SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 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-2023-51468	Unrestricted Upload of File with Dangerous Type vulnerability in Jacques Malgrange Rencontre – Dating Site.This issue affects Rencontre – Dating Site: from n/a through 3.10.1.	10.0	More Details
CVE-2023-25054	Improper Control of Generation of Code ('Code Injection') vulnerability in David F. Carr RSVPMaker.This issue affects RSVPMaker: from n/a through 10.6.6.	10.0	More Details
CVE-2023-6339	Google Nest WiFi Pro root code-execution & user-data compromise	10.0	More Details
CVE-2023-48419	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege	10.0	More Details
CVE-2023-52181	Deserialization of Untrusted Data vulnerability in Presslabs Theme per user.This issue affects Theme per user: from n/a through 1.0.1.	10.0	More Details
CVE-2023-51475	Unrestricted Upload of File with Dangerous Type vulnerability in IOSS WP MLM SOFTWARE PLUGIN.This issue affects WP MLM SOFTWARE PLUGIN: from n/a through 4.0.	10.0	More Details
CVE-2023-51473	Unrestricted Upload of File with Dangerous Type vulnerability in Pixelemu TerraClassifieds – Simple Classifieds Plugin.This issue affects TerraClassifieds – Simple Classifieds Plugin: from n/a through 2.0.3.	10.0	More Details
CVE-2023-51419	Unrestricted Upload of File with Dangerous Type vulnerability in Bertha.Ai BERTHA AI. Your AI co-pilot for WordPress and Chrome.This issue affects BERTHA AI. Your AI co-pilot for WordPress and Chrome: from n/a through 1.11.10.7.	10.0	More Details
CVE-2023-51411	Unrestricted Upload of File with Dangerous Type vulnerability in Shabti Kaplan Frontend Admin by DynamiApps.This issue affects Frontend Admin by DynamiApps: from n/a through 3.18.3.	10.0	More Details
CVE-2023-51505	Deserialization of Untrusted Data vulnerability in realmag777 Active Products Tables for WooCommerce. Professional products tables for WooCommerce store.This issue affects Active Products Tables for WooCommerce. Professional products tables for WooCommerce store : from n/a through 1.0.6.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48418	In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation	10.0	More Details
CVE-2023-7163	A security issue exists in D-Link D-View 8 v2.0.2.89 and prior that could allow an attacker to manipulate the probe inventory of the D-View service. This could result in the disclosure of information from other probes, denial of service conditions due to the probe inventory becoming full, or the execution of tasks on other probes.	10.0	More Details
CVE-2023-51421	Unrestricted Upload of File with Dangerous Type vulnerability in Soft8Soft LLC Verge3D Publishing and E-Commerce.This issue affects Verge3D Publishing and E-Commerce: from n/a through 4.5.2.	9.9	More Details
CVE-2023-46623	Improper Control of Generation of Code ('Code Injection') vulnerability in TienCOP WP EXtra.This issue affects WP EXtra: from n/a through 6.2.	9.9	More Details
CVE-2023-51470	Deserialization of Untrusted Data vulnerability in Jacques Malgrange Rencontre – Dating Site.This issue affects Rencontre – Dating Site: from n/a through 3.11.1.	9.9	More Details
CVE-2023-51422	Deserialization of Untrusted Data vulnerability in Saleswonder Team Webinar Plugin: Create live/evergreen/automated/instant webinars, stream & Zoom Meetings	WebinarIgnition.This issue affects Webinar Plugin: Create live/evergreen/automated/instant webinars, stream & Zoom Meetings	WebinarIgnition: from n/a through 3.05.0.	9.9	More Details
CVE-2023-49830	Improper Control of Generation of Code ('Code Injection') vulnerability in Brainstorm Force Astra Pro.This issue affects Astra Pro: from n/a through 4.3.1.	9.9	More Details
CVE-2023-47840	Improper Control of Generation of Code ('Code Injection') vulnerability in Qode Interactive Qode Essential Addons.This issue affects Qode Essential Addons: from n/a through 1.5.2.	9.9	More Details
CVE-2023-51417	Unrestricted Upload of File with Dangerous Type vulnerability in Joris van Montfort JVM Gutenberg Rich Text Icons.This issue affects JVM Gutenberg Rich Text Icons: from n/a through 1.2.3.	9.9	More Details
CVE-2023-32095	Improper Control of Generation of Code ('Code Injection') vulnerability in Milan Dinić Rename Media Files.This issue affects Rename Media Files: from n/a through 1.0.1.	9.9	More Details
CVE-2023-52182	Deserialization of Untrusted Data vulnerability in ARI Soft ARI Stream Quiz – WordPress Quizzes Builder.This issue affects ARI Stream Quiz – WordPress Quizzes Builder: from n/a through 1.3.0.	9.9	More Details
CVE-2023-51410	Unrestricted Upload of File with Dangerous Type vulnerability in WPVibes WP Mail Log.This issue affects WP Mail Log: from n/a through 1.1.2.	9.9	More Details
CVE-2023-41543	SQL injection vulnerability in jeecg-boot v3.5.3, allows remote attackers to escalate privileges and obtain sensitive information via the component /sys/replicate/check.	9.8	More Details
CVE-2023-50578	Mingsoft MCMS v5.2.9 was discovered to contain a SQL injection vulnerability via the categoryType parameter at /content/list.do.	9.8	More Details
CVE-2023-41542	SQL injection vulnerability in jeecg-boot version 3.5.3, allows remote attackers to escalate privileges and obtain sensitive information via the jmreport/qurestSql component.	9.8	More Details
CVE-2023-50035	PHPGurukul Small CRM 3.0 is vulnerable to SQL Injection on the Users login panel because of "password" parameter is directly used in the SQL query without any sanitization and the SQL Injection payload being executed.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41544	SSTI injection vulnerability in jeecg-boot version 3.5.3, allows remote attackers to execute arbitrary code via crafted HTTP request to the /jmreport/loadTableData component.	9.8	More Details
CVE-2023-52252	Unified Remote 3.13.0 allows remote attackers to execute arbitrary Lua code because of a wildcarded Access-Control-Allow-Origin for the Remote upload endpoint.	9.8	More Details
CVE-2023-50104	ZZCMS 2023 has a file upload vulnerability in 3/E_bak5.1/upload/index.php, allowing attackers to exploit this loophole to gain server privileges and execute arbitrary code.	9.8	More Details
