is received, a flowd crash and restart will be observed. This issue affects Juniper Networks Junos OS on SRX Series: * All versions earlier than 20.4R3-S8; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S3; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3.	7.5	More Details
CVE-2024-21595	An Improper Validation of Syntactic Correctness of Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). If an attacker sends high rate of specific ICMP traffic to a device with VXLAN configured, this causes a deadlock of the PFE and results in the device becoming unresponsive. A manual restart will be required to recover the device. This issue only affects EX4100, EX4400, EX4600, QFX5000 Series devices. This issue affects: Juniper Networks Junos OS * 21.4R3 versions earlier than 21.4R3-S4; * 22.1R3 versions earlier than 22.1R3-S3; * 22.2R2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2; * 23.1 versions earlier than 23.1R2.	7.5	More Details
CVE-2023-51810	SQL injection vulnerability in StackIdeas EasyDiscuss v.5.0.5 and fixed in v.5.0.10 allows a remote attacker to obtain sensitive information via a crafted request to the search parameter in the Users module.	7.5	More Details
CVE-2024-21604	An Allocation of Resources Without Limits or Throttling vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a high rate of specific valid packets are processed by the routing engine (RE) this will lead to a loss of connectivity of the RE with other components of the chassis and thereby a complete and persistent system outage. Please note that a carefully designed lo0 firewall filter will block or limit these packets which should prevent this issue from occurring. The following log messages can be seen when this issue occurs: <host> kernel: nf_conntrack: nf_conntrack: table full, dropping packet This issue affects Juniper Networks Junos OS Evolved: * All versions earlier than 20.4R3-S7-EVO; * 21.2R1-EVO and later versions; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S2-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO; * 22.4-EVO versions earlier than 22.4R2-EVO.	7.5	More Details
CVE-2024-21616	An Improper Validation of Syntactic Correctness of Input vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On all Junos OS MX Series and SRX Series platforms, when SIP ALG is enabled, and a specific SIP packet is received and processed, NAT IP allocation fails for genuine traffic, which causes Denial of Service (DoS). Continuous receipt of this specific SIP ALG packet will cause a sustained DoS condition. NAT IP usage can be monitored by running the following command. user@srx> show security nat resource-usage source-pool <source_pool_name> Pool name: source_pool_name .. Address Factor-index Port-range Used Avail Total Usage X.X.X.X 0 Single Ports 50258 52342 62464 96% <<<<< - Alg Ports 0 2048 2048 0% This issue affects: Juniper Networks Junos OS on MX Series and SRX Series * All versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2.	7.5	More Details
CVE-2023-51070	An access control issue in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to arbitrarily adjust sensitive SMB settings on the QStar Server.	7.5	More Details
CVE-2023-49261	The "tokenKey" value used in user authorization is visible in the HTML source of the login page.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46942	Lack of authentication in NPM's package @evershop/evershop before version 1.0.0-rc.8, allows remote attackers to obtain sensitive information via improper authorization in GraphQL endpoints.	7.5	More Details
CVE-2023-51804	An issue in rymcu forest v.0.02 allows a remote attacker to obtain sensitive information via manipulation of the HTTP body URL in the com.rymcu.forest.web.api.common.UploadController file.	7.5	More Details
CVE-2023-49259	The authentication cookies are generated using an algorithm based on the username, hardcoded secret and the up-time, and can be guessed in a reasonable time.	7.5	More Details
CVE-2023-51065	Incorrect access control in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to obtain system backups and other sensitive information from the QStar Server.	7.5	More Details
CVE-2023-51282	An issue in mingSoft MCMS v.5.2.4 allows a a remote attacker to obtain sensitive information via a crafted script to the password parameter.	7.5	More Details
CVE-2023-52288	An issue was discovered in the flaskcode package through 0.0.8 for Python. An unauthenticated directory traversal, exploitable with a GET request to a /resource-data/<file_path>.txt URI (from views.py), allows attackers to read arbitrary files.	7.5	More Details
CVE-2023-52289	An issue was discovered in the flaskcode package through 0.0.8 for Python. An unauthenticated directory traversal, exploitable with a POST request to a /update-resource-data/<file_path> URI (from views.py), allows attackers to write to arbitrary files.	7.5	More Details
CVE-2023-34061	Cloud Foundry routing release versions from v0.163.0 to v0.283.0 are vulnerable to a DOS attack. An unauthenticated attacker can use this vulnerability to force route pruning and therefore degrade the service availability of the Cloud Foundry deployment.	7.5	More Details
CVE-2023-49256	It is possible to download the configuration backup without authorization and decrypt included passwords using hardcoded static key.	7.5	More Details
CVE-2023-6029	The EazyDocs WordPress plugin before 2.3.6 does not have authorization and CSRF checks when handling documents and does not ensure that they are documents from the plugin, allowing unauthenticated users to delete arbitrary posts, as well as add and delete documents/sections.	7.5	More Details
CVE-2023-48383	NetVision Information airPASS has a path traversal vulnerability within its parameter in a specific URL. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	7.5	More Details
CVE-2023-49568	A denial of service (DoS) vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to perform denial of service attacks by providing specially crafted responses from a Git server which triggers resource exhaustion in go-git clients. Applications using only the in-memory filesystem supported by go-git are not affected by this vulnerability. This is a go-git implementation issue and does not affect the upstream git cli.	7.5	More Details
CVE-2023-6266	The Backup Migration plugin for WordPress is vulnerable to unauthorized access of data due to insufficient path and file validation on the BMI_BACKUP case of the handle_downloading function in all versions up to, and including, 1.3.6. This makes it possible for unauthenticated attackers to download back-up files which can contain sensitive information such as user passwords, PII, database credentials, and much more.	7.5	More Details
CVE-2023-31032	NVIDIA DGX A100 SBIOS contains a vulnerability where a user may cause a dynamic variable evaluation by local access. A successful exploit of this vulnerability may lead to denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22409	DataHub is an open-source metadata platform. In affected versions a low privileged user could remove a user, edit group members, or edit another user's profile information. The default privileges gave too many broad permissions to low privileged users. These have been constrained in PR #9067 to prevent abuse. This issue can result in privilege escalation for lower privileged users up to admin privileges, potentially, if a group with admin privileges exists. May not impact instances that have modified default privileges. This issue has been addressed in datahub version 0.12.1. Users are advised to upgrade.	7.5	More Details
CVE-2024-22362	Drupal contains a vulnerability with improper handling of structural elements. If this vulnerability is exploited, an attacker may be able to cause a denial-of-service (DoS) condition.	7.5	More Details
CVE-2023-51127	FLIR AX8 thermal sensor cameras up to and including 1.46.16 are vulnerable to Directory Traversal due to improper access restriction. This vulnerability allows an unauthenticated, remote attacker to obtain arbitrary sensitive file contents by uploading a specially crafted symbolic link file.	7.5	More Details
CVE-2023-52116	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device.	7.5	More Details
CVE-2023-52099	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52100	The Celia Keyboard module has a vulnerability in access control. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-40393	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14. Photos in the Hidden Photos Album may be viewed without authentication.	7.5	More Details
CVE-2023-52102	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52104	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52105	The nearby module has a privilege escalation vulnerability. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2024-0553	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981.	7.5	More Details
CVE-2024-0567	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.	7.5	More Details
CVE-2023-1405	The Formidable Forms WordPress plugin before 6.2 unserializes user input, which could allow anonymous users to perform PHP Object Injection when a suitable gadget is present.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52114	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2023-49738	An information disclosure vulnerability exists in the image404Raw.php functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.	7.5	More Details
CVE-2023-45232	EDK2's Network Package is susceptible to an infinite loop vulnerability when parsing unknown options in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.	7.5	More Details
CVE-2023-45139	fontTools is a library for manipulating fonts, written in Python. The subsetting module has a XML External Entity Injection (XXE) vulnerability which allows an attacker to resolve arbitrary entities when a candidate font (OT-SVG fonts), which contains a SVG table, is parsed. This allows attackers to include arbitrary files from the filesystem fontTools is running on or make web requests from the host system. This vulnerability has been patched in version 4.43.0.	7.5	More Details
CVE-2023-45233	EDK2's Network Package is susceptible to an infinite lop vulnerability when parsing a PadN option in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.	7.5	More Details
CVE-2023-4703	The All in One B2B for WooCommerce WordPress plugin through 1.0.3 does not properly validate parameters when updating user details, allowing an unauthenticated attacker to update the details of any user. Updating the password of an Admin user leads to privilege escalation.	7.5	More Details
CVE-2023-5922	The Royal Elementor Addons and Templates WordPress plugin before 1.3.81 does not ensure that users accessing posts via an AJAX action (and REST endpoint, currently disabled in the plugin) have the right to do so, allowing unauthenticated users to access arbitrary draft, private and password protected posts/pages content	7.5	More Details
CVE-2023-49427	Buffer Overflow vulnerability in Tenda AX12 V22.03.01.46, allows remote attackers to cause a denial of service (DoS) via list parameter in SetNetControlList function.	7.5	More Details
CVE-2024-20932	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 17.0.9; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 21.3.8 and 22.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-48864	SEMCMS v4.8 was discovered to contain a SQL injection vulnerability via the languageID parameter in /web_inc.php.	7.5	More Details
CVE-2023-52115	The iaware module has a Use-After-Free (UAF) vulnerability. Successful exploitation of this vulnerability may affect the system functions.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21602	A NULL Pointer Dereference vulnerability in Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a specific IPv4 UDP packet is received and sent to the Routing Engine (RE) packetio crashes and restarts which causes a momentary traffic interruption. Continued receipt of such packets will lead to a sustained DoS. This issue does not happen with IPv6 packets. This issue affects Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L: * 21.4-EVO versions earlier than 21.4R3-S6-EVO; * 22.1-EVO versions earlier than 22.1R3-S5-EVO; * 22.2-EVO versions earlier than 22.2R2-S1-EVO, 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions earlier than 21.4R1-EVO.	7.5	More Details
CVE-2023-52113	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2024-21674	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives).	7.5	More Details
CVE-2023-52109	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52107	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52098	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2023-52108	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2023-42869	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Ventura 13.4, iOS 16.5 and iPadOS 16.5. Multiple issues in libxml2.	7.5	More Details
CVE-2023-44112	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-44117	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52110	The sensor module has an out-of-bounds access vulnerability.Successful exploitation of this vulnerability may affect availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4566	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-52111	Authorization vulnerability in the BootLoader module. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2023-42463	Wazuh is a free and open source platform used for threat prevention, detection, and response. This bug introduced a stack overflow hazard that could allow a local privilege escalation. This vulnerability was patched in version 4.5.3.	7.4	More Details
CVE-2023-21901	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L).	7.4	More Details
CVE-2024-21589	An Improper Access Control vulnerability in the Juniper Networks Paragon Active Assurance Control Center allows an unauthenticated network-based attacker to access reports without authenticating, potentially containing sensitive configuration information. A feature was introduced in version 3.1.0 of the Paragon Active Assurance Control Center which allows users to selectively share account data. By exploiting this vulnerability, it is possible to access reports without being logged in, resulting in the opportunity for malicious exfiltration of user data. Note that the Paragon Active Assurance Control Center SaaS offering is not affected by this issue. This issue affects Juniper Networks Paragon Active Assurance versions 3.1.0, 3.2.0, 3.2.2, 3.3.0, 3.3.1, 3.4.0. This issue does not affect Juniper Networks Paragon Active Assurance versions earlier than 3.1.0.	7.4	More Details
CVE-2024-20918	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20952	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	7.4	More Details
CVE-2024-0480	A vulnerability was found in Taokeyun up to 1.0.5. It has been declared as critical. Affected by this vulnerability is the function index of the file application/index/controller/m/Drs.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250585 was assigned to this vulnerability.	7.3	More Details
CVE-2024-0510	A vulnerability, which was classified as critical, has been found in HaoKeKeJi YiQiNiu up to 3.1. Affected by this issue is the function http_post of the file /application/pay/controller/Api.php. 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. The identifier of this vulnerability is VDB-250652.	7.3	More Details
CVE-2024-0359	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250126 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-0479	A vulnerability was found in Taokeyun up to 1.0.5. It has been classified as critical. Affected is the function login of the file application/index/controller/m/User.php of the component HTTP POST Request Handler. The manipulation of the argument username 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-250584.	7.3	More Details
CVE-2024-0474	A vulnerability classified as critical was found in code-projects Dormitory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument username leads to sql 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-250579.	7.3	More Details
CVE-2023-6751	The Hostinger plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the function publish_website in all versions up to, and including, 1.9.7. This makes it possible for unauthenticated attackers to enable and disable maintenance mode.	7.3	More Details
CVE-2023-49810	A login attempt restriction bypass vulnerability exists in the checkLoginAttempts functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to captcha bypass, which can be abused by an attacker to brute force user credentials. An attacker can send a series of HTTP requests to trigger this vulnerability.	7.3	More Details
CVE-2024-0570	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6265. This vulnerability affects unknown code of the file /cgi-bin/cstecgi.cgi of the component Setting Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. It is recommended to upgrade the affected component. VDB-250786 is the identifier assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0429	A denial service vulnerability has been found on Hex Workshop affecting version 6.7, an attacker could send a command line file arguments and control the Structured Exception Handler (SEH) records resulting in a service shutdown.	7.3	More Details
CVE-2024-0603	A vulnerability classified as critical has been found in ZhiCms up to 4.0. This affects an unknown part of the file app/plug/controller/giftcontroller.php. The manipulation of the argument mylike leads to deserialization. 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-250839.	7.3	More Details
CVE-2023-5356	Incorrect authorization checks in GitLab CE/EE from all versions starting from 8.13 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2, allows a user to abuse slack/mattermost integrations to execute slash commands as another user.	7.3	More Details
CVE-2024-22191	Avo is a framework to create admin panels for Ruby on Rails apps. A stored cross-site scripting (XSS) vulnerability was found in the key_value field of Avo v3.2.3 and v2.46.0. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the victim's browser. The value of the key_value is inserted directly into the HTML code. In the current version of Avo (possibly also older versions), the value is not properly sanitized before it is inserted into the HTML code. This vulnerability could be used to steal sensitive information from victims that could be used to hijack victims' accounts or redirect them to malicious websites. Avo 3.2.4 and 2.47.0 include a fix for this issue. Users are advised to upgrade.	7.3	More Details
CVE-2024-22625	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_category.php?id=.	7.2	More Details
CVE-2023-6828	The Contact Form, Survey & Popup Form Plugin for WordPress – ARForms Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ arf_http_referrer_url’ parameter in all versions up to, and including, 1.5.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-46474	File Upload vulnerability PMB v.7.4.8 allows a remote attacker to execute arbitrary code and escalate privileges via a crafted PHP file uploaded to the start_import.php file.	7.2	More Details
CVE-2024-22626	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_retailer.php?id=.	7.2	More Details
CVE-2024-22627	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_distributor.php?id=.	7.2	More Details
CVE-2024-22628	Budget and Expense Tracker System v1.0 is vulnerable to SQL Injection via /expense_budget/admin/?page=reports/budget&date_start=2023-12-28&date_end=	7.2	More Details
CVE-2024-0200	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3. This vulnerability was reported via the GitHub Bug Bounty program.	7.2	More Details
CVE-2023-6336	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on MacOS allows User-Controlled Filename.This issue affects Workforce Access: before 8.7.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2655	The Contact Form by WD WordPress plugin through 1.13.23 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2023-4797	The Newsletters WordPress plugin before 4.9.3 does not properly escape user-controlled parameters when they are appended to SQL queries and shell commands, which could enable an administrator to run arbitrary commands on the server.	7.2	More Details
CVE-2022-3764	The plugin does not filter the "delete_entries" parameter from user requests, leading to an SQL Injection vulnerability.	7.2	More Details
CVE-2023-6636	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation on the 'gspb_save_files' function in versions up to, and including, 7.6.2. This makes it possible for authenticated attackers with administrator-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2023-6620	The POST SMTP Mailer WordPress plugin before 2.8.7 does not properly sanitise and escape several parameters before using them in SQL statements, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2024-0534	A vulnerability classified as critical has been found in Tenda A15 15.13.07.13. Affected is an unknown function of the file /goform/SetOnlineDevName of the component Web-based Management Interface. The manipulation of the argument mac 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-250704. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-0533	A vulnerability was found in Tenda A15 15.13.07.13. It has been rated as critical. This issue affects some unknown processing of the file /goform/SetOnlineDevName of the component Web-based Management Interface. The manipulation of the argument devName 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-250703. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2021-24151	The WP Editor WordPress plugin before 1.2.7 did not sanitise or validate its setting fields leading to an authenticated (admin+) blind SQL injection issue via an arbitrary parameter when making a request to save the settings.	7.2	More Details
CVE-2022-1538	Theme Demo Import WordPress plugin before 1.1.1 does not validate the imported file, allowing high-privilege users such as admin to upload arbitrary files (such as PHP) even when FILE_MODS and FILE_EDIT are disallowed.	7.2	More Details
CVE-2023-6558	The Export and Import Users and Customers plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation on the 'upload_import_file' function in versions up to, and including, 2.4.8. This makes it possible for authenticated attackers with shop manager-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2023-46712	A improper access control in Fortinet FortiPortal version 7.0.0 through 7.0.6, Fortinet FortiPortal version 7.2.0 through 7.2.1 allows attacker to escalate its privilege via specifically crafted HTTP requests.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0532	A vulnerability was found in Tenda A15 15.13.07.13. It has been declared as critical. This vulnerability affects unknown code of the file /goform/WifiExtraSet of the component Web-based Management Interface. The manipulation of the argument wpapsk_crypto2_4g 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-250702 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-2024-0531	A vulnerability was found in Tenda A15 15.13.07.13. It has been classified as critical. This affects an unknown part of the file /goform/setBlackRule of the component Web-based Management Interface. The manipulation of the argument deviceList 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-250701 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-2023-50916	Kyocera Device Manager before 3.1.1213.0 allows NTLM credential exposure during UNC path authentication via a crafted change from a local path to a UNC path. It allows administrators to configure the backup location of the database used by the application. Attempting to change this location to a UNC path via the GUI is rejected due to the use of a \ (backslash) character, which is supposed to be disallowed in a pathname. Intercepting and modifying this request via a proxy, or sending the request directly to the application endpoint, allows UNC paths to be set for the backup location. Once such a location is set, Kyocera Device Manager attempts to confirm access and will try to authenticate to the UNC path; depending on the configuration of the environment, this may authenticate to the UNC with Windows NTLM hashes. This could allow NTLM credential relaying or cracking attacks.	7.2	More Details
CVE-2024-21643	IdentityModel Extensions for .NET provide assemblies for web developers that wish to use federated identity providers for establishing the caller's identity. Anyone leveraging the `SignedHttpRequest`protocol or the `SignedHttpRequestValidator`is vulnerable. Microsoft.IdentityModel trusts the `jku`claim by default for the `SignedHttpRequest`protocol. This raises the possibility to make any remote or local `HTTP GET` request. The vulnerability has been fixed in Microsoft.IdentityModel.Protocols.SignedHttpRequest. Users should update all their Microsoft.IdentityModel versions to 7.1.2 (for 7x) or higher, 6.34.0 (for 6x) or higher.	7.1	More Details
CVE-2023-38610	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2024-22142	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs Profile Builder Pro allows Reflected XSS.This issue affects Profile Builder Pro: from n/a through 3.10.0.	7.1	More Details
CVE-2024-0556	A Weak Cryptography for Passwords vulnerability has been detected on WIC200 affecting version 1.1. This vulnerability allows a remote user to intercept the traffic and retrieve the credentials from another user and decode it in base64 allowing the attacker to see the credentials in plain text.	7.1	More Details
CVE-2023-32436	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2023-42876	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22198	Nginx-UI is a web interface to manage Nginx configurations. It is vulnerable to arbitrary command execution by abusing the configuration settings. The `Home > Preference` page exposes a list of system settings such as `Run Mode`, `Jwt Secret`, `Node Secret` and `Terminal Start Command`. While the UI doesn't allow users to modify the `Terminal Start Command` setting, it is possible to do so by sending a request to the API. This issue may lead to authenticated remote code execution, privilege escalation, and information disclosure. This vulnerability has been patched in version 2.0.0.beta.9.	7.1	More Details
CVE-2024-22428	Dell iDRAC Service Module, versions 5.2.0.0 and prior, contain an Incorrect Default Permissions vulnerability. It may allow a local unprivileged user to escalate privileges and execute arbitrary code on the affected system. Dell recommends customers upgrade at the earliest opportunity.	7.0	More Details
CVE-2023-51782	An issue was discovered in the Linux kernel before 6.6.8. rose_ioctl in net/rose/af_rose.c has a use-after-free because of a rose_accept race condition.	7.0	More Details
CVE-2023-51781	An issue was discovered in the Linux kernel before 6.6.8. atalk_ioctl in net/appletalk/ddp.c has a use-after-free because of an atalk_recvmsg race condition.	7.0	More Details
CVE-2023-51780	An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl in net/atm/ioctl.c has a use-after-free because of a vcc_recvmsg race condition.	7.0	More Details
CVE-2024-22196	Nginx-UI is an online statistics for Server Indicators Monitor CPU usage, memory usage, load average, and disk usage in real-time. This issue may lead to information disclosure. By using `DefaultQuery`, the `"desc"` and `"id"` values are used as default values if the query parameters are not set. Thus, the `order` and `sort_by` query parameter are user-controlled and are being appended to the `order` variable without any sanitization. This issue has been patched in version 2.0.0.beta.9.	7.0	More Details
CVE-2023-5097	Improper Input Validation vulnerability in HYPR Workforce Access on Windows allows Path Traversal.This issue affects Workforce Access: before 8.7.	7.0	More Details
CVE-2023-42832	A race condition was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to gain root privileges.	7.0	More Details
CVE-2023-51751	ScaleFusion 10.5.2 does not properly limit users to the Edge application because Alt-F4 can be used. This is fixed in 10.5.7 by preventing the launching of the file explorer in Agent-based Multi-App and Single App Kiosk mode.	6.8	More Details
CVE-2024-0316	Improper cleanup vulnerability in exceptions thrown in FireEye Endpoint Security, affecting version 5.2.0.958244. This vulnerability could allow an attacker to send multiple request packets to the containment_notify/preview parameter, which could lead to a service outage.	6.8	More Details
CVE-2023-4001	An authentication bypass flaw was found in GRUB due to the way that GRUB uses the UUID of a device to search for the configuration file that contains the password hash for the GRUB password protection feature. An attacker capable of attaching an external drive such as a USB stick containing a file system with a duplicate UUID (the same as in the "/boot/" file system) can bypass the GRUB password protection feature on UEFI systems, which enumerate removable drives before non-removable ones. This issue was introduced in a downstream patch in Red Hat's version of grub2 and does not affect the upstream package.	6.8	More Details
CVE-2023-42135	PAX A920Pro/A50 devices with PayDroid_8.1.0_Sagittarius_V11.1.50_20230614 or earlier can allow local code execution via parameter injection by bypassing the input validation when flashing a specific partition. The attacker must have physical USB access to the device in order to exploit this vulnerability.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50124	Flient Smart Door Lock v1.0 is vulnerable to Use of Default Credentials. Due to default credentials on a debug interface, in combination with certain design choices, an attacker can unlock the Flient Smart Door Lock by replacing the fingerprint that is stored on the scanner.	6.8	More Details
CVE-2024-0565	An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcpy length, leading to a denial of service.	6.8	More Details
CVE-2023-31033	NVIDIA DGX A100 BMC contains a vulnerability where a user may cause a missing authentication issue for a critical function by an adjacent network . A successful exploit of this vulnerability may lead to escalation of privileges, code execution, denial of service, information disclosure, and data tampering.	6.8	More Details
CVE-2023-42134	PAX Android based POS devices with PayDroid_8.1.0_Sagittarius_V11.1.45_20230314 or earlier can allow the signed partition overwrite and subsequently local code execution via hidden command. The attacker must have physical USB access to the device in order to exploit this vulnerability.	6.8	More Details
CVE-2023-6395	The Mock software contains a vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server.	6.7	More Details
CVE-2024-0315	Remote file inclusion vulnerability in FireEye Central Management affecting version 9.1.1.956704. This vulnerability allows an attacker to upload a malicious PDF file to the system during the report creation process.	6.6	More Details
CVE-2023-6583	The Import and export users and customers plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.24.2 via the Recurring Import functionality. This makes it possible for authenticated attackers, with administrator access and above, to read and delete the contents of arbitrary files on the server including wp-config.php, which can contain sensitive information.	6.6	More Details
CVE-2023-6457	Incorrect Default Permissions vulnerability in Hitachi Tuning Manager on Windows (Hitachi Tuning Manager server component) allows local users to read and write specific files.This issue affects Hitachi Tuning Manager: before 8.8.5-04.	6.6	More Details
CVE-2023-6955	A missing authorization check vulnerability exists in GitLab Remote Development affecting all versions prior to 16.5.6, 16.6 prior to 16.6.4 and 16.7 prior to 16.7.2. This condition allows an attacker to create a workspace in one group that is associated with an agent from another group.	6.6	More Details
CVE-2023-31034	NVIDIA DGX A100 SBIOS contains a vulnerability where a local attacker can cause input validation checks to be bypassed by causing an integer overflow. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	6.6	More Details
CVE-2024-20973	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-21670	Ursa is a cryptographic library for use with blockchains. The revocation schema that is part of the Ursa CL-Signatures implementations has a flaw that could impact the privacy guarantees defined by the AnonCreds verifiable credential model, allowing a malicious holder of a revoked credential to generate a valid Non-Revocation Proof for that credential as part of an AnonCreds presentation. A verifier may verify a credential from a holder as being "not revoked" when in fact, the holder's credential has been revoked. Ursa has moved to end-of-life status and no fix is expected.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21603	An Improper Check for Unusual or Exceptional Conditions vulnerability in the kernel of Juniper Network Junos OS on MX Series allows a network based attacker with low privileges to cause a denial of service. If a scaled configuration for Source class usage (SCU) / destination class usage (DCU) (more than 10 route classes) is present and the SCU/DCU statistics are gathered by executing specific SNMP requests or CLI commands, a 'vmcore' for the RE kernel will be seen which leads to a device restart. Continued exploitation of this issue will lead to a sustained DoS. This issue only affects MX Series devices with MPC10, MPC11 or LC9600, and MX304. No other MX Series devices are affected. This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R2; * 22.3 versions earlier than 22.3R2.	6.5	More Details
CVE-2023-52339	In libebml before 1.4.5, an integer overflow in MemIOCallback.cpp can occur when reading or writing. It may result in buffer overflows.	6.5	More Details
CVE-2024-22411	Avo is a framework to create admin panels for Ruby on Rails apps. In Avo 3 pre12, any HTML inside text that is passed to `error` or `succeed` in an `Avo::BaseAction` subclass will be rendered directly without sanitization in the toast/notification that appears in the UI on Action completion. A malicious user could exploit this vulnerability to trigger a cross site scripting attack on an unsuspecting user. This issue has been addressed in the 3.3.0 and 2.47.0 releases of Avo. Users are advised to upgrade.	6.5	More Details
CVE-2024-22192	Ursa is a cryptographic library for use with blockchains. The revocation scheme that is part of the Ursa CL-Signatures implementations has a flaw that could impact the privacy guarantees defined by the AnonCreds verifiable credential model. Notably, a malicious verifier may be able to generate a unique identifier for a holder providing a verifiable presentation that includes a Non-Revocation proof. The impact of the flaw is that a malicious verifier may be able to determine a unique identifier for a holder presenting a Non-Revocation proof. Ursa has moved to end-of-life status and no fix is expected.	6.5	More Details
CVE-2024-21617	An Incomplete Cleanup vulnerability in Nonstop active routing (NSR) component of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause memory leak leading to Denial of Service (DoS). On all Junos OS platforms, when NSR is enabled, a BGP flap will cause memory leak. A manual reboot of the system will restore the services. Note: NSR is not supported on the SRX Series and is therefore not affected by this vulnerability. The memory usage can be monitored using the below commands. user@host> show chassis routing-engine no-forwarding user@host> show system memory l no-more This issue affects: Juniper Networks Junos OS * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S1, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2. This issue does not affect Junos OS versions earlier than 20.4R3-S7.	6.5	More Details
CVE-2024-20977	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-20985	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-22027	Improper input validation vulnerability in WordPress Quiz Maker Plugin prior to 6.5.0.6 allows a remote authenticated attacker to perform a Denial of Service (DoS) attack against external services.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21613	A Missing Release of Memory after Effective Lifetime vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause an rpd crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when traffic engineering is enabled for OSPF or ISIS, and a link flaps, a patroot memory leak is observed. This memory leak, over time, will lead to an rpd crash and restart. The memory usage can be monitored using the below command. user@host> show task memory detail	match patroot This issue affects: Juniper Networks Junos OS * All versions earlier than 21.2R3-S3; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-EVO; * 22.1 versions earlier than 22.1R3-EVO; * 22.2 versions earlier than 22.2R3-EVO.	6.5	More Details
CVE-2024-20975	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2023-6048	The Estatik Real Estate Plugin WordPress plugin before 4.1.1 does not prevent user with low privileges on the site, like subscribers, from setting any of the site's options to 1, which could be used to break sites and lead to DoS when certain options are reset	6.5	More Details
CVE-2024-20963	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-20961	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2023-50290	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Solr. The Solr Metrics API publishes all unprotected environment variables available to each Apache Solr instance. Users are able to specify which environment variables to hide, however, the default list is designed to work for known secret Java system properties. Environment variables cannot be strictly defined in Solr, like Java system properties can be, and may be set for the entire host, unlike Java system properties which are set per-Java-proccess. The Solr Metrics API is protected by the "metrics-read" permission. Therefore, Solr Clouds with Authorization setup will only be vulnerable via users with the "metrics-read" permission. This issue affects Apache Solr: from 9.0.0 before 9.3.0. Users are recommended to upgrade to version 9.3.0 or later, in which environment variables are not published via the Metrics API.	6.5	More Details
CVE-2023-46749	Apache Shiro before 1.13.0 or 2.0.0-alpha-4, may be susceptible to a path traversal attack that results in an authentication bypass when used together with path rewriting Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+, or ensure `blockSemicolon` is enabled (this is the default).	6.5	More Details
CVE-2023-51071	An access control issue in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to arbitrarily disable the SMB service on a victim's Qstar instance by executing a specific command in a link.	6.5	More Details
CVE-2023-0824	The User registration & user profile WordPress plugin through 2.0 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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47459	An issue in Knovos Discovery v.22.67.0 allows a remote attacker to obtain sensitive information via the /DiscoveryReview/Service/CaseManagement.svc/GetProductSiteName component.	6.5	More Details