CVE-2023-51135	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formPasswordSetup.	9.8	More Details
CVE-2023-51133	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formRoute.	9.8	More Details
CVE-2023-4674	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yaztek Software Technologies and Computer Systems E-Commerce Software allows SQL Injection.This issue affects E-Commerce Software: through 20231229. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-51136	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formRebootSchedule.	9.8	More Details
CVE-2023-50589	Grupo Embras GEOSIAP ERP v2.2.167.02 was discovered to contain a SQL injection vulnerability via the codLogin parameter on the login page.	9.8	More Details
CVE-2023-50651	TOTOLINK X6000R v9.4.0cu.852_B20230719 was discovered to contain a remote command execution (RCE) vulnerability via the component /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2023-52262	outdoorbits little-backup-box (aka Little Backup Box) before f39f91c allows remote attackers to execute arbitrary code because the PHP extract function is used for untrusted input.	9.8	More Details
CVE-2023-47883	The com.altamirano.fabricio.tvbrowser TV browser application through 4.5.1 for Android is vulnerable to JavaScript code execution via an explicit intent due to an exposed MainActivity.	9.8	More Details
CVE-2023-33025	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.	9.8	More Details
CVE-2023-4675	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GM Information Technologies MDO allows SQL Injection.This issue affects MDO: through 20231229. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-6190	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in İzmir Katip Çelebi University University Information Management System allows Absolute Path Traversal.This issue affects University Information Management System: before 30.11.2023.	9.8	More Details
CVE-2023-4541	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ween Software Admin Panel allows SQL Injection.This issue affects Admin Panel: through 20231229. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-51084	hyavijava v6.0.07.1 was discovered to contain a stack overflow via the ResultConverter.convert2Xml method.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43481	An issue in Shenzhen TCL Browser TV Web BrowseHere (aka com.tcl.browser) 6.65.022_dab24cc6_231221_gp allows a remote attacker to execute arbitrary JavaScript code via the com.tcl.browser.portal.browse.activity.BrowsePageActivity component.	9.8	More Details
CVE-2023-52173	XnView Classic before 2.51.3 on Windows has a Write Access Violation at xnview.exe+0x3ADBD0.	9.8	More Details
CVE-2023-52174	XnView Classic before 2.51.3 on Windows has a Write Access Violation at xnview.exe+0x3125D6.	9.8	More Details
CVE-2023-23634	SQL Injection vulnerability in Documize version 5.4.2, allows remote attackers to execute arbitrary code via the user parameter of the /api/dashboard/activity endpoint.	9.8	More Details
CVE-2024-21623	OTCLient is an alternative tibia client for otserv. Prior to commit db560de0b56476c87a2f967466407939196dd254, the /mehah/otclient "`Analysis - SonarCloud`" workflow is vulnerable to an expression injection in Actions, allowing an attacker to run commands remotely on the runner, leak secrets, and alter the repository using this workflow. Commit db560de0b56476c87a2f967466407939196dd254 contains a fix for this issue.	9.8	More Details
CVE-2023-47458	An issue in SpringBlade v.3.7.0 and before allows a remote attacker to escalate privileges via the lack of permissions control framework.	9.8	More Details
CVE-2023-43955	The com.phlox.tvwebbrowser TV Bro application through 2.0.0 for Android mishandles external intents through WebView. This allows attackers to execute arbitrary code, create arbitrary files. and perform arbitrary downloads via JavaScript that uses takeBlobDownloadData.	9.8	More Details
CVE-2023-32874	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893).	9.8	More Details
CVE-2023-4671	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Talent Software ECOP allows Command Line Execution through SQL Injection.This issue affects ECOP: before 32255.	9.8	More Details
CVE-2023-6436	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ekol Informatics Website Template allows SQL Injection.This issue affects Website Template: through 20231215.	9.8	More Details
CVE-2023-49001	An issue in Indi Browser (aka kvbrowser) v.12.11.23 allows an attacker to bypass intended access restrictions via interaction with the com.example.gurry.kvbrowswer.webview component.	9.8	More Details
CVE-2023-5877	The affiliate-toolkit WordPress plugin before 3.4.3 lacks authorization and authentication for requests to it's affiliate-toolkit-starter/tools/atkp_imagereceiver.php endpoint, allowing unauthenticated visitors to make requests to arbitrary URL's, including RFC1918 private addresses, leading to a Server Side Request Forgery (SSRF) issue.	9.8	More Details
CVE-2023-49000	An issue in ArtistScope ArtisBrowser v.34.1.5 and before allows an attacker to bypass intended access restrictions via interaction with the com.artis.browser.IntentReceiverActivity component. NOTE: this is disputed by the vendor, who indicates that ArtisBrowser 34 does not support CSS3.	9.8	More Details
CVE-2023-51545	Cross-Site Request Forgery (CSRF), Deserialization of Untrusted Data vulnerability in ThemeHigh Job Manager & Career – Manage job board listings, and recruitments.This issue affects Job Manager & Career – Manage job board listings, and recruitments: from n/a through 1.4.4.	9.6	More Details
CVE-2023-51414	Deserialization of Untrusted Data vulnerability in EnvialoSimple EnvíaloSimple: Email Marketing y Newsletters.This issue affects EnvíaloSimple: Email Marketing y Newsletters: from n/a through 2.1.	9.6	More Details
CVE-2023-4280	An unvalidated input in Silicon Labs TrustZone implementation in v4.3.x and earlier of the Gecko SDK allows an attacker to access the trusted region of memory from the untrusted region.	9.3	More Details