CVE-2023-51805	SQL Injection vulnerability in TDuckCLoud tduck-platform v.4.0 allows a remote attacker to obtain sensitive information via the getFormKey parameter in the search function of FormDataMysqlService.java file.	6.5	More Details
CVE-2023-45231	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing Neighbor Discovery Redirect message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	6.5	More Details
CVE-2024-22137	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MailMunch Constant Contact Forms by MailMunch allows Stored XSS.This issue affects Constant Contact Forms by MailMunch: from n/a through 2.0.11.	6.5	More Details
CVE-2023-6683	A flaw was found in the QEMU built-in VNC server while processing ClientCutText messages. The qemu_clipboard_request() function can be reached before vnc_server_cut_text_caps() was called and had the chance to initialize the clipboard peer, leading to a NULL pointer dereference. This could allow a malicious authenticated VNC client to crash QEMU and trigger a denial of service.	6.5	More Details
CVE-2023-6824	The WP Customer Area WordPress plugin before 8.2.1 does not properly validates user capabilities in some of its AJAX actions, allowing any users to retrieve other user's account address.	6.5	More Details
CVE-2023-4969	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures.	6.5	More Details
CVE-2023-31025	NVIDIA DGX A100 BMC contains a vulnerability where an attacker may cause an LDAP user injection. A successful exploit of this vulnerability may lead to information disclosure.	6.5	More Details
CVE-2023-51978	In PHPGurukul Art Gallery Management System v1.1, "Update Artist Image" functionality of "imageid" parameter is vulnerable to SQL Injection.	6.5	More Details
CVE-2024-0507	An attacker with access to a Management Console user account with the editor role could escalate privileges through a command injection vulnerability in the Management Console. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.11.3, 3.10.5, 3.9.8, and 3.8.13 This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2024-21600	An Improper Neutralization of Equivalent Special Elements vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows a unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When MPLS packets are meant to be sent to a flexible tunnel interface (FTI) and if the FTI tunnel is down, these will hit the reject NH, due to which the packets get sent to the CPU and cause a host path wedge condition. This will cause the FPC to hang and requires a manual restart to recover. Please note that this issue specifically affects PTX1000, PTX3000, PTX5000 with FPC3, PTX10002-60C, and PTX10008/16 with LC110x. Other PTX Series devices and Line Cards (LC) are not affected. The following log message can be seen when the issue occurs: Cmerror Op Set: Host Loopback: HOST LOOPBACK WEDGE DETECTED IN PATH ID <id> (URI: /fpc/<fpc>/pfe/<pfe>/cm/<cm>/Host_Loopback/<cm>/HOST_LOOPBACK_MAKE_CMERROR_ID[<id>]) This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S8; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R2-S2, 22.1R3; * 22.2 versions earlier than 22.2R2-S1, 22.2R3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45229	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing the IA_NA or IA_TA option in a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	6.5	More Details
CVE-2023-47997	An issue discovered in BitmapAccess.cpp::FreeImage_AllocateBitmap in FreeImage 3.18.0 leads to an infinite loop and allows attackers to cause a denial of service.	6.5	More Details
CVE-2023-6242	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.4 (for Pro) & 2.2.7 (for Free). This is due to missing or incorrect nonce validation on the evo_eventpost_update_meta function. This makes it possible for unauthenticated attackers to update arbitrary post metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2023-49863	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage.json.php image upload functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.This vulnerability is triggered by the `downloadURL_webpimage` parameter.	6.5	More Details
CVE-2023-40385	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14, Safari 17, iOS 17 and iPadOS 17. A remote attacker may be able to view leaked DNS queries with Private Relay turned on.	6.5	More Details
CVE-2023-48249	The vulnerability allows an authenticated remote attacker to list arbitrary folders in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request. By abusing this vulnerability, it is possible to steal session cookies of other active users.	6.5	More Details
CVE-2023-50126	Missing encryption in the RFID tags of the Hozard alarm system (Alarmsysteem) v1.0 allow attackers to create a cloned tag via brief physical proximity to one of the original tags, which results in an attacker being able to bring the alarm system to a disarmed state.	6.5	More Details
CVE-2023-42862	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, iOS 16.4 and iPadOS 16.4, watchOS 9.4. Processing an image may result in disclosure of process memory.	6.5	More Details
CVE-2023-42865	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, iOS 16.4 and iPadOS 16.4, watchOS 9.4. Processing an image may result in disclosure of process memory.	6.5	More Details
CVE-2023-5455	A Cross-site request forgery vulnerability exists in ipa/session/login_password in all supported versions of IPA. This flaw allows an attacker to trick the user into submitting a request that could perform actions as the user, resulting in a loss of confidentiality and system integrity. During community penetration testing it was found that for certain HTTP end-points FreeIPA does not ensure CSRF protection. Due to implementation details one cannot use this flaw for reflection of a cookie representing already logged-in user. An attacker would always have to go through a new authentication attempt.	6.5	More Details
CVE-2023-50129	Missing encryption in the NFC tags of the Flient Smart Door Lock v1.0 allows attackers to create a cloned tag via brief physical proximity to the original tags, which results in an attacker gaining access to the perimeter.	6.5	More Details
CVE-2023-6638	The GTG Product Feed for Shopping plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_settings' function in versions up to, and including, 1.2.4. This makes it possible for unauthenticated attackers to update plugin settings.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21666	The Customer Management Framework (CMF) for Pimcore adds functionality for customer data management, segmentation, personalization and marketing automation. An authenticated and unauthorized user can access the list of potential duplicate users and see their data. Permissions are enforced when reaching the `/admin/customermanagementframework/duplicates/list` endpoint allowing an authenticated user without the permissions to access the endpoint and query the data available there. Unauthorized user(s) can access PII data from customers. This vulnerability has been patched in version 4.0.6.	6.5	More Details
CVE-2023-37932	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability [CWE-22] in FortiVoiceEntreprise version 7.0.0 and before 6.4.7 allows an authenticated attacker to read arbitrary files from the system via sending crafted HTTP or HTTPS requests	6.5	More Details
CVE-2024-21667	pimcore/customer-data-framework is the Customer Management Framework for management of customer data within Pimcore. An authenticated and unauthorized user can access the GDPR data extraction feature and query over the information returned, leading to customer data exposure. Permissions are not enforced when reaching the `/admin/customermanagementframework/gdpr-data/search-data-objects` endpoint allowing an authenticated user without the permissions to access the endpoint and query the data available there. An unauthorized user can access PII data from customers. This vulnerability has been patched in version 4.0.6.	6.5	More Details
CVE-2023-6637	The CAOS	Host Google Analytics Locally plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_settings' function in versions up to, and including, 4.7.14. This makes it possible for unauthenticated attackers to update plugin settings.	6.5	More Details
CVE-2024-21599	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). If an MX Series device receives PTP packets on an MPC3E that doesn't support PTP this causes a memory leak which will result in unpredictable behavior and ultimately in an MPC crash and restart. To monitor for this issue, please use the following FPC vty level commands: show heap shows an increase in "LAN buffer" utilization and show clksync ptp nbr-upd-info shows non-zero "Pending PFEs" counter. This issue affects Juniper Networks Junos OS on MX Series with MPC3E: * All versions earlier than 20.4R3-S3; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3; * 21.3 versions earlier than 21.3R2-S1, 21.3R3; * 21.4 versions earlier than 21.4R2; * 22.1 versions earlier than 22.1R2.	6.5	More Details
CVE-2023-49864	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage.json.php image upload functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.This vulnerability is triggered by the `downloadURL_image` parameter.	6.5	More Details
CVE-2023-6994	The List category posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catlist' shortcode in all versions up to, and including, 0.89.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.5	More Details
CVE-2023-6244	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.4 (Pro) & 2.2.8 (Free). This is due to missing or incorrect nonce validation on the save_virtual_event_settings function. This makes it possible for unauthenticated attackers to modify virtual event settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2023-48242	The vulnerability allows an authenticated remote attacker to download arbitrary files in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request.	6.5	More Details
CVE-2023-48245	The vulnerability allows an unauthenticated remote attacker to upload arbitrary files under the context of the application OS user (“root”) via a crafted HTTP request.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6554	When access to the "admin" folder is not protected by some external authorization mechanisms e.g. Apache Basic Auth, it is possible for any user to download protected information like exam answers.	6.5	More Details
CVE-2024-21587	An Improper Handling of Exceptional Conditions vulnerability in the broadband edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an attacker directly connected to the vulnerable system who repeatedly flaps DHCP subscriber sessions to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Memory can only be recovered by manually restarting bbe-smgd. This issue only occurs if BFD liveness detection for DHCP subscribers is enabled. Systems without BFD liveness detection enabled are not vulnerable to this issue. Indication of the issue can be observed by periodically executing the 'show system processes extensive' command, which will indicate an increase in memory allocation for bbe-smgd. A small amount of memory is leaked every time a DHCP subscriber logs in, which will become visible over time, ultimately leading to memory starvation. user@junos> show system processes extensive | match bbe-smgd 13071 root 24 0 415M 201M select 0 0:41 7.28% bbe-smgd{bbe-smgd} 13071 root 20 0 415M 201M select 1 0:04 0.00% bbe-smgd{bbe-smgd} ... user@junos> show system processes extensive | match bbe-smgd 13071 root 20 0 420M 208M select 0 4:33 0.10% bbe-smgd{bbe-smgd} 13071 root 20 0 420M 208M select 0 0:12 0.00% bbe-smgd{bbe-smgd} ... This issue affects Juniper Networks Junos OS on MX 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-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2.	6.5	More Details
CVE-2023-49862	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage.json.php image upload functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.This vulnerability is triggered by the `downloadURL_gifimage` parameter.	6.5	More Details
CVE-2023-48246	The vulnerability allows a remote attacker to download arbitrary files in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request.	6.5	More Details
CVE-2023-47171	An information disclosure vulnerability exists in the aVideoEncoder.json.php chunkFile path functionality of WWBN AVideo 11.6 and dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.	6.5	More Details
CVE-2023-6158	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the evo_eventpost_update_meta function in all versions up to, and including, 4.5.4 (for Pro) and 2.2.7 (for free). This makes it possible for unauthenticated attackers to update and remove arbitrary post metadata. Note that certain parameters may allow for content injection.	6.5	More Details
CVE-2023-36842	An Improper Check for Unusual or Exceptional Conditions vulnerability in Juniper DHCP Daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause the jdhcpd to consume all the CPU cycles resulting in a Denial of Service (DoS). On Junos OS devices with forward-snooped-client configured, if an attacker sends a specific DHCP packet to a non-configured interface, this will cause an infinite loop. The DHCP process will have to be restarted to recover the service. This issue affects: Juniper Networks Junos OS * 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-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49295	quic-go is an implementation of the QUIC protocol (RFC 9000, RFC 9001, RFC 9002) in Go. An attacker can cause its peer to run out of memory sending a large number of PATH_CHALLENGE frames. The receiver is supposed to respond to each PATH_CHALLENGE frame with a PATH_RESPONSE frame. The attacker can prevent the receiver from sending out (the vast majority of) these PATH_RESPONSE frames by collapsing the peers congestion window (by selectively acknowledging received packets) and by manipulating the peer's RTT estimate. This vulnerability has been patched in versions 0.37.7, 0.38.2 and 0.39.4.	6.4	More Details
CVE-2023-6561	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the featured image alt text in all versions up to, and including, 4.5.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4962	The Video PopUp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'video_popup' shortcode in versions up to, and including, 1.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-7070	The Email Encoder – Protect Email Addresses and Phone Numbers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's eeb_mailto shortcode in all versions up to, and including, 2.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4372	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'esi' shortcode in versions up to, and including, 5.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-7071	The Essential Blocks – Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Table of Contents block in all versions up to, and including, 4.4.6 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-2023-4960	The WCFM Marketplace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wcfm_stores' shortcode in versions up to, and including, 3.6.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6645	The Post Grid Combo – 36+ Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS parameter in all versions up to, and including, 2.2.64 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6335	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on Windows allows User-Controlled Filename.This issue affects Workforce Access: before 8.7.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6938	The Oxygen Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a custom field in all versions up to, and including, 4.8 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. NOTE: Version 4.8.1 of the Oxygen Builder plugin for WordPress addresses this vulnerability by implementing an optional filter to provide output escaping for dynamic data. Please see https://oxygenbuilder.com/documentation/other/security/#filtering-dynamic-data for more details.	6.4	More Details
CVE-2023-6988	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's extend_builder_render_js shortcode in all versions up to, and including, 1.0.239 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-22209	Open edX Platform is a service-oriented platform for authoring and delivering online learning. A user with a JWT and more limited scopes could call endpoints exceeding their access. This vulnerability has been patched in commit 019888f.	6.4	More Details
CVE-2023-6934	The Limit Login Attempts Reloaded plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 2.25.26 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6782	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.0.92 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6781	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom fields in all versions up to, and including, 2.10.26 due to insufficient input sanitization and output escaping on user supplied values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6776	The 3D FlipBook plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘Ready Function’ field in all versions up to, and including, 1.15.2 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-2023-6684	The Ibtana – WordPress Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ive' shortcode in versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping on 'width' and 'height' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-0468	A vulnerability has been found in code-projects Fighting Cock Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/action/new-father.php. The manipulation of the argument image 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-250573 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0543	A vulnerability classified as critical has been found in CodeAstro Real Estate Management System up to 1.0. This affects an unknown part of the file propertydetail.php. The manipulation of the argument pid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250713 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0487	A vulnerability was found in code-projects Fighting Cock Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/action/delete-vaccine.php. The manipulation of the argument ref leads to sql injection. 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-250592.	6.3	More Details
CVE-2024-0488	A vulnerability was found in code-projects Fighting Cock Information System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/action/new-feed.php. The manipulation of the argument type_feed leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250593 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0489	A vulnerability was found in code-projects Fighting Cock Information System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/action/edit_chicken.php. The manipulation of the argument ref leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250594 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0498	A vulnerability was found in Project Worlds Lawyer Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file searchLawyer.php. The manipulation of the argument experience leads to sql 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-250603.	6.3	More Details
CVE-2024-0470	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been classified as critical. This affects an unknown part of the file /admin_route/inc_service_credits.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250575.	6.3	More Details
CVE-2024-0601	A vulnerability was found in ZhongFuCheng3y Austin 1.0. It has been rated as critical. Affected by this issue is the function getRemoteUrl2File of the file src\main\java\com\java3y\austin\support\utils\AustinFileUtils.java of the component Email Message Template Handler. The manipulation 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-250838 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0497	A vulnerability was found in Campcodes Student Information System 1.0. It has been classified as critical. Affected is an unknown function of the file /classes/Users.php?f=save. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250602 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0492	A vulnerability classified as critical was found in Kashipara Billing Software 1.0. Affected by this vulnerability is an unknown functionality of the file buyer_detail_submit.php of the component HTTP POST Request Handler. The manipulation of the argument gstn_no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250597 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0493	A vulnerability, which was classified as critical, has been found in Kashipara Billing Software 1.0. Affected by this issue is some unknown functionality of the file submit_delivery_list.php of the component HTTP POST Request Handler. The manipulation of the argument customer_details leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250598 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0494	A vulnerability, which was classified as critical, was found in Kashipara Billing Software 1.0. This affects an unknown part of the file material_bill.php of the component HTTP POST Request Handler. The manipulation of the argument itemtypeid leads to sql 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-250599.	6.3	More Details
CVE-2024-0469	A vulnerability was found in code-projects Human Resource Integrated System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file update_personal_info.php. The manipulation of the argument sex leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250574 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0464	A vulnerability classified as critical has been found in code-projects Online Faculty Clearance 1.0. This affects an unknown part of the file delete_faculty.php of the component HTTP GET Request Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250569 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0471	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin_route/dec_service_credits.php. The manipulation of the argument date leads to sql 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-250576.	6.3	More Details
CVE-2024-0486	A vulnerability has been found in code-projects Fighting Cock Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/action/add_con.php. The manipulation of the argument chicken leads to sql 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-250591.	6.3	More Details
CVE-2024-0473	A vulnerability classified as critical has been found in code-projects Dormitory Management System 1.0. Affected is an unknown function of the file comment.php. The manipulation of the argument com leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250578 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0484	A vulnerability, which was classified as critical, has been found in code-projects Fighting Cock Information System 1.0. This issue affects some unknown processing of the file admin/action/update_mother.php. The manipulation of the argument age_mother leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250589 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0483	A vulnerability classified as critical was found in Taokeyun up to 1.0.5. This vulnerability affects the function index of the file application/index/controller/app/Task.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql 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-250588.	6.3	More Details
CVE-2024-0482	A vulnerability classified as critical has been found in Taokeyun up to 1.0.5. This affects the function index of the file application/index/controller/app/Video.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql 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-250587.	6.3	More Details
CVE-2024-0481	A vulnerability was found in Taokeyun up to 1.0.5. It has been rated as critical. Affected by this issue is the function shopGoods of the file application/index/controller/app/store/Goods.php of the component HTTP POST Request Handler. The manipulation of the argument keyword leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250586 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0478	A vulnerability was found in code-projects Fighting Cock Information System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/pages/edit_chicken.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-250583.	6.3	More Details
CVE-2024-0475	A vulnerability, which was classified as critical, has been found in code-projects Dormitory Management System 1.0. Affected by this issue is some unknown functionality of the file modifyuser.php. The manipulation of the argument user_id leads to sql injection. 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-250580.	6.3	More Details
CVE-2024-0477	A vulnerability has been found in code-projects Fighting Cock Information System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/action/update-deworm.php. The manipulation of the argument usage_deworm leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250582 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0527	A vulnerability, which was classified as critical, has been found in CXBSoft Url-shorting up to 1.3.1. This issue affects some unknown processing of the file /admin/pages/update_go.php of the component HTTP POST Request Handler. The manipulation of the argument version leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-250697 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-2024-20930	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Content Access SDK, Image Export SDK, PDF Export SDK, HTML Export SDK). The supported version that is affected is 8.5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	6.3	More Details
CVE-2024-0523	A vulnerability was found in CmsEasy up to 7.7.7. It has been declared as critical. Affected by this vulnerability is the function getslide_child_action in the library lib/admin/language_admin.php. The manipulation of the argument sid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250693 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-2024-0485	A vulnerability, which was classified as critical, was found in code-projects Fighting Cock Information System 1.0. Affected is an unknown function of the file admin/pages/tables/add_con.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250590 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0540	A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been classified as critical. Affected is the function formOfflineSet of the component httpd. The manipulation of the argument ssidIndex 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-250710 is the identifier 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 Number	Description	Base Score	Reference
CVE-2024-0495	A vulnerability has been found in Kashipara Billing Software 1.0 and classified as critical. This vulnerability affects unknown code of the file party_submit.php of the component HTTP POST Request Handler. The manipulation of the argument party_name leads to sql 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-250600.	6.3	More Details
CVE-2024-0426	A vulnerability, which was classified as critical, has been found in ForU CMS up to 2020-06-23. This issue affects some unknown processing of the file admin/cms_template.php. The manipulation of the argument t_name/t_path leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250445 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0496	A vulnerability was found in Kashipara Billing Software 1.0 and classified as critical. This issue affects some unknown processing of the file item_list_edit.php of the component HTTP POST Request Handler. 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 identifier VDB-250601 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0579	A vulnerability classified as critical was found in Totolink X2000R 1.0.0-B20221212.1452. Affected by this vulnerability is the function formMapDelDevice of the file /boafrm/formMapDelDevice. The manipulation of the argument macstr leads to 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-250795. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0463	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /production/admin_view_info.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. 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-250568.	6.3	More Details
CVE-2023-48255	The vulnerability allows an unauthenticated remote attacker to send malicious network requests containing arbitrary client-side script code and obtain its execution inside a victim's session via a crafted URL, HTTP request, or simply by waiting for the victim to view the poisoned log.	6.3	More Details
CVE-2024-0462	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /production/designee_view_status.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql 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-250567.	6.3	More Details
CVE-2024-0461	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been classified as critical. Affected is an unknown function of the file deactivate.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250566 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2011-10005	A vulnerability, which was classified as critical, was found in EasyFTP 1.7.0.2. Affected is an unknown function of the component MKD Command Handler. The manipulation leads to 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-250716.	6.3	More Details
CVE-2023-29444	An uncontrolled search path element vulnerability (DLL hijacking) has been discovered that could allow a locally authenticated adversary to escalate privileges to SYSTEM. Alternatively, they could host a trojanized version of the software and trick victims into downloading and installing their malicious version to gain initial access and code execution.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0415	A vulnerability classified as critical was found in DeShang DSMall up to 6.1.0. Affected by this vulnerability is an unknown functionality of the file application/home/controller/TaobaoExport.php of the component Image URL Handler. The manipulation leads to improper access controls. 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-250435.	6.3	More Details
CVE-2024-0389	A vulnerability, which was classified as critical, was found in SourceCodester Student Attendance System 1.0. Affected is an unknown function of the file attendance_report.php. The manipulation of the argument class_id leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250230 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0460	A vulnerability was found in code-projects Faculty Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/pages/student-print.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250565 was assigned to this vulnerability.	6.3	More Details
CVE-2023-7226	A vulnerability was found in meetyoucrop big-whale 1.1 and classified as critical. Affected by this issue is some unknown functionality of the file /auth/user/all.api of the component Admin Module. The manipulation of the argument id leads to improper ownership management. 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-250232.	6.3	More Details
CVE-2024-20675	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	6.3	More Details
CVE-2023-45175	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 267973.	6.2	More Details
CVE-2023-45173	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the NFS kernel extension to cause a denial of service. IBM X-Force ID: 267971.	6.2	More Details
CVE-2023-6915	A Null pointer dereference problem was found in ida_free in lib/idr.c in the Linux Kernel. This issue may allow an attacker using this library to cause a denial of service problem due to a missing check at a function return.	6.2	More Details
CVE-2023-38267	IBM Security Access Manager Appliance (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) could allow a local user to possibly elevate their privileges due to sensitive configuration information being exposed. IBM X-Force ID: 260584.	6.2	More Details
CVE-2023-45169	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the pmsvcs kernel extension to cause a denial of service. IBM X-Force ID: 267967.	6.2	More Details
CVE-2023-45171	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the kernel to cause a denial of service. IBM X-Force ID: 267969.	6.2	More Details
CVE-2024-23177	An issue was discovered in the WatchAnalytics extension in MediaWiki before 1.40.2. XSS can occur via the Special:PageStatistics page parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20940	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Create, Update, Authoring Flow). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-20938	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: ECC). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data as well as unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-0239	The Contact Form 7 Connector WordPress plugin before 1.2.3 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 administrators.	6.1	More Details
CVE-2024-23179	An issue was discovered in the GlobalBlocking extension in MediaWiki before 1.40.2. For a Special:GlobalBlock?uselang=x-xss URI, i18n-based XSS can occur via the parentheses message. This affects subtitle links in buildSubtitleLinks.	6.1	More Details
CVE-2024-20934	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Engineering Change Order). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data as well as unauthorized read access to a subset of Oracle Installed Base accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-0251	The Advanced Woo Search plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search parameter in all versions up to, and including, 2.96 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. This only affects sites when the Dynamic Content for Elementor plugin is also installed.	6.1	More Details
CVE-2024-0238	The EventON Premium WordPress plugin before 4.5.6, EventON WordPress plugin before 2.2.8 do not have authorisation in an AJAX action, and does not ensure that the post to be updated belong to the plugin, allowing unauthenticated users to update arbitrary post metadata.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20936	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data as well as unauthorized read access to a subset of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-0233	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not properly sanitise and escape a parameter before outputting it back in pages, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-7151	The Product Enquiry for WooCommerce WordPress plugin before 3.2 does not sanitise and escape the page parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2024-0187	The Community by PeepSo WordPress plugin before 6.3.1.2 does not sanitise and escape various parameters and generated URLs before outputting them back attributes, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-0479	The Print Invoice & Delivery Notes for WooCommerce WordPress plugin before 4.7.2 is vulnerable to reflected XSS by echoing a GET value in an admin note within the WooCommerce orders page. This means that this vulnerability can be exploited for users with the edit_others_shop_orders capability. WooCommerce must be installed and active. This vulnerability is caused by a urldecode() after cleanup with esc_url_raw(), allowing double encoding.	6.1	More Details
CVE-2024-23173	An issue was discovered in the Cargo extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. The Special:Drilldown page allows XSS via artist, album, and position parameters because of applied filter values in drilldown/CargoAppliedFilter.php.	6.1	More Details
CVE-2023-0769	The hiWeb Migration Simple WordPress plugin through 2.0.0.1 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 admins.	6.1	More Details
CVE-2023-3771	The T1 WordPress theme through 19.0 is vulnerable to unauthenticated open redirect with which any attacker and redirect users to arbitrary websites.	6.1	More Details
CVE-2022-1617	The WP-Invoice WordPress plugin through 4.3.1 does not have CSRF check in place when updating its settings, and is lacking sanitisation as well as escaping in some of them, allowing attacker to make a logged in admin change them and add XSS payload in them	6.1	More Details
CVE-2023-5558	The LearnPress WordPress plugin before 4.2.5.5 does not sanitise and escape user input 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-2022-1618	The Coru LFMember WordPress plugin through 1.0.2 does not have CSRF check in place when adding a new game, and is lacking sanitisation as well as escaping in their settings, allowing attacker to make a logged in admin add an arbitrary game with XSS payloads	6.1	More Details
CVE-2023-52068	kodbox v1.43 was discovered to contain a cross-site scripting (XSS) vulnerability via the operation and login logs.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0402	The Super Forms - Drag & Drop Form Builder WordPress plugin before 6.0.4 does not escape the bob_czy_panstwa_sprawa_zostala_rozwiazana parameter before outputting it back in an attribute via the super_language_switcher AJAX action, leading to a Reflected Cross-Site Scripting. The action is also lacking CSRF, making the attack easier to perform against any user.	6.1	More Details
CVE-2020-26628	A Cross-Site Scripting (XSS) vulnerability was discovered in Hospital Management System V4.0 which allows an attacker to execute arbitrary web scripts or HTML code via a malicious payload appended to a username on the 'Edit Profile" page and triggered by another user visiting the profile.	6.1	More Details
CVE-2023-52274	member/index/register.html in YzmCMS 6.5 through 7.0 allows XSS via the Referer HTTP header.	6.1	More Details
CVE-2023-41619	Emlog Pro v2.1.14 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/article.php?action=write.	6.1	More Details
CVE-2022-40361	Cross Site Scripting Vulnerability in Elite CRM v1.2.11 allows attacker to execute arbitrary code via the language parameter to the /ngs/login endpoint.	6.1	More Details
CVE-2024-20908	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: Advanced UI). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2023-49394	Zentao versions 4.1.3 and before has a URL redirect vulnerability, which prevents the system from functioning properly.	6.1	More Details
CVE-2023-48104	Alinto SOGo before 5.9.1 is vulnerable to HTML Injection.	6.1	More Details
CVE-2023-6632	The Happy Addons for Elementor plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via DOM in all versions up to and including 3.9.1.1 (versions up to 2.9.1.1 in Happy Addons for Elementor Pro) 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-2024-20950	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data as well as unauthorized read access to a subset of Oracle Customer Interaction History accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20948	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2023-49260	An XSS attack can be performed by changing the MOTD banner and pointing the victim to the "terminal_tool.cgi" path. It can be used together with the vulnerability CVE-2023-49255.	6.1	More Details
CVE-2023-49258	User browser may be forced to execute JavaScript and pass the authentication cookie to the attacker leveraging the XSS vulnerability located at "/gui/terminal_tool.cgi" in the "data" parameter.	6.1	More Details