CVE-2023-33030	Memory corruption in HLOS while running playready use-case.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33032	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	9.3	More Details
CVE-2023-50839	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.8.1.	9.3	More Details
CVE-2023-51469	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mestres do WP Checkout Mestres WP.This issue affects Checkout Mestres WP: from n/a through 7.1.9.6.	9.3	More Details
CVE-2023-51423	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saleswonder Team Webinar Plugin: Create live/evergreen/automated/instant webinars, stream & Zoom Meetings	WebinarIgnition.This issue affects Webinar Plugin: Create live/evergreen/automated/instant webinars, stream & Zoom Meetings	WebinarIgnition: from n/a through 3.05.0.	9.3	More Details
CVE-2023-50255	Deepin-Compressor is the default archive manager of Deepin Linux OS. Prior to 5.12.21, there's a path traversal vulnerability in deepin-compressor that can be exploited to achieve Remote Command Execution on the target system upon opening crafted archives. Users are advised to update to version 5.12.21 which addresses the issue. There are no known workarounds for this vulnerability.	9.3	More Details
CVE-2023-51434	Some Honor products are affected by buffer overflow vulnerability, successful exploitation could cause code execution.	9.3	More Details
CVE-2023-49777	Deserialization of Untrusted Data vulnerability in YITH YITH WooCommerce Product Add-Ons.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.3.0.	9.1	More Details
CVE-2023-51420	Improper Control of Generation of Code ('Code Injection') vulnerability in Soft8Soft LLC Verge3D Publishing and E-Commerce.This issue affects Verge3D Publishing and E-Commerce: from n/a through 4.5.2.	9.1	More Details
CVE-2023-45751	Improper Control of Generation of Code ('Code Injection') vulnerability in POSIMYTH Nexter Extension.This issue affects Nexter Extension: from n/a through 2.0.3.	9.1	More Details
CVE-2023-40606	Improper Control of Generation of Code ('Code Injection') vulnerability in Kanban for WordPress Kanban Boards for WordPress.This issue affects Kanban Boards for WordPress: from n/a through 2.5.21.	9.1	More Details
CVE-2023-39157	Improper Control of Generation of Code ('Code Injection') vulnerability in Crocoblock JetElements For Elementor.This issue affects JetElements For Elementor: from n/a through 2.6.10.	9.0	More Details
CVE-2023-51412	Unrestricted Upload of File with Dangerous Type vulnerability in Piotnet Piotnet Forms.This issue affects Piotnet Forms: from n/a through 1.0.25.	9.0	More Details
CVE-2023-6879	Increasing the resolution of video frames, while performing a multi-threaded encode, can result in a heap overflow in av1_loop_restoration_dealloc().	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52139	Misskey is an open source, decentralized social media platform. Third-party applications may be able to access some endpoints or Websocket APIs that are incorrectly specified as [kind](https://github.com/misskey-dev/misskey/blob/406b4bdbe79b5b0b68fcdcb3c4b6e419460a0258/packages/backend/src/server/api/endpoints.ts#L811) or [secure](https://github.com/misskey-dev/misskey/blob/406b4bdbe79b5b0b68fcdcb3c4b6e419460a0258/packages/backend/src/server/api/endpoints.ts#L805) without the user's permission and perform operations such as reading or adding non-public content. As a result, if the user who authenticated the application is an administrator, confidential information such as object storage secret keys and SMTP server passwords will be leaked, and general users can also create invitation codes without permission and leak non-public user information. This is patched in version [2023.12.1](https://github.com/misskey-dev/misskey/commit/c96bc36fedc804dc840ea791a9355d7df0748e64).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-52077	Nexkey is a lightweight fork of Misskey v12 optimized for small to medium size servers. Prior to 12.23Q4.5, Nexkey allows external apps using tokens issued by administrators and moderators to call admin APIs. This allows malicious third-party apps to perform operations such as updating server settings, as well as compromise object storage and email server credentials. This issue has been patched in 12.23Q4.5.	8.9	More Details
CVE-2023-46987	SeaCMS v12.9 was discovered to contain a remote code execution (RCE) vulnerability via the component /augap/adminip.php.	8.8	More Details
CVE-2023-40038	Arris DG860A and DG1670A devices have predictable default WPA2 PSKs that could lead to unauthorized remote access. (They use the first 6 characters of the SSID and the last 6 characters of the BSSID, decrementing the last digit.)	8.8	More Details
CVE-2023-50038	There is an arbitrary file upload vulnerability in the background of textpattern cms v4.8.8, which leads to the loss of server permissions.	8.8	More Details
CVE-2023-49230	An issue was discovered in Peplink Balance Two before 8.4.0. A missing authorization check in captive portals allows attackers to modify the portals' configurations without prior authentication.	8.8	More Details
CVE-2023-50071	Sourcecodester Customer Support System 1.0 has multiple SQL injection vulnerabilities in /customer_support/ajax.php?action=save_department via id or name.	8.8	More Details
CVE-2023-47804	Apache OpenOffice documents can contain links that call internal macros with arbitrary arguments. Several URI Schemes are defined for this purpose. Links can be activated by clicks, or by automatic document events. The execution of such links must be subject to user approval. In the affected versions of OpenOffice, approval for certain links is not requested; when activated, such links could therefore result in arbitrary script execution. This is a corner case of CVE-2022-47502.	8.8	More Details
CVE-2023-49299	Improper Input Validation vulnerability in Apache DolphinScheduler. An authenticated user can cause arbitrary, unsandboxed javascript to be executed on the server.This issue affects Apache DolphinScheduler: until 3.1.9. Users are recommended to upgrade to version 3.1.9, which fixes the issue.	8.8	More Details