CVE-2024-0310	A content-security-policy vulnerability in ENS Control browser extension prior to 10.7.0 Update 15 allows a remote attacker to alter the response header parameter setting to switch the content security policy into report-only mode, allowing an attacker to bypass the content-security-policy configuration.	6.1	More Details
CVE-2023-51790	Cross Site Scripting vulnerability in piwigo v.14.0.0 allows a remote attacker to obtain sensitive information via the lang parameter in the Admin Tools plug-in component.	6.1	More Details
CVE-2021-24432	The Advanced AJAX Product Filters WordPress plugin does not sanitise the 'term_id' POST parameter before outputting it in the page, leading to reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2024-20928	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2023-6050	The Estatik Real Estate Plugin WordPress plugin before 4.1.1 does not sanitise and escape various parameters and generated URLs before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-51064	QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 was discovered to contain a DOM Based reflected XSS vulnerability within the component qnme-ajax?method=tree_table.	6.1	More Details
CVE-2023-6882	The Simple Membership plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘environment_mode’ parameter in all versions up to, and including, 4.3.8 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 Number	Description	Base Score	Reference
CVE-2021-24870	The WP Fastest Cache WordPress plugin before 0.9.5 is lacking a CSRF check in its wpfc_save_cdn_integration AJAX action, and does not sanitise and escape some the options available via the action, which could allow attackers to make logged in high privilege users call it and set a Cross-Site Scripting payload	6.1	More Details
CVE-2023-51067	An unauthenticated reflected cross-site scripting (XSS) vulnerability in QStar Archive Solutions Release RELEASE_3-0 Build 7 allows attackers to execute arbitrary javascript on a victim's browser via a crafted link.	6.1	More Details
CVE-2024-20942	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: LOV). Supported versions that are affected are 11.5, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-0454	ELAN Match-on-Chip FPR solution has design fault about potential risk of valid SID leakage and enumeration with spoof sensor. This fault leads to that Windows Hello recognition would be bypass with cloning SID to cause broken account identity. Version which is lower than 3.0.12011.08009(Legacy)/3.3.12011.08103(ESS) would suffer this risk on DELL Inspiron platform.	6.0	More Details
CVE-2024-20926	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details
CVE-2024-21601	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the Flow-processing Daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (Dos). On SRX Series devices when two different threads try to simultaneously process a queue which is used for TCP events flowd will crash. One of these threads can not be triggered externally, so the exploitation of this race condition is outside the attackers direct control. Continued exploitation of this issue will lead to a sustained DoS. This issue affects Juniper Networks Junos OS: * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S3; * 22.2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2-S1, 22.4R3. This issue does not affect Juniper Networks Junos OS versions earlier than 21.2R1.	5.9	More Details
CVE-2023-50127	Hozard alarm system (Alarmsysteem) v1.0 is vulnerable to Improper Authentication. Commands sent via the SMS functionality are accepted from random phone numbers, which allows an attacker to bring the alarm system to a disarmed state from any given phone number.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21585	An Improper Handling of Exceptional Conditions vulnerability in BGP session processing of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker, using specific timing outside the attacker's control, to flap BGP sessions and cause the routing protocol daemon (rpd) process to crash and restart, leading to a Denial of Service (DoS) condition. Continued BGP session flapping will create a sustained Denial of Service (DoS) condition. This issue only affects routers configured with non-stop routing (NSR) enabled. Graceful Restart (GR) helper mode, enabled by default, is also required for this issue to be exploitable. Note: NSR is not supported on the SRX Series and is therefore not affected by this vulnerability. When the BGP session flaps on the NSR-enabled router, the device enters GR-helper/LLGR-helper mode due to the peer having negotiated GR/LLGR-restarter capability and the backup BGP requests for replication of the GR/LLGR-helper session, master BGP schedules, and initiates replication of GR/LLGR stale routes to the backup BGP. In this state, if the BGP session with the BGP peer comes up again, unsolicited replication is initiated for the peer without cleaning up the ongoing GR/LLGR-helper mode replication. This parallel two instances of replication for the same peer leads to the assert if the BGP session flaps again. This issue affects: Juniper Networks Junos OS * 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-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO; * 22.3 versions earlier than 22.3R3-S1-EVO; * 22.4 versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO; * 23.2 versions earlier than 23.2R1-S1-EVO, 23.2R2-EVO.	5.9	More Details
CVE-2023-50125	A default engineer password set on the Hozard alarm system (Alarmsysteem) v1.0 allows an attacker to bring the alarm system to a disarmed state.	5.9	More Details
CVE-2023-45236	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	5.8	More Details
CVE-2023-41781	There is a Cross-site scripting (XSS) vulnerability in ZTE MF258. Due to insufficient input validation of SMS interface parameter, an XSS attack will be triggered.	5.7	More Details
CVE-2023-29447	An insufficiently protected credentials vulnerability in KEPServerEX could allow an adversary to capture user credentials as the web server uses basic authentication.	5.7	More Details
CVE-2023-37522	HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower has missing or insecure tags that could allow an attacker to execute a malicious script on the user's browser.	5.6	More Details
CVE-2023-37523	Missing or insecure tags in the HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower could allow an attacker to execute a malicious script on the user's browser.	5.6	More Details
CVE-2022-45793	Sysmac Studio installs executables in a directory with poor permissions. This can allow a locally-authenticated attacker to overwrite files which will result in code execution with privileges of a different user.	5.5	More Details
CVE-2024-0364	A vulnerability, which was classified as critical, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file admin/query-details.php. The manipulation of the argument adminremark leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250131.	5.5	More Details
CVE-2023-50120	MP4Box GPAC version 2.3-DEV-rev636-gfbd7e13aa-master was discovered to contain an infinite loop in the function av1_uvlc at media_tools/av_parsers.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48504	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-0466	A vulnerability, which was classified as critical, has been found in code-projects Employee Profile Management System 1.0. This issue affects some unknown processing of the file file_table.php. The manipulation of the argument per_id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250571.	5.5	More Details
CVE-2024-0362	A vulnerability classified as critical was found in PHPGurukul Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/change-password.php. The manipulation of the argument cpass leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-250129 was assigned to this vulnerability.	5.5	More Details
CVE-2023-37644	SWFTools 0.9.2 772e55a allows attackers to trigger a large memory-allocation attempt via a crafted document, as demonstrated by pdf2swf. This occurs in png_read_chunk in lib/png.c.	5.5	More Details
CVE-2022-32931	This issue was addressed with improved data protection. This issue is fixed in macOS Ventura 13. An app with root privileges may be able to access private information.	5.5	More Details
CVE-2024-0357	A vulnerability was found in coderd-repos Eva 1.0.0 and classified as critical. Affected by this issue is some unknown functionality of the file /system/traceLog/page of the component HTTP POST Request Handler. The manipulation of the argument property leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250124.	5.5	More Details
CVE-2022-42816	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-50920	An issue was discovered on GL.iNet devices before version 4.5.0. They assign the same session ID after each user reboot, allowing attackers to share session identifiers between different sessions and bypass authentication or access control measures. Attackers can impersonate legitimate users or perform unauthorized actions. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	5.5	More Details
CVE-2022-46710	A logic issue was addressed with improved checks. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. Location data may be shared via iCloud links even if Location metadata is disabled via the Share Sheet.	5.5	More Details
CVE-2024-20721	Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-0363	A vulnerability, which was classified as critical, has been found in PHPGurukul Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file admin/patient-search.php. The manipulation of the argument searchdata leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250130 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-41987	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-42929	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access protected user data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40437	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to read sensitive location information.	5.5	More Details
CVE-2024-0361	A vulnerability classified as critical has been found in PHPGurukul Hospital Management System 1.0. Affected is an unknown function of the file admin/contact.php. The manipulation of the argument mobnum leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250128.	5.5	More Details
CVE-2023-42831	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to fingerprint the user.	5.5	More Details
CVE-2023-42829	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to access SSH passphrases.	5.5	More Details
CVE-2023-41994	A logic issue was addressed with improved checks This issue is fixed in macOS Sonoma 14. A camera extension may be able to access the camera view from apps other than the app for which it was granted permission.	5.5	More Details
CVE-2023-41069	This issue was addressed by improving Face ID anti-spoofing models. This issue is fixed in iOS 17 and iPadOS 17. A 3D model constructed to look like the enrolled user may authenticate via Face ID.	5.5	More Details
CVE-2023-48248	The vulnerability allows an authenticated remote attacker to upload a malicious file to the SD card containing arbitrary client-side script code and obtain its execution inside a victim's session via a crafted URL, HTTP request, or simply by waiting for the victim to view the poisoned file.	5.5	More Details
CVE-2023-40438	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14, iOS 16.7 and iPadOS 16.7. An app may be able to access edited photos saved to a temporary directory.	5.5	More Details
CVE-2023-40433	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may bypass Gatekeeper checks.	5.5	More Details
CVE-2023-28185	An integer overflow was addressed through improved input validation. This issue is fixed in tvOS 16.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4, watchOS 9.4, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2023-40430	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access removable volumes without user consent.	5.5	More Details
CVE-2023-40411	This issue was addressed with improved data protection. This issue is fixed in macOS Sonoma 14. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-0360	A vulnerability was found in PHPGurukul Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin/edit-doctor-specialization.php. The manipulation of the argument doctorspecilization leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250127.	5.5	More Details
CVE-2024-0554	A Cross-site scripting (XSS) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could store a malicious javascript payload in the device model parameter via '/setup/diags_ir_learn.asp', allowing the attacker to retrieve the session details of another user.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38607	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14. An app may be able to modify Printer settings.	5.5	More Details
CVE-2023-32424	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4, watchOS 9.4. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	5.5	More Details
CVE-2023-48258	The vulnerability allows a remote attacker to delete arbitrary files on the file system via a crafted URL or HTTP request through a victim's session.	5.5	More Details
CVE-2022-48577	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-20709	Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-48619	An issue was discovered in drivers/input/input.c in the Linux kernel before 5.17.10. An attacker can cause a denial of service (panic) because input_set_capability mishandles the situation in which an event code falls outside of a bitmap.	5.5	More Details
CVE-2024-0355	A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management System up to 1.1. Affected is an unknown function of the file add-category.php. The manipulation of the argument category leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250122 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2024-0443	A flaw was found in the blkgs destruction path in block/blk-cgroup.c in the Linux kernel, leading to a cgroup blkio memory leakage problem. When a cgroup is being destroyed, cgroup_rstat_flush() is only called at css_release_work_fn(), which is called when the blkcg reference count reaches 0. This circular dependency will prevent blkcg and some blkgs from being freed after they are made offline. This issue may allow an attacker with a local access to cause system instability, such as an out of memory error.	5.5	More Details
CVE-2024-23301	Relax-and-Recover (aka ReaR) through 2.7 creates a world-readable initrd when using GRUB_RESCUE=y. This allows local attackers to gain access to system secrets otherwise only readable by root.	5.5	More Details
CVE-2024-0530	A vulnerability was found in CXBSoft Post-Office up to 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /apps/reg_go.php of the component HTTP POST Request Handler. The manipulation of the argument username_reg leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250700. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2024-0529	A vulnerability has been found in CXBSoft Post-Office up to 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /apps/login_auth.php of the component HTTP POST Request Handler. The manipulation of the argument username_login leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250699. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2024-0528	A vulnerability, which was classified as critical, was found in CXBSoft Post-Office 1.0. Affected is an unknown function of the file /admin/pages/update_go.php of the component HTTP POST Request Handler. The manipulation of the argument version leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250698 is the identifier 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 Number	Description	Base Score	Reference
CVE-2024-20946	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2024-0526	A vulnerability classified as critical was found in CXBSoft Url-shorting up to 1.3.1. This vulnerability affects unknown code of the file /pages/short_to_long.php of the component HTTP POST Request Handler. The manipulation of the argument shorturl leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250696. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2024-0525	A vulnerability classified as critical has been found in CXBSoft Url-shorting up to 1.3.1. This affects an unknown part of the file /pages/long_s_short.php of the component HTTP POST Request Handler. The manipulation of the argument longurl leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250695. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2024-0524	A vulnerability was found in CXBSoft Url-shorting up to 1.3.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument url leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250694 is the identifier 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-2024-21594	A Heap-based Buffer Overflow vulnerability in the Network Services Daemon (NSD) of Juniper Networks Junos OS allows authenticated, low privileged, local attacker to cause a Denial of Service (DoS). On an SRX 5000 Series device, when executing a specific command repeatedly, memory is corrupted, which leads to a Flow Processing Daemon (flowd) crash. The NSD process has to be restarted to restore services. If this issue occurs, it can be checked with the following command: user@host> request security policies check The following log message can also be observed: Error: policies are out of sync for PFE node<number>.fpc<number>.pic<number>. This issue affects: Juniper Networks Junos OS on SRX 5000 Series * All versions earlier than 20.4R3-S6; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S4; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3-S1; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	5.5	More Details
CVE-2024-20715	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-0505	A vulnerability was found in ZhongFuCheng3y Austin 1.0 and classified as critical. This issue affects the function getFile of the file com/java3y/austin/web/controller/MaterialController.java of the component Upload Material Menu. The manipulation leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250619.	5.5	More Details
CVE-2024-20714	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-20713	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20712	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-20711	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-20710	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-20969	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2023-42872	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to access sensitive user data.	5.5	More Details
CVE-2022-4961	A vulnerability was found in Weitong Mall 1.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file platform-shop\src\main\resources\com\platform\dao\OrderDao.xml. The manipulation of the argument sidx/order leads to sql injection. The associated identifier of this vulnerability is VDB-250243.	5.5	More Details
CVE-2024-20967	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2023-51806	File Upload vulnerability in Ujcms v.8.0.2 allows a local attacker to execute arbitrary code via a crafted file.	5.4	More Details
CVE-2023-0079	The Customer Reviews for WooCommerce WordPress plugin before 5.17.0 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-2022-2413	The Slide Anything WordPress plugin before 2.3.47 does not properly sanitize or escape the slide title before outputting it in the admin pages, allowing a logged in user with roles as low as Author to inject a javascript payload into the slide title even when the unfiltered_html capability is disabled.	5.4	More Details
CVE-2022-3194	The Dokan WordPress plugin before 3.6.4 allows vendors to inject arbitrary javascript in product reviews, which may allow them to run stored XSS attacks against other users like site administrators.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48783	An Authorization Bypass Through User-Controlled Key vulnerability [CWE-639] affecting PortiPortal version 7.2.1 and below, version 7.0.6 and below, version 6.0.14 and below, version 5.3.8 and below may allow a remote authenticated user with at least read-only permissions to access to other organization endpoints via crafted GET requests.	5.4	More Details
CVE-2023-4757	The Staff / Employee Business Directory for Active Directory WordPress plugin before 1.2.3 does not sanitize and escape data returned from the LDAP server before rendering it in the page, allowing users who can control their entries in the LDAP directory to inject malicious javascript which could be used against high-privilege users such as a site admin.	5.4	More Details
CVE-2024-22491	A Stored Cross Site Scripting (XSS) vulnerability in beetl-bbs 2.0 allows attackers to run arbitrary code via the post/save content parameter.	5.4	More Details
CVE-2022-3739	The WP Best Quiz WordPress plugin through 1.0 does not sanitize and escape some parameters, which could allow users with a role as low as Author to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2024-23178	An issue was discovered in the Phonos extension in MediaWiki before 1.40.2. PhonosButton.js allows i18n-based XSS via the phonos-purge-needed-error message.	5.4	More Details
CVE-2021-24567	The Simple Post WordPress plugin through 1.1 does not sanitize user input when an authenticated user Text value, then it does not escape these values when outputting to the browser leading to an Authenticated Stored XSS Cross-Site Scripting issue.	5.4	More Details
CVE-2023-3372	The Lana Shortcodes WordPress plugin before 1.2.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which allows users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0094	The UpQode Google Maps WordPress plugin through 1.0.5 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-2021-24559	The Qyrr WordPress plugin before 0.7 does not escape the data-uri of the QR Code when outputting it in a src attribute, allowing for Cross-Site Scripting attacks. Furthermore, the data_uri_to_meta AJAX action, available to all authenticated users, only had a CSRF check in place, with the nonce available to users with a role as low as Contributor allowing any user with such role (and above) to set a malicious data-uri in arbitrary QR Code posts, leading to a Stored Cross-Site Scripting issue.	5.4	More Details
CVE-2024-20987	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2023-0376	The Qubely WordPress plugin before 1.8.5 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2024-23174	An issue was discovered in the PageTriage extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. XSS can occur via the rev-deleted-user, pagetriage-tags-quickfilter-label, pagetriage-triage, pagetriage-filter-date-range-format-placeholder, pagetriage-filter-date-range-to, pagetriage-filter-date-range-from, pagetriage-filter-date-range-heading, pagetriage-filter-set-button, or pagetriage-filter-reset-button message.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24433	The simple sort&search WordPress plugin through 0.0.3 does not make sure that the indexurl parameter of the shortcodes "category_sims", "order_sims", "orderby_sims", "period_sims", and "tag_sims" use allowed URL protocols, which can lead to stored cross-site scripting by users with a role as low as Contributor	5.4	More Details
CVE-2024-23172	An issue was discovered in the CheckUser extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. XSS can occur via message definitions. e.g., in SpecialCheckUserLog.	5.4	More Details
CVE-2024-23171	An issue was discovered in the CampaignEvents extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. The Special:EventDetails page allows XSS via the x-xss language setting for internationalization (i18n).	5.4	More Details
CVE-2023-51807	Cross Site Scripting vulnerability in OFCMS v.1.14 allows a remote attacker to obtain sensitive information via a crafted payload to the title addition component.	5.4	More Details
CVE-2023-7083	The Voting Record WordPress plugin through 2.0 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-2024-22492	A stored XSS vulnerability exists in JFinalcms 5.0.0 via the /gusetbook/save contact parameter, which allows remote attackers to inject arbitrary web script or HTML.	5.4	More Details
CVE-2024-20944	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iSupport accessible data as well as unauthorized read access to a subset of Oracle iSupport accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2023-6369	The Export WP Page to Static HTML/CSS plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on multiple AJAX actions in all versions up to, and including, 2.1.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to disclose sensitive information or perform unauthorized actions, such as saving advanced plugin settings.	5.4	More Details
CVE-2024-0319	Open Redirect vulnerability in FireEye HXTool affecting version 4.6, the exploitation of which could allow an attacker to redirect a legitimate user to a malicious page by changing the 'redirect_uri' parameter.	5.4	More Details
CVE-2024-0320	Cross-Site Scripting in FireEye Malware Analysis (AX) affecting version 9.0.3.936530. This vulnerability allows an attacker to send a specially crafted JavaScript payload in the application URL to retrieve the session details of a legitimate user.	5.4	More Details
CVE-2023-7084	The Voting Record WordPress plugin through 2.0 is missing sanitisation as well as escaping, which could allow any authenticated users, such as subscriber to perform Stored XSS attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20979	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2023-51252	PublicCMS 4.0 is vulnerable to Cross Site Scripting (XSS). Because files can be uploaded and online preview function is provided, pdf files and html files containing malicious code are uploaded, an XSS popup window is realized through online viewing.	5.4	More Details
CVE-2023-6556	The FOX – Currency Switcher Professional for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via currency options in all versions up to, and including, 1.4.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-0314	XSS vulnerability in FireEye Central Management affecting version 9.1.1.956704, which could allow an attacker to modify special HTML elements in the application and cause a reflected XSS, leading to a session hijacking.	5.4	More Details
CVE-2024-22195	Jinja is an extensible templating engine. Special placeholders in the template allow writing code similar to Python syntax. It is possible to inject arbitrary HTML attributes into the rendered HTML template, potentially leading to Cross-Site Scripting (XSS). The Jinja `xmlattr` filter can be abused to inject arbitrary HTML attribute keys and values, bypassing the auto escaping mechanism and potentially leading to XSS. It may also be possible to bypass attribute validation checks if they are blacklist-based.	5.4	More Details
CVE-2024-22494	A stored XSS vulnerability exists in JFinalcms 5.0.0 via the /gusetbook/save mobile parameter, which allows remote attackers to inject arbitrary web script or HTML.	5.4	More Details
CVE-2024-22493	A stored XSS vulnerability exists in JFinalcms 5.0.0 via the /gusetbook/save content parameter, which allows remote attackers to inject arbitrary web script or HTML.	5.4	More Details
CVE-2024-0318	Cross-Site Scripting in FireEye HXTool affecting version 4.6. This vulnerability allows an attacker to store a specially crafted JavaScript payload in the 'Profile Name' and 'Hostname/IP' parameters that will be triggered when items are loaded.	5.4	More Details
CVE-2024-0317	Cross-Site Scripting in FireEye EX, affecting version 9.0.3.936727. Exploitation of this vulnerability allows an attacker to send a specially crafted JavaScript payload via the 'type' and 's_f_name' parameters to an authenticated user to retrieve their session details.	5.4	More Details
CVE-2023-5118	The application is vulnerable to Stored Cross-Site Scripting (XSS) in the endpoint /sofer/DocumentService.asc/SaveAnnotation, where input data transmitted via the POST method in the parameters author and text are not adequately sanitized and validated. This allows for the injection of malicious JavaScript code. The vulnerability was identified in the function for adding new annotations while editing document content. Reporters inform that the vulnerability has been removed in software versions above 11.1.x. Previous versions may also be vulnerable, but this has not been confirmed.	5.4	More Details
CVE-2024-21640	Chromium Embedded Framework (CEF) is a simple framework for embedding Chromium-based browsers in other applications.`CefVideoConsumerOSR::OnFrameCaptured` does not check `pixel_format` properly, which leads to out-of-bounds read out of the sandbox. This vulnerability was patched in commit 1f55d2e.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6990	The Weaver Xtreme theme for WordPress is vulnerable to Stored Cross-Site Scripting via custom post meta in all versions up to, and including, 6.3.0 due to insufficient input sanitization and output escaping on user supplied meta (page-head-code). This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2023-4247	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.33.3. This is due to missing or incorrect nonce validation on the give_sendwp_disconnect function. This makes it possible for unauthenticated attackers to deactivate the SendWP plugin 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-2024-0417	A vulnerability, which was classified as critical, was found in DeShang DSShop up to 2.1.5. This affects an unknown part of the file application/home/controller/MemberAuth.php. The manipulation of the argument member_info 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-250437 was assigned to this vulnerability.	5.4	More Details
CVE-2023-4248	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.33.3. This is due to missing or incorrect nonce validation on the give_stripe_disconnect_connect_stripe_account function. This makes it possible for unauthenticated attackers to deactivate the plugin's stripe integration settings 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-2023-50072	A Stored Cross-Site Scripting (XSS) vulnerability exists in OpenKM version 7.1.40 (dbb6e88) With Professional Extension that allows an authenticated user to upload a note on a file which acts as a stored XSS payload. Any user who opens the note of a document file will trigger the XSS.	5.4	More Details
CVE-2024-0416	A vulnerability, which was classified as critical, has been found in DeShang DSMall up to 5.0.3. Affected by this issue is some unknown functionality of the file application/home/controller/MemberAuth.php. The manipulation of the argument file_name leads to path traversal: '../filedir'. 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-250436.	5.4	More Details
CVE-2023-51068	An authenticated reflected cross-site scripting (XSS) vulnerability in QStar Archive Solutions Release RELEASE_3-0 Build 7 allows attackers to execute arbitrary javascript on a victim's browser via a crafted link.	5.4	More Details
CVE-2023-50128	The remote keyless system of the Hozard alarm system (alarmsystemen) v1.0 sends an identical radio frequency signal for each request, which results in an attacker being able to conduct replay attacks to bring the alarm system to a disarmed state.	5.3	More Details
CVE-2024-0546	A vulnerability, which was classified as problematic, has been found in EasyFTP 1.7.0. This issue affects some unknown processing of the component LIST 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 associated identifier of this vulnerability is VDB-250715.	5.3	More Details
CVE-2023-48261	The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.	5.3	More Details
CVE-2022-1563	The WPGraphQL WooCommerce WordPress plugin before 0.12.4 does not prevent unauthenticated attackers from enumerating a shop's coupon codes and values via GraphQL.	5.3	More Details
CVE-2024-0547	A vulnerability has been found in Ability FTP Server 2.34 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component APPE Command Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250717 was assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0548	A vulnerability was found in FreeFloat FTP Server 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the component SIZE Command 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-250718 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-5253	A missing authentication check in the WebSocket channel used for the Check Point IoT integration in Nozomi Networks Guardian and CMC, may allow an unauthenticated attacker to obtain assets data without authentication. Malicious unauthenticated users with knowledge on the underlying system may be able to extract limited asset information.	5.3	More Details
CVE-2024-0354	A vulnerability, which was classified as critical, has been found in unknown-o download-station up to 1.1.8. This issue affects some unknown processing of the file index.php. The manipulation of the argument f leads to path traversal: '../filedir'. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250121 was assigned to this vulnerability.	5.3	More Details
CVE-2024-0418	A vulnerability has been found in iSharer and upRedSun File Sharing Wizard up to 1.5.0 and classified as problematic. This vulnerability affects unknown code of the component GET Request 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. VDB-250438 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2024-0237	The EventON WordPress plugin through 4.5.8, EventON WordPress plugin before 2.2.7 do not have authorisation in some AJAX actions, allowing unauthenticated users to update virtual events settings, such as meeting URL, moderator, access details etc	5.3	More Details
CVE-2024-0545	A vulnerability classified as problematic was found in CodeCanyon RISE Rise Ultimate Project Manager 3.5.3. This vulnerability affects unknown code of the file /index.php/signin. The manipulation of the argument redirect with the input http://evil.com leads to open redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250714 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-6496	The Manage Notification E-mails plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.8.5 via the card_famne_export_settings function. This makes it possible for unauthenticated attackers to obtain plugin settings.	5.3	More Details
CVE-2023-50172	A recovery notification bypass vulnerability exists in the userRecoverPass.php captcha validation functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to the silent creation of a recovery pass code for any user.	5.3	More Details
CVE-2024-0236	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve the settings of arbitrary virtual events, including any meeting password set (for example for Zoom)	5.3	More Details
CVE-2023-41603	D-Link R15 before v1.08.02 was discovered to contain no firewall restrictions for IPv6 traffic. This allows attackers to arbitrarily access any services running on the device that may be inadvertently listening via IPv6.	5.3	More Details
CVE-2024-0235	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve email addresses of any users on the blog	5.3	More Details
CVE-2023-6582	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.0.3 via the ekit_widgetarea_content function. This makes it possible for unauthenticated attackers to obtain contents of posts in draft, private or pending review status that should not be visible to the general public. This applies to posts created with Elementor only.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21639	CEF (Chromium Embedded Framework) is a simple framework for embedding Chromium-based browsers in other applications. `CefLayeredWindowUpdaterOSR::OnAllocatedSharedMemory` does not check the size of the shared memory, which leads to out-of-bounds read outside the sandbox. This vulnerability was patched in commit 1f55d2e.	5.3	More Details
CVE-2024-21607	An Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on MX Series and EX9200 Series allows an unauthenticated, network-based attacker to cause partial impact to the integrity of the device. If the "tcp-reset" option is added to the "reject" action in an IPv6 filter which matches on "payload-protocol", packets are permitted instead of rejected. This happens because the payload-protocol match criteria is not supported in the kernel filter causing it to accept all packets without taking any other action. As a fix the payload-protocol match will be treated the same as a "next-header" match to avoid this filter bypass. This issue doesn't affect IPv4 firewall filters. This issue affects Juniper Networks Junos OS on MX Series and EX9200 Series: * All versions earlier than 20.4R3-S7; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2-S2, 22.4R3.	5.3	More Details
CVE-2023-45237	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	5.3	More Details
CVE-2023-51062	An unauthenticated log file read in the component log-smblog-save of QStar Archive Solutions RELEASE_3-0 Build 7 Patch 0 allows attackers to disclose the SMB Log contents via executing a crafted command.	5.3	More Details
CVE-2023-6855	The Paid Memberships Pro – Content Restriction, User Registration, & Paid Subscriptions plugin for WordPress is vulnerable to unauthorized modification of membership levels created by the plugin due to an incorrectly implemented capability check in the pmpro_rest_api_get_permissions_check function in all versions up to 2.12.5 (inclusive). This makes it possible for unauthenticated attackers to change membership levels including prices.	5.3	More Details
CVE-2024-21596	A Heap-based Buffer Overflow vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). If an attacker sends a specific BGP UPDATE message to the device, this will cause a memory overwrite and therefore an RPD crash and restart in the backup Routing Engine (RE). Continued receipt of these packets will cause a sustained Denial of Service (DoS) condition in the backup RE. The primary RE is not impacted by this issue and there is no impact on traffic. This issue only affects devices with NSR enabled. Note: NSR is not supported on the SRX Series and is therefore not affected by this vulnerability. This issue requires an attacker to have an established BGP session to a system affected by the issue. This issue affects both eBGP and iBGP implementations. This issue affects: Juniper Networks Junos OS * 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-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.1 versions earlier than 23.1R2; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S4-EVO; * 22.2-EVO versions earlier than 22.2R3-S2-EVO; * 22.3-EVO versions later than 22.3R1-EVO; * 22.4-EVO versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO; * 23.1-EVO versions earlier than 23.1R2-EVO; * 23.2-EVO versions earlier than 23.2R1-S2-EVO, 23.2R2-EVO.	5.3	More Details
CVE-2023-6592	The FastDup WordPress plugin before 2.2 does not prevent directory listing in sensitive directories containing export files.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21597	An Exposure of Resource to Wrong Sphere vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass the intended access restrictions. In an Abstracted Fabric (AF) scenario if routing-instances (RI) are configured, specific valid traffic destined to the device can bypass the configured lo0 firewall filters as it's received in the wrong RI context. This issue affects Juniper Networks Junos OS on MX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	5.3	More Details