CVE-2023-50692	File Upload vulnerability in JIZHICMS v.2.5, allows remote attacker to execute arbitrary code via a crafted file uploaded and downloaded to the download_url parameter in the app/admin/exts/ directory.	8.8	More Details
CVE-2023-52082	Lychee is a free photo-management tool. Prior to 5.0.2, Lychee is vulnerable to an SQL injection on any binding when using mysql/mariadb. This injection is only active for users with the `.env` settings set to DB_LOG_SQL=true and DB_LOG_SQL_EXPLAIN=true. The defaults settings of Lychee are safe. The patch is provided on version 5.0.2. To work around this issue, disable SQL EXPLAIN logging.	8.8	More Details
CVE-2023-50070	Sourcecodester Customer Support System 1.0 has multiple SQL injection vulnerabilities in /customer_support/ajax.php?action=save_ticket via department_id, customer_id, and subject.	8.8	More Details
CVE-2023-50094	reNgine before 2.1.2 allows OS Command Injection if an adversary has a valid session ID. The attack places shell metacharacters in an api/tools/waf_detector/?url= string. The commands are executed as root via subprocess.check_output.	8.8	More Details
CVE-2024-21632	omniauth-microsoft_graph provides an Omniauth strategy for the Microsoft Graph API. Prior to versions 2.0.0, the implementation did not validate the legitimacy of the `email` attribute of the user nor did it give/document an option to do so, making it susceptible to nOAuth misconfiguration in cases when the `email` is used as a trusted user identifier. This could lead to account takeover. Version 2.0.0 contains a fix for this issue.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50842	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Matthew Fries MF Gig Calendar.This issue affects MF Gig Calendar: from n/a through 1.2.1.	8.5	More Details
CVE-2023-50841	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Repute Infosystems BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin.This issue affects BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin: from n/a through 1.0.72.	8.5	More Details
CVE-2023-7080	The V8 inspector intentionally allows arbitrary code execution within the Workers sandbox for debugging. wrangler dev would previously start an inspector server listening on all network interfaces. This would allow an attacker on the local network to connect to the inspector and run arbitrary code. Additionally, the inspector server did not validate Origin/Host headers, granting an attacker that can trick any user on the local network into opening a malicious website the ability to run code. If wrangler dev --remote was being used, an attacker could access production resources if they were bound to the worker. This issue was fixed in wrangler@3.19.0 and wrangler@2.20.2. Whilst wrangler dev's inspector server listens on local interfaces by default as of wrangler@3.16.0, an SSRF vulnerability in miniflare https://github.com/cloudflare/workers-sdk/security/advisories/GHSA-fwvg-2739-22v7 (CVE-2023-7078) allowed access from the local network until wrangler@3.18.0. wrangler@3.19.0 and wrangler@2.20.2 introduced validation for the Origin/Host headers.	8.5	More Details
CVE-2023-52133	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WhileTrue Most And Least Read Posts Widget.This issue affects Most And Least Read Posts Widget: from n/a through 2.5.16.	8.5	More Details
CVE-2023-50840	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdevelop, oplugins Booking Manager.This issue affects Booking Manager: from n/a through 2.1.5.	8.5	More Details
CVE-2023-22677	Improper Control of Generation of Code ('Code Injection') vulnerability in BinaryStash WP Booklet.This issue affects WP Booklet: from n/a through 2.1.8.	8.5	More Details
CVE-2023-33114	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	8.4	More Details
CVE-2023-33108	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued.	8.4	More Details
CVE-2023-33094	Memory corruption while running VK synchronization with KASAN enabled.	8.4	More Details
CVE-2023-33113	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	8.4	More Details
CVE-2023-4164	There is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of health data with no additional execution privileges needed.	8.4	More Details
CVE-2023-43514	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	8.4	More Details
CVE-2023-33033	Memory corruption in Audio during playback with speaker protection.	8.4	More Details
CVE-2023-32795	Deserialization of Untrusted Data vulnerability in WooCommerce Product Add-Ons.This issue affects Product Add-Ons: from n/a through 6.1.3.	8.2	More Details
CVE-2022-44589	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in miniOrange miniOrange's Google Authenticator – WordPress Two Factor Authentication – 2FA , Two Factor, OTP SMS and Email	Passwordless login.This issue affects miniOrange's Google Authenticator – WordPress Two Factor Authentication – 2FA , Two Factor, OTP SMS and Email	Passwordless login: from n/a through 5.6.1.	8.1	More Details
CVE-2024-21627	PrestaShop is an open-source e-commerce platform. Prior to versions 8.1.3 and 1.7.8.11, some event attributes are not detected by the `isCleanHTML` method. Some modules using the `isCleanHTML` method could be vulnerable to cross-site scripting. Versions 8.1.3 and 1.7.8.11 contain a patch for this issue. The best workaround is to use the `HTMLPurifier` library to sanitize html input coming from users. The library is already available as a dependency in the PrestaShop project. Beware though that in legacy object models, fields of `HTML` type will call `isCleanHTML`.	8.1	More Details
CVE-2023-33085	Memory corruption in wearables while processing data from AON.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52277	Royal RoyalTSX before 6.0.2.1 allows attackers to cause a denial of service (Heap Memory Corruption and application crash) or possibly have unspecified other impact via a long hostname in an RTSZ file, if the victim clicks on Test Connection. This occurs during SecureGatewayHost object processing in RAPortCheck.createNWConnection.	7.8	More Details
CVE-2022-46487	Improper initialization of x87 and SSE floating-point configuration registers in the __scone_entry component of SCONE before 5.8.0 for Intel SGX allows a local attacker to compromise the execution integrity of floating-point operations in an enclave or access sensitive information via side-channel analysis.	7.8	More Details
CVE-2023-33110	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	7.8	More Details
CVE-2023-46989	SQL Injection vulnerability in the Innovadeluxe Quick Order module for PrestaShop before v.1.4.0, allows local attackers to execute arbitrary code via the getProducts() function in the productlist.php file.	7.8	More Details
CVE-2023-50445	Shell Injection vulnerability GL.iNet A1300 v4.4.6, AX1800 v4.4.6, AXT1800 v4.4.6, MT3000 v4.4.6, MT2500 v4.4.6, MT6000 v4.5.0, MT1300 v4.3.7, MT300N-V2 v4.3.7, AR750S v4.3.7, AR750 v4.3.7, AR300M v4.3.7, and B1300 v4.3.7., allows local attackers to execute arbitrary code via the get_system_log and get_crash_log functions of the logread module, as well as the upgrade_online function of the upgrade module.	7.8	More Details
CVE-2024-0193	A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-collected when the pipapo set is removed, the element can be deactivated twice. This can cause a use-after-free issue on an NFT_CHAIN object or NFT_OBJECT object, allowing a local unprivileged user with CAP_NET_ADMIN capability to escalate their privileges on the system.	7.8	More Details
CVE-2020-17163	Visual Studio Code Python Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-33117	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	7.8	More Details
CVE-2023-33118	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	7.8	More Details
CVE-2023-33120	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	7.8	More Details
CVE-2023-50571	easy-rules-mvel v4.1.0 was discovered to contain a remote code execution (RCE) vulnerability via the component MVELRule.	7.8	More Details
CVE-2023-47039	A vulnerability was found in Perl. This security issue occurs while Perl for Windows relies on the system path environment variable to find the shell (`cmd.exe`). When running an executable that uses the Windows Perl interpreter, Perl attempts to find and execute `cmd.exe` within the operating system. However, due to path search order issues, Perl initially looks for cmd.exe in the current working directory. This flaw allows an attacker with limited privileges to place`cmd.exe` in locations with weak permissions, such as `C:\ProgramData`. By doing so, arbitrary code can be executed when an administrator attempts to use this executable from these compromised locations.	7.8	More Details
CVE-2023-6998	Improper privilege management vulnerability in CoolKit Technology eWeLink on Android and iOS allows application lockscreen bypass.This issue affects eWeLink before 5.2.0.	7.7	More Details
CVE-2023-52137	The [`tj-actions/verify-changed-files`](https://github.com/tj-actions/verify-changed-files) action allows for command injection in changed filenames, allowing an attacker to execute arbitrary code and potentially leak secrets. The [`verify-changed-files`](https://github.com/tj-actions/verify-changed-files) workflow returns the list of files changed within a workflow execution. This could potentially allow filenames that contain special characters such as `;` which can be used by an attacker to take over the [GitHub Runner](https://docs.github.com/en/actions/using-github-hosted-runners/about-github-hosted-runners) if the output value is used in a raw fashion (thus being directly replaced before execution) inside a `run` block. By running custom commands, an attacker may be able to steal secrets such as `GITHUB_TOKEN` if triggered on other events than `pull_request`. This has been patched in versions [17](https://github.com/tj-actions/verify-changed-files/releases/tag/v17) and [17.0.0](https://github.com/tj-actions/verify-changed-files/releases/tag/v17.0.0) by enabling `safe_output` by default and returning filename paths escaping special characters for bash environments.	7.7	More Details
CVE-2023-52131	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Zinc Page Generator.This issue affects Page Generator: from n/a through 1.7.1.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52132	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jewel Theme WP Adminify.This issue affects WP Adminify: from n/a through 3.1.6.	7.6	More Details
CVE-2023-52134	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eyal Fitoussi GEO my WordPress.This issue affects GEO my WordPress: from n/a through 4.0.2.	7.6	More Details
CVE-2023-50855	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sam Perrow Pre* Party Resource Hints.This issue affects Pre* Party Resource Hints: from n/a through 1.8.18.	7.6	More Details
CVE-2023-50843	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Clockwork Clockwork SMS Notfications.This issue affects Clockwork SMS Notfications: from n/a through 3.0.4.	7.6	More Details
CVE-2023-50838	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Basix NEX-Forms – Ultimate Form Builder – Contact forms and much more.This issue affects NEX-Forms – Ultimate Form Builder – Contact forms and much more: from n/a through 8.5.5.	7.6	More Details
CVE-2023-52180	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Really Simple Plugins Recipe Maker For Your Food Blog from Zip Recipes.This issue affects Recipe Maker For Your Food Blog from Zip Recipes: from n/a through 8.1.0.	7.6	More Details
CVE-2023-50844	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in James Ward Mail logging – WP Mail Catcher.This issue affects Mail logging – WP Mail Catcher: from n/a through 2.1.3.	7.6	More Details
CVE-2023-50845	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AyeCode - WordPress Business Directory Plugins GeoDirectory – WordPress Business Directory Plugin, or Classified Directory.This issue affects GeoDirectory – WordPress Business Directory Plugin, or Classified Directory: from n/a through 2.3.28.	7.6	More Details