CVE-2021-4227	The ark-commenteditor WordPress plugin through 2.15.6 does not properly sanitise or encode the comments when in Source editor, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page to the comment section	5.3	More Details
CVE-2023-48260	The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.	5.3	More Details
CVE-2023-7234	OPCUAServerToolkit will write a log message once an OPC UA client has successfully connected containing the client's self-defined description field.	5.3	More Details
CVE-2023-52112	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally.	5.3	More Details
CVE-2024-0411	A vulnerability was found in DeShang DSMall up to 6.1.0. It has been classified as problematic. This affects an unknown part of the file public/install.php of the component HTTP GET Request Handler. The manipulation leads to improper access controls. 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-250431.	5.3	More Details
CVE-2023-48254	The vulnerability allows a remote attacker to inject and execute arbitrary client-side script code inside a victim’s session via a crafted URL or HTTP request.	5.3	More Details
CVE-2024-0358	A vulnerability was found in DeShang DSO2O up to 4.1.0. It has been classified as critical. This affects an unknown part of the file /install/install.php. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250125 was assigned to this vulnerability.	5.3	More Details
CVE-2024-0412	A vulnerability was found in DeShang DSShop up to 3.1.0. It has been declared as problematic. This vulnerability affects unknown code of the file public/install.php of the component HTTP GET Request Handler. The manipulation 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-250432.	5.3	More Details
CVE-2024-0413	A vulnerability was found in DeShang DSKMS up to 3.1.2. It has been rated as problematic. This issue affects some unknown processing of the file public/install.php. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250433 was assigned to this vulnerability.	5.3	More Details
CVE-2023-49107	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Agent modules).This issue affects Hitachi Device Manager: before 8.8.5-04.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0490	A vulnerability was found in Huaxia ERP up to 3.1. It has been rated as problematic. This issue affects some unknown processing of the file /user/getAllList. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-250595.	5.3	More Details
CVE-2023-48256	The vulnerability allows a remote attacker to inject arbitrary HTTP response headers or manipulate HTTP response bodies inside a victim's session via a crafted URL or HTTP request.	5.3	More Details
CVE-2024-0414	A vulnerability classified as problematic has been found in DeShang DSCMS up to 3.1.2/7.1. Affected is an unknown function of the file public/install.php. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250434 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-28898	The Real-Time Streaming Protocol implementation in the MIB3 infotainment incorrectly handles requests to /logs URI, when the id parameter equals to zero. This issue allows an attacker connected to the in-vehicle Wi-Fi network to cause denial-of-service of the infotainment system, when the certain preconditions are met. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	5.3	More Details
CVE-2023-48247	The vulnerability allows an unauthenticated remote attacker to read arbitrary files under the context of the application OS user ("root") via a crafted HTTP request.	5.3	More Details
CVE-2024-0419	A vulnerability was found in Jasper httpdx up to 1.5.4 and classified as problematic. This issue affects some unknown processing of the component HTTP POST Request 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 associated identifier of this vulnerability is VDB-250439.	5.3	More Details
CVE-2024-0333	Insufficient data validation in Extensions in Google Chrome prior to 120.0.6099.216 allowed an attacker in a privileged network position to install a malicious extension via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2023-6334	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in HYPR Workforce Access on Windows allows Overflow Buffers.This issue affects Workforce Access: before 8.7.	5.3	More Details
CVE-2023-0437	When calling bson_utf8_validate on some inputs a loop with an exit condition that cannot be reached may occur, i.e. an infinite loop. This issue affects All MongoDB C Driver versions prior to versions 1.25.0.	5.3	More Details
CVE-2024-0491	A vulnerability classified as problematic has been found in Huaxia ERP up to 3.1. Affected is an unknown function of the file src/main/java/com/jsh/erp/controller/UserController.java. The manipulation leads to weak password recovery. It is possible to launch the attack remotely. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-250596.	5.3	More Details
CVE-2024-0425	A vulnerability classified as critical was found in ForU CMS up to 2020-06-23. This vulnerability affects unknown code of the file /admin/index.php?act=reset_admin_psw. The manipulation leads to weak password recovery. 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-250444.	5.3	More Details
CVE-2023-48244	The vulnerability allows a remote attacker to inject and execute arbitrary client-side script code inside a victim's session via a crafted URL or HTTP request.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22207	fastify-swagger-ui is a Fastify plugin for serving Swagger UI. Prior to 2.1.0, the default configuration of `@fastify/swagger-ui` without `baseDir` set will lead to all files in the module's directory being exposed via http routes served by the module. The vulnerability is fixed in v2.1.0. Setting the `baseDir` option can also work around this vulnerability.	5.3	More Details
CVE-2023-48926	An issue in 202 ecommerce Advanced Loyalty Program: Loyalty Points before v2.3.4 for PrestaShop allows unauthenticated attackers to arbitrarily change an order status.	5.3	More Details
CVE-2021-4432	A vulnerability was found in PCMan FTP Server 2.0.7. It has been classified as problematic. This affects an unknown part of the component USER Command Handler. 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-250719.	5.3	More Details
CVE-2023-48259	The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.	5.3	More Details
CVE-2024-21337	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	5.2	More Details
CVE-2023-31001	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) temporarily stores sensitive information in files that could be accessed by a local user. IBM X-Force ID: 254653.	5.1	More Details
CVE-2024-20904	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	5.0	More Details
CVE-2024-20983	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-6624	The Import and export users and customers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.24.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.9	More Details
CVE-2020-26630	A Time-Based SQL Injection vulnerability was discovered in Hospital Management System V4.0 which can allow an attacker to dump database information via a special payload in the 'Doctor Specialization' field under the 'Go to Doctors' tab after logging in as an admin.	4.9	More Details
CVE-2024-20981	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26627	A Time-Based SQL Injection vulnerability was discovered in Hospital Management System V4.0 which can allow an attacker to dump database information via a crafted payload entered into the 'Admin Remark' parameter under the 'Contact Us Queries -> Unread Query' tab.	4.9	More Details
CVE-2024-20971	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-20965	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-22407	Shopware is an open headless commerce platform. In the Shopware CMS, the state handler for orders fails to sufficiently verify user authorizations for actions that modify the payment, delivery, and/or order status. Due to this inadequate implementation, users lacking 'write' permissions for orders are still able to change the order state. This issue has been addressed and users are advised to update to Shopware 6.5.7.4. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.	4.9	More Details
CVE-2023-6005	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 does not sanitize 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-2023-6046	The EventON WordPress plugin before 2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored HTML Injection attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2023-42941	The issue was addressed with improved checks. This issue is fixed in iOS 17.2 and iPadOS 17.2. An attacker in a privileged network position may be able to perform a denial-of-service attack using crafted Bluetooth packets.	4.8	More Details
CVE-2023-7154	The Hubbub Lite (formerly Grow Social) WordPress plugin before 1.32.0 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-2023-6732	The Ultimate Maps by Supsystic WordPress plugin before 1.2.16 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-2023-6163	The WP Crowdfunding WordPress plugin before 2.1.10 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-2021-25117	The WP-PostRatings WordPress plugin before 1.86.1 does not sanitise the postratings_image parameter from its options page (wp-admin/admin.php?page=wp-postratings/postratings-options.php). Even though the page is only accessible to administrators, and protected against CSRF attacks, the issue is still exploitable when the unfiltered_html capability is disabled.	4.8	More Details
CVE-2023-36236	Cross Site Scripting vulnerability in webkil Bagisto v.1.5.0 and before allows an attacker to execute arbitrary code via a crafted SVG file uplad.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3829	The Font Awesome 4 Menus WordPress plugin through 4.7.0 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-2023-6941	The Keap Official Opt-in Forms WordPress plugin through 1.0.11 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-2022-23179	The Contact Form & Lead Form Elementor Builder WordPress plugin before 1.7.0 does not escape some of its form fields before outputting them in attributes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2024-21654	Rubygems.org is the Ruby community's gem hosting service. Rubygems.org users with MFA enabled would normally be protected from account takeover in the case of email account takeover. However, a workaround on the forgotten password form allows an attacker to bypass the MFA requirement and takeover the account. This vulnerability has been patched in commit 0b3272a.	4.8	More Details
CVE-2023-0389	The Calculated Fields Form WordPress plugin before 1.1.151 does not sanitise and escape some of its form 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-2024-20906	Vulnerability in the Integrated Lights Out Manager (ILOM) product of Oracle Systems (component: System Management). Supported versions that are affected are 3, 4 and 5. Easily exploitable vulnerability allows high privileged attacker with network access via ICMP to compromise Integrated Lights Out Manager (ILOM). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Integrated Lights Out Manager (ILOM), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	4.8	More Details
CVE-2023-4925	The Easy Forms for Mailchimp WordPress plugin through 6.8.10 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-2023-3647	The IURNY by INDIGITALL WordPress plugin before 3.2.3 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-2022-3836	The Seed Social WordPress plugin before 2.0.4 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-2024-21982	ONTAP versions 9.4 and higher are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information to unprivileged attackers when the object-store profiler command is being run by an administrative user.	4.8	More Details
CVE-2023-28899	By sending a specific reset UDS request via OBDII port of Skoda vehicles, it is possible to cause vehicle engine shutdown and denial of service of other vehicle components even when the vehicle is moving at a high speed. No safety critical functions affected.	4.7	More Details
CVE-2024-0502	A vulnerability was found in SourceCodester House Rental Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file manage_user.php of the component Edit User. The manipulation of the argument id/name/username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250610 is the identifier assigned to this vulnerability.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0459	A vulnerability has been found in Blood Bank & Donor Management 5.6 and classified as critical. This vulnerability affects unknown code of the file /admin/request-received-bydonar.php. The manipulation leads to sql 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-250564.	4.7	More Details
CVE-2024-0558	A vulnerability has been found in DedeBIZ 6.3.0 and classified as critical. This vulnerability affects unknown code of the file /admin/makehtml_freelist_action.php. The manipulation of the argument startid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250726 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-2023-6737	The Enable Media Replace plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the SHORTPIXEL_DEBUG parameter in all versions up to, and including, 4.1.4 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. Exploiting this vulnerability requires the attacker to know the ID of an attachment uploaded by the user they are attacking.	4.7	More Details
CVE-2023-29446	An improper input validation vulnerability has been discovered that could allow an adversary to inject a UNC path via a malicious project file. This allows an adversary to capture NLTMv2 hashes and potentially crack them offline.	4.7	More Details
CVE-2024-0232	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service.	4.7	More Details
CVE-2022-32919	The issue was addressed with improved UI handling. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. Visiting a website that frames malicious content may lead to UI spoofing.	4.7	More Details
CVE-2023-49106	Missing Password Field Masking vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Agent component).This issue affects Hitachi Device Manager: before 8.8.5-04.	4.6	More Details
CVE-2024-22028	Insufficient technical documentation issue exists in thermal camera TMC series all firmware versions. The user of the affected product is not aware of the internally saved data. By accessing the affected product physically, an attacker may retrieve the internal data.	4.6	More Details
CVE-2024-0555	A Cross-Site Request Forgery (CSRF) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could lead another user into executing unwanted actions inside the application they are logged in. This vulnerability is possible due to the lack of propper CSRF token implementation.	4.6	More Details
CVE-2023-51750	ScaleFusion 10.5.2 does not properly limit users to the Edge application because file downloads can occur. NOTE: the vendor's position is "Not vulnerable if the default Windows device profile configuration is used which utilizes modern management with website allow-listing rules."	4.6	More Details
CVE-2023-52106	Vulnerability of permission verification for APIs in the DownloadProviderMain module. Impact: Successful exploitation of this vulnerability will affect integrity and availability.	4.4	More Details
CVE-2024-20959	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6446	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.40 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-2023-6924	The Photo Gallery by 10Web plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widgets in versions up to, and including, 1.8.18 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with administrator-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. It can also be exploited with a contributor-level permission with a page builder plugin.	4.4	More Details
CVE-2023-5691	The Chatbot for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in version 2.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-6741	The WP Customer Area WordPress plugin before 8.2.1 does not properly validate users capabilities in some of its AJAX actions, allowing malicious users to edit other users' account address.	4.3	More Details
CVE-2023-6630	The Contact Form 7 – Dynamic Text Extension plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.1.0 via the CF7_get_custom_field and CF7_get_current_user shortcodes due to missing validation on a user controlled key. This makes it possible for authenticated attackers with contributor access or higher to access arbitrary metadata of any post type, referencing the post by id and the meta by key.	4.3	More Details
CVE-2023-6066	The WP Custom Widget area WordPress plugin through 1.2.5 does not properly apply capability and nonce checks on any of its AJAX action callback functions, which could allow attackers with subscriber+ privilege to create, delete or modify menus on the site.	4.3	More Details
CVE-2023-6223	The LearnPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.2.5.7 via the /wp-json/lp/v1/profile/course-tab REST API due to missing validation on the 'userID' user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve the details of another user's course progress.	4.3	More Details
CVE-2023-6506	The WP 2FA – Two-factor authentication for WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.5.0 via the send_backup_codes_email due to missing validation on a user controlled key. This makes it possible for subscriber-level attackers to email arbitrary users on the site.	4.3	More Details
CVE-2023-6520	The WP 2FA – Two-factor authentication for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.0. This is due to missing or incorrect nonce validation on the send_backup_codes_email function. This makes it possible for unauthenticated attackers to send emails with arbitrary content to registered users via a forged request granted they can trick a site administrator or other registered user into performing an action such as clicking on a link. While a nonce check is present, it is only executed if a nonce is set. By omitting a nonce from the request, the check can be bypassed.	4.3	More Details
CVE-2023-6883	The Easy Social Feed plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on multiple AJAX functions in all versions up to, and including, 6.5.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform unauthorized actions, such as modifying the plugin's Facebook and Instagram access tokens and updating group IDs.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4246	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.33.3. This is due to missing or incorrect nonce validation on the give_sendwp_remote_install_handler function. This makes it possible for unauthenticated attackers to install and activate the SendWP plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-6504	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the wppb_toolbox_usermeta_handler function in all versions up to, and including, 3.10.7. This makes it possible for authenticated attackers, with contributor-level access and above, to expose sensitive information within user metadata.	4.3	More Details
CVE-2024-21665	ecommerce-framework-bundle is the Pimcore Ecommerce Framework Bundle. An authenticated and unauthorized user can access the back-office orders list and be able to query over the information returned. Access control and permissions are not being enforced. This vulnerability has been patched in version 1.0.10.	4.3	More Details