CVE-2023-51547	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPManageNinja LLC Fluent Support – WordPress Helpdesk and Customer Support Ticket Plugin.This issue affects Fluent Support – WordPress Helpdesk and Customer Support Ticket Plugin: from n/a through 1.7.6.	7.6	More Details
CVE-2023-50852	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Booking Calendar	Appointment Booking	BookIt.This issue affects Booking Calendar	Appointment Booking	BookIt: from n/a through 2.4.3.	7.6	More Details
CVE-2023-50854	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Squirrly Squirrly SEO - Advanced Pack.This issue affects Squirrly SEO - Advanced Pack: from n/a through 2.3.8.	7.6	More Details
CVE-2023-50857	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FunnelKit Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit.This issue affects Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit: from n/a through 2.6.1.	7.6	More Details
CVE-2023-52135	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WS Form WS Form LITE – Drag & Drop Contact Form Builder for WordPress.This issue affects WS Form LITE – Drag & Drop Contact Form Builder for WordPress: from n/a through 1.9.170.	7.6	More Details
CVE-2023-50837	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WebFactory Ltd Login Lockdown – Protect Login Form.This issue affects Login Lockdown – Protect Login Form: from n/a through 2.06.	7.6	More Details
CVE-2023-50847	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Collne Inc. Welcart e-Commerce.This issue affects Welcart e-Commerce: from n/a through 2.9.3.	7.6	More Details
CVE-2023-33014	Information disclosure in Core services while processing a Diag command.	7.6	More Details
CVE-2023-50856	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FunnelKit Funnel Builder for WordPress by FunnelKit – Customize WooCommerce Checkout Pages, Create Sales Funnels & Maximize Profits.This issue affects Funnel Builder for WordPress by FunnelKit – Customize WooCommerce Checkout Pages, Create Sales Funnels & Maximize Profits: from n/a through 2.14.3.	7.6	More Details
CVE-2023-50846	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RegistrationMagic RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login.This issue affects RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login: from n/a through 5.2.4.5.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50848	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aaron J 404 Solution.This issue affects 404 Solution: from n/a through 2.34.0.	7.6	More Details
CVE-2023-50849	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in E2Pdf.Com E2Pdf – Export To Pdf Tool for WordPress.This issue affects E2Pdf – Export To Pdf Tool for WordPress: from n/a through 1.20.23.	7.6	More Details
CVE-2023-50851	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in N Squared Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin.This issue affects Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin: from n/a before 1.6.6.1.	7.6	More Details
CVE-2023-50853	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nasirahmed Advanced Form Integration – Connect WooCommerce and Contact Form 7 to Google Sheets and other platforms.This issue affects Advanced Form Integration – Connect WooCommerce and Contact Form 7 to Google Sheets and other platforms: from n/a through 1.75.0.	7.6	More Details
CVE-2023-52267	ehttp 1.0.6 before 17405b9 has a simple_log.cpp _log out-of-bounds-read during error logging for long strings.	7.5	More Details
CVE-2023-52266	ehttp 1.0.6 before 17405b9 has an epoll_socket.cpp read_func use-after-free. An attacker can make many connections over a short time to trigger this.	7.5	More Details
CVE-2021-46900	Sympa before 6.2.62 relies on a cookie parameter for certain security objectives, but does not ensure that this parameter exists and has an unpredictable value. Specifically, the cookie parameter is both a salt for stored passwords and an XSS protection mechanism.	7.5	More Details
CVE-2023-52286	Tencent tdsqlpcloud through 1.8.5 allows unauthenticated remote attackers to discover database credentials via an index.php/api/install/get_db_info request, a related issue to CVE-2023-42387.	7.5	More Details
CVE-2021-46901	examples/6lbr/apps/6lbr-webserver/httpd.c in CETIC-6LBR (aka 6lbr) 1.5.0 has a strcat stack-based buffer overflow via a request for a long URL over a 6LoWPAN network.	7.5	More Details
CVE-2023-7078	Sending specially crafted HTTP requests to Miniflare's server could result in arbitrary HTTP and WebSocket requests being sent from the server. If Miniflare was configured to listen on external network interfaces (as was the default in wrangler until 3.19.0), an attacker on the local network could access other local servers.	7.5	More Details
CVE-2023-41815	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). Malicious code could be executed in the File Manager section. This issue affects Pandora FMS: from 700 through 774.	7.5	More Details
CVE-2023-31300	An issue was discovered in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows remote attackers to obtain sensitive information via transmission of unencrypted, cleartext credentials during Password Reset feature.	7.5	More Details
CVE-2023-50110	TestLink through 1.9.20 allows type juggling for authentication bypass because === is not used.	7.5	More Details
CVE-2023-3171	A flaw was found in EAP-7 during deserialization of certain classes, which permits instantiation of HashMap and HashTable with no checks on resources consumed. This issue could allow an attacker to submit malicious requests using these classes, which could eventually exhaust the heap and result in a Denial of Service.	7.5	More Details
CVE-2023-6064	The PayHere Payment Gateway WordPress plugin before 2.2.12 automatically creates publicly-accessible log files containing sensitive information when transactions occur.	7.5	More Details
CVE-2023-33112	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	7.5	More Details
CVE-2023-49552	An Out of Bounds Write in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_op_json_stringify function in the msj.c file.	7.5	More Details
CVE-2023-49551	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_op_json_parse function in the msj.c file.	7.5	More Details
CVE-2023-49550	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs+0x4ec508 component.	7.5	More Details
CVE-2023-49549	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_getretvalpos function in the msj.c file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50020	An issue was discovered in open5gs v2.6.6. SIGPIPE can be used to crash AMF.	7.5	More Details
CVE-2023-45893	An indirect Object Reference (IDOR) in the Order and Invoice pages in Floorsight Customer Portal Q3 2023 allows an unauthenticated remote attacker to view sensitive customer information.	7.5	More Details
CVE-2023-45892	An issue discovered in the Order and Invoice pages in Floorsight Insights Q3 2023 allows an unauthenticated remote attacker to view sensitive customer information.	7.5	More Details
CVE-2022-3010	The Priva TopControl Suite contains predictable credentials for the SSH service, based on the Serial number. Which makes it possible for an attacker to calculate the login credentials for the Priva TopControll suite.	7.5	More Details
CVE-2023-43512	Transient DOS while parsing GATT service data when the total amount of memory that is required by the multiple services is greater than the actual size of the services buffer.	7.5	More Details
CVE-2023-43511	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	7.5	More Details
CVE-2023-33116	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	7.5	More Details
CVE-2023-33109	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	7.5	More Details
CVE-2023-6113	The WP STAGING WordPress Backup Plugin before 3.1.3 and WP STAGING Pro WordPress Backup Plugin before 5.1.3 do not prevent visitors from leaking key information about ongoing backups processes, allowing unauthenticated attackers to download said backups later.	7.5	More Details
CVE-2023-33062	Transient DOS in WLAN Firmware while parsing a BTM request.	7.5	More Details
CVE-2023-33040	Transient DOS in Data Modem during DTLS handshake.	7.5	More Details
CVE-2023-32890	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963).	7.5	More Details
CVE-2023-32889	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895).	7.5	More Details
CVE-2023-32888	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894).	7.5	More Details
CVE-2023-32887	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892).	7.5	More Details
CVE-2023-32886	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807.	7.5	More Details
CVE-2023-31294	CSV Injection vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows remote attackers to obtain sensitive information via the Delivery Name field.	7.5	More Details
CVE-2023-50096	STMicroelectronics STSAFE-A1xx middleware before 3.3.7 allows MCU code execution if an adversary has the ability to read from and write to the I2C bus. This is caused by an StSafeA_ReceiveBytes buffer overflow in the X-CUBE-SAFEA1 Software Package for STSAFE-A sample applications (1.2.0), and thus can affect user-written code that was derived from a published sample application.	7.5	More Details
CVE-2023-6421	The Download Manager WordPress plugin before 3.2.83 does not protect file download's passwords, leaking it upon receiving an invalid one.	7.5	More Details
CVE-2023-6271	The Backup Migration WordPress plugin before 1.3.6 stores in-progress backups information in easy to find, publicly-accessible files, which may allow attackers monitoring those to leak sensitive information from the site's backups.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31295	CSV Injection vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows remote attackers to obtain sensitive information via the User Profile field.	7.5	More Details
CVE-2023-49553	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_destroy function in the msj.c file.	7.5	More Details
CVE-2023-51006	An issue in the openFile method of Chinese Perpetual Calendar v9.0.0 allows attackers to read any file via unspecified vectors.	7.5	More Details
CVE-2023-52075	ReVanced API proxies requests needed to feed the ReVanced Manager and website with data. Up to and including commit 71f81f7f20cd26fd707335bca9838fa3e7df20d2, ReVanced API lacks error caching causing rate limit to be triggered thus increasing server load. This causes a denial of service for all users using the API. It is recommended to implement proper error caching.	7.5	More Details
CVE-2023-51080	The NumberUtil.toBigDecimal method in hutool-core v5.8.23 was discovered to contain a stack overflow.	7.5	More Details
CVE-2023-51075	hutool-core v5.8.23 was discovered to contain an infinite loop in the StrSplitter.splitByRegex function. This vulnerability allows attackers to cause a Denial of Service (DoS) via manipulation of the first two parameters.	7.5	More Details
CVE-2023-52152	mupnp/net/uri.c in mUPnP for C through 3.0.2 has an out-of-bounds read and application crash because it lacks a certain host length recalculation.	7.5	More Details
CVE-2023-49002	An issue in Xenom Technologies (sinous) Phone Dialer-voice Call Dialer v.1.2.5 allows an attacker to bypass intended access restrictions via interaction with com.funprime.calldialer.ui.activities.OutgoingActivity.	7.5	More Details
CVE-2023-51443	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.11, when handling DTLS-SRTP for media setup, FreeSWITCH is susceptible to Denial of Service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack. If an attacker manages to send a ClientHello DTLS message with an invalid CipherSuite (such as `TLS_NULL_WITH_NULL_NULL`) to the port on the FreeSWITCH server that is expecting packets from the caller, a DTLS error is generated. This results in the media session being torn down, which is followed by teardown at signaling (SIP) level too. Abuse of this vulnerability may lead to a massive Denial of Service on vulnerable FreeSWITCH servers for calls that rely on DTLS-SRTP. To address this vulnerability, upgrade FreeSWITCH to 1.10.11 which includes the security fix. The solution implemented is to drop all packets from addresses that have not been validated by an ICE check.	7.5	More Details