CVE-2023-6598	The SpeedyCache plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the speedycache_save_varniship, speedycache_img_update_settings, speedycache_preloading_add_settings, and speedycache_preloading_delete_resource functions in all versions up to, and including, 1.1.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to update plugin options.	4.3	More Details
CVE-2024-0522	A vulnerability was found in Allegro RomPager 4.01. It has been classified as problematic. Affected is an unknown function of the file usertable.htm?action=delete of the component HTTP POST Request Handler. The manipulation of the argument username leads to cross-site request forgery. It is possible to launch the attack remotely. Upgrading to version 4.30 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-250692. NOTE: The vendor explains that this is a very old issue that got fixed 20 years ago but without a public disclosure.	4.3	More Details
CVE-2023-6742	The Gallery Plugin for WordPress – Envira Photo Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the 'envira_gallery_insert_images' function in all versions up to, and including, 1.8.7.1. This makes it possible for authenticated attackers, with contributor access and above, to modify galleries on other users' posts.	4.3	More Details
CVE-2023-7019	The LightStart – Maintenance Mode, Coming Soon and Landing Page Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the insert_template function in all versions up to, and including, 2.6.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to change page designs.	4.3	More Details
CVE-2022-4962	A vulnerability was found in Apollo 2.0.0/2.0.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /users of the component Configuration Center. The manipulation leads to improper authorization. The attack may be launched 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. VDB-250430 is the identifier assigned to this vulnerability. NOTE: The maintainer explains that user data information like user id, name, and email are not sensitive.	4.3	More Details
CVE-2024-21655	Discourse is a platform for community discussion. For fields that are client editable, limits on sizes are not imposed. This allows a malicious actor to cause a Discourse instance to use excessive disk space and also often excessive bandwidth. The issue is patched 3.1.4 and 3.2.0.beta4.	4.3	More Details
CVE-2010-10011	A vulnerability, which was classified as problematic, was found in Acritum Femitter Server 1.04. Affected is an unknown function. The manipulation leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250446 is the identifier assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0356	A vulnerability has been found in Mandelo ssm_shiro_blog 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file updateRoles of the component Backend. The manipulation leads to improper access controls. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250123.	4.3	More Details
CVE-2023-40362	An issue was discovered in CentralSquare Click2Gov Building Permit before October 2023. Lack of access control protections allows remote attackers to arbitrarily delete the contractors from any user's account when the user ID and contractor information is known.	4.3	More Details
CVE-2023-6843	The easy.jobs- Best Recruitment Plugin for Job Board Listing, Manager, Career Page for Elementor & Gutenberg WordPress plugin before 2.4.7 does not properly secure some of its AJAX actions, allowing any logged-in users to modify its settings.	4.3	More Details
CVE-2023-7125	The Community by PeepSo WordPress plugin before 6.3.1.2 does not have CSRF check when creating a user post (visible on their wall in their profile page), which could allow attackers to make logged in users perform such action via a CSRF attack	4.3	More Details
CVE-2023-3178	The POST SMTP Mailer WordPress plugin before 2.5.7 does not have proper CSRF checks in some AJAX actions, which could allow attackers to make logged in users with the manage_postman_smtp capability delete arbitrary logs via a CSRF attack.	4.3	More Details
CVE-2022-0775	The WooCommerce WordPress plugin before 6.2.1 does not have proper authorisation check when deleting reviews, which could allow any authenticated users, such as subscriber to delete arbitrary comment	4.3	More Details
CVE-2023-37934	An allocation of resources without limits or throttling vulnerability [CWE-770] in FortiPAM 1.0 all versions allows an authenticated attacker to perform a denial of service attack via sending crafted HTTP or HTTPS requests in a high frequency.	4.3	More Details
CVE-2023-6292	The Ecwid Ecommerce Shopping Cart WordPress plugin before 6.12.5 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.	4.3	More Details
CVE-2022-1760	The Core Control WordPress plugin through 1.2.1 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	4.3	More Details
CVE-2022-23180	The Contact Form & Lead Form Elementor Builder WordPress plugin before 1.7.4 doesn't have authorisation and nonce checks, which could allow any authenticated users, such as subscriber to update and change various settings	4.3	More Details
CVE-2023-49715	A unrestricted php file upload vulnerability exists in the import.json.php temporary copy functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary code execution when chained with an LFI vulnerability. An attacker can send a series of HTTP requests to trigger this vulnerability.	4.3	More Details
CVE-2024-0569	A vulnerability classified as problematic has been found in Totolink T8 4.1.5cu.833_20220905. This affects the function getSysStatusCfg of the file /cgi-bin/cstecgi.cgi of the component Setting Handler. The manipulation of the argument ssid/key leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.5cu.862_B20230228 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-250785 was assigned to this vulnerability.	4.3	More Details
CVE-2023-42934	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app with root privileges may be able to access private information.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49801	Lif Auth Server is a server for validating logins, managing information, and account recovery for Lif Accounts. The issue relates to the `get_pfp` and `get_banner` routes on Auth Server. The issue is that there is no check to ensure that the file that Auth Server is receiving through these URLs is correct. This could allow an attacker access to files they shouldn't have access to. This issue has been patched in version 1.4.0.	4.2	More Details
CVE-2023-31031	NVIDIA DGX A100 SBIOS contains a vulnerability where a user may cause a heap-based buffer overflow by local access. A successful exploit of this vulnerability may lead to code execution, denial of service, information disclosure, and data tampering.	4.2	More Details
CVE-2023-28897	The secret value used for access to critical UDS services of the MIB3 infotainment is hardcoded in the firmware. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	4.0	More Details
CVE-2024-0581	An Uncontrolled Resource Consumption vulnerability has been found on Sandsprite Scdbg.exe, affecting version 1.0. This vulnerability allows an attacker to send a specially crafted shellcode payload to the '/foff' parameter and cause an application shutdown. A malware program could use this shellcode sequence to shut down the application and evade the scan.	4.0	More Details
CVE-2024-20920	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	3.8	More Details
CVE-2024-20955	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2023-49098	Discourse-reactions is a plugin that allows user to add their reactions to the post. Data about a user's reaction notifications could be exposed. This vulnerability was patched in commit 2c26939.	3.5	More Details
CVE-2024-0472	A vulnerability was found in code-projects Dormitory Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file modifyuser.php. The manipulation of the argument mname leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-250577 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0503	A vulnerability was found in code-projects Online FIR System 1.0. It has been classified as problematic. This affects an unknown part of the file registercomplaint.php. The manipulation of the argument Name/Address 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-250611.	3.5	More Details
CVE-2022-4958	A vulnerability classified as problematic has been found in qkmc-rk redbbs 1.0. Affected is an unknown function of the component Post Handler. The manipulation of the argument title 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-250236.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0465	A vulnerability classified as problematic was found in code-projects Employee Profile Management System 1.0. This vulnerability affects unknown code of the file download.php. The manipulation of the argument download_file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-250570 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0467	A vulnerability, which was classified as problematic, was found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file edit_position_query.php. The manipulation of the argument pos_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-250572.	3.5	More Details
CVE-2024-0422	A vulnerability was found in CodeAstro POS and Inventory Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /new_item of the component New Item Creation Page. The manipulation of the argument new_item 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-250441 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0423	A vulnerability was found in CodeAstro Online Food Ordering System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file dishes.php. The manipulation of the argument res_id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250442 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0599	A vulnerability was found in Jspxcms 10.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file src\main\java\com\jspxcms\core\web\back\InfoController.java of the component Document Management Page. The manipulation of the argument title 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-250837 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0424	A vulnerability classified as problematic has been found in CodeAstro Simple Banking System 1.0. This affects an unknown part of the file createuser.php of the component Create a User Page. The manipulation 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-250443.	3.5	More Details
CVE-2023-2030	An issue has been discovered in GitLab CE/EE affecting all versions from 12.2 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which an attacker could potentially modify the metadata of signed commits.	3.5	More Details
CVE-2022-4959	A vulnerability classified as problematic was found in qkmc-rk redbbs 1.0. Affected by this vulnerability is an unknown functionality of the component Nickname Handler. The manipulation 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-250237 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4960	A vulnerability, which was classified as problematic, has been found in cloudfavorites favorites-web 1.3.0. Affected by this issue is some unknown functionality of the component Nickname Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250238 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0504	A vulnerability has been found in code-projects Simple Online Hotel Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file add_reserve.php of the component Make a Reservation Page. The manipulation of the argument Firstname/Lastname 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. VDB-250618 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40394	The issue was addressed with improved validation of environment variables. This issue is fixed in iOS 16.6 and iPadOS 16.6. An app may be able to access sensitive user data.	3.3	More Details
CVE-2023-40383	A path handling issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3. An app may be able to access user-sensitive data.	3.3	More Details
CVE-2022-42839	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. An app may be able to read sensitive location information.	3.3	More Details
CVE-2023-40439	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to read sensitive location information.	3.3	More Details
CVE-2023-42830	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information.	3.3	More Details
CVE-2022-31021	Ursa is a cryptographic library for use with blockchains. A weakness in the Hyperledger AnonCreds specification that is not mitigated in the Ursa and AnonCreds implementations is that the Issuer does not publish a key correctness proof demonstrating that a generated private key is sufficient to meet the unlinkability guarantees of AnonCreds. The Ursa and AnonCreds CL-Signatures implementations always generate a sufficient private key. A malicious issuer could in theory create a custom CL Signature implementation (derived from the Ursa or AnonCreds CL-Signatures implementations) that uses weakened private keys such that presentations from holders could be shared by verifiers to the issuer who could determine the holder to which the credential was issued. This vulnerability could impact holders of AnonCreds credentials implemented using the CL-signature scheme in the Ursa and AnonCreds implementations of CL Signatures. The ursa project has has moved to end-of-life status and no fix is expected.	3.3	More Details
CVE-2023-38612	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.7, iOS 16.7 and iPadOS 16.7, iOS 17 and iPadOS 17, macOS Sonoma 14, macOS Ventura 13.6. An app may be able to access protected user data.	3.3	More Details
CVE-2023-28197	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4. An app may be able to access user-sensitive data.	3.3	More Details
CVE-2023-20573	A privileged attacker can prevent delivery of debug exceptions to SEV-SNP guests potentially resulting in guests not receiving expected debug information.	3.2	More Details
CVE-2023-7048	The My Sticky Bar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.6. This is due to missing or incorrect nonce validation in mystickymenu-contact-leads.php. This makes it possible for unauthenticated attackers to trigger the export of a CSV file containing contact leads via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Because the CSV file is exported to a public location, it can be downloaded during a very short window of time before it is automatically deleted by the export function.	3.1	More Details
CVE-2023-49099	Discourse is a platform for community discussion. Under very specific circumstances, secure upload URLs associated with posts can be accessed by guest users even when login is required. This vulnerability has been patched in 3.2.0.beta4 and 3.1.4.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49619	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Answer. This issue affects Apache Answer: through 1.2.0. Under normal circumstances, a user can only bookmark a question once, and will only increase the number of questions bookmarked once. However, repeat submissions through the script can increase the number of collection of the question many times. Users are recommended to upgrade to version [1.2.1], which fixes the issue.	3.1	More Details
CVE-2024-20910	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. While the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.0	More Details
CVE-2024-20912	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Easily exploitable vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2024-20957	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Package Build SEC). Supported versions that are affected are Prior to 9.2.8.1. Easily exploitable vulnerability allows high privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2023-2252	The Directorist WordPress plugin before 7.5.4 is vulnerable to Local File Inclusion as it does not validate the file parameter when importing CSV files.	2.7	More Details
CVE-2024-20922	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2.5	More Details
CVE-2024-0500	A vulnerability, which was classified as problematic, was found in SourceCodester House Rental Management System 1.0. Affected is an unknown function of the component Manage Tenant Details. 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-250608.	2.4	More Details
CVE-2024-0230	A session management issue was addressed with improved checks. This issue is fixed in Magic Keyboard Firmware Update 2.0.6. An attacker with physical access to the accessory may be able to extract its Bluetooth pairing key and monitor Bluetooth traffic.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0501	A vulnerability has been found in SourceCodester House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Manage Invoice Details. The manipulation of the argument Invoice 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-250609 was assigned to this vulnerability.	2.4	More Details
CVE-2023-40529	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 17 and iPadOS 17. A person with physical access to a device may be able to use VoiceOver to access private calendar information.	2.4	More Details
CVE-2024-0557	A vulnerability, which was classified as problematic, was found in DedeBIZ 6.3.0. This affects an unknown part of the component Website Copyright Setting. The manipulation 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 identifier VDB-250725 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-0499	A vulnerability, which was classified as problematic, has been found in SourceCodester House Rental Management System 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument page 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-250607.	2.4	More Details
CVE-2024-0476	A vulnerability, which was classified as problematic, was found in Blood Bank & Donor Management 1.0. This affects an unknown part of the file request-received-bydonar.php. The manipulation 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 identifier VDB-250581 was assigned to this vulnerability.	2.4	More Details
CVE-2024-20914	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.3	More Details
CVE-2023-37521	HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower can sometimes include sensitive information in a query string which could allow an attacker to execute a malicious attack.	2.3	More Details
CVE-2024-22194	cdo-local-uuid project provides a specialized UUID-generating function that can, on user request, cause a program to generate deterministic UUIDs. An information leakage vulnerability is present in `cdo-local-uuid` at version `0.4.0`, and in `case-utils` in unpatched versions (matching the pattern `0.x.0`) at and since `0.5.0`, before `0.15.0`. The vulnerability stems from a Python function, `cdo_local_uuid.local_uuid()`, and its original implementation `case_utils.local_uuid()`.	2.2	More Details
CVE-2023-22514	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2023-22525	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2023-51195	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 Number	Description	Base Score	Reference
CVE-2023-22512	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2023-22510	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2024-0227	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-51381	Rejected reason: This CVE ID has been rejected or withdrawn by GitHub.	N/A	More Details
CVE-2024-0584	Rejected reason: Do not use this CVE as it is duplicate of CVE-2023-6932	N/A	More Details
CVE-2024-0395	Rejected reason: NON Security Issue.	N/A	More Details
CVE-2023-22507	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2024-0393	Rejected reason: This CVE ID was unused by the CNA.	N/A	More Details
CVE-2023-22502	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2023-22520	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details