CVE-2023-32513	Deserialization of Untrusted Data vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform.This issue affects GiveWP – Donation Plugin and Fundraising Platform: from n/a through 2.25.3.	7.5	More Details
CVE-2023-26159	Versions of the package follow-redirects before 1.15.4 are vulnerable to Improper Input Validation due to the improper handling of URLs by the url.parse() function. When new URL() throws an error, it can be manipulated to misinterpret the hostname. An attacker could exploit this weakness to redirect traffic to a malicious site, potentially leading to information disclosure, phishing attacks, or other security breaches.	7.3	More Details
CVE-2023-23431	Some Honor products are affected by signature management vulnerability, successful exploitation could cause the forged system file overwrite the correct system file.	7.3	More Details
CVE-2023-51664	tj-actions/changed-files is a Github action to retrieve all files and directories. Prior to 41.0.0, the `tj-actions/changed-files` workflow allows for command injection in changed filenames, allowing an attacker to execute arbitrary code and potentially leak secrets. This issue may lead to arbitrary command execution in the GitHub Runner. This vulnerability has been addressed in version 41.0.0. Users are advised to upgrade.	7.3	More Details
CVE-2023-23436	Some Honor products are affected by signature management vulnerability, successful exploitation could cause the forged system file overwrite the correct system file	7.3	More Details
CVE-2023-7156	A vulnerability has been found in Campcodes Online College Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file index.php of the component Search. The manipulation of the argument category leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249178 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-7172	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 component Admin Dashboard. The manipulation 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-249356.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7161	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3.1. This affects an unknown part of the file index.php?para=index of the component Login. The manipulation of the argument check_VirtualSiteId 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-249183.	7.3	More Details
CVE-2024-0182	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/ of the component Admin Login. The manipulation of the argument username/password leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-249440.	7.3	More Details
CVE-2023-23432	Some Honor products are affected by signature management vulnerability, successful exploitation could cause the forged system file overwrite the correct system file.	7.3	More Details
CVE-2023-7158	A vulnerability was found in MicroPython up to 1.21.0. It has been classified as critical. Affected is the function slice_indices of the file objslice.c. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.22.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-249180.	7.3	More Details
CVE-2023-4464	A vulnerability, which was classified as critical, has been found in Poly Trio 8300, Trio 8500, Trio 8800, Trio C60, CCX 350, CCX 400, CCX 500, CCX 505, CCX 600, CCX 700, EDGE E100, EDGE E220, EDGE E300, EDGE E320, EDGE E350, EDGE E400, EDGE E450, EDGE E500, EDGE E550, VVX 101, VVX 150, VVX 201, VVX 250, VVX 300, VVX 301, VVX 310, VVX 311, VVX 350, VVX 400, VVX 401, VVX 410, VVX 411, VVX 450, VVX 500, VVX 501, VVX 600 and VVX 601. This issue affects some unknown processing of the component Diagnostic Telnet Mode. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-249257 was assigned to this vulnerability.	7.2	More Details
CVE-2023-33037	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	7.1	More Details
CVE-2023-50901	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes HT Mega – Absolute Addons For Elementor allows Reflected XSS.This issue affects HT Mega – Absolute Addons For Elementor: from n/a through 2.3.8.	7.1	More Details
CVE-2023-7114	Mattermost version 2.10.0 and earlier fails to sanitize deeplink paths, which allows an attacker to perform CSRF attacks against the server.	7.1	More Details
CVE-2023-51373	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ian Kennerley Google Photos Gallery with Shortcodes allows Reflected XSS.This issue affects Google Photos Gallery with Shortcodes: from n/a through 4.0.2.	7.1	More Details
CVE-2023-50892	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem - Creative Multi-Purpose & WooCommerce WordPress Theme allows Reflected XSS.This issue affects TheGem - Creative Multi-Purpose & WooCommerce WordPress Theme: from n/a through 5.9.1.	7.1	More Details
CVE-2023-33036	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	7.1	More Details
CVE-2023-51435	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause information leak.	7.1	More Details
CVE-2023-50893	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UpSolution Impreza – WordPress Website and WooCommerce Builder allows Reflected XSS.This issue affects Impreza – WordPress Website and WooCommerce Builder: from n/a through 8.17.4.	7.1	More Details
CVE-2023-51501	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Undsgn Uncode - Creative & WooCommerce WordPress Theme allows Reflected XSS.This issue affects Uncode - Creative & WooCommerce WordPress Theme: from n/a through 2.8.6.	7.1	More Details
CVE-2023-47882	The Kami Vision YI IoT com.yunyi.smartcamera application through 4.1.9_20231127 for Android allows a remote attacker to execute arbitrary JavaScript code via an implicit intent to the com.ants360.yicamera.activity.WebViewActivity component.	7.1	More Details
CVE-2023-51431	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause device service exceptions.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52079	msgpackr is a fast MessagePack NodeJS/JavaScript implementation. Prior to 1.10.1, when decoding user supplied MessagePack messages, users can trigger stuck threads by crafting messages that keep the decoder stuck in a loop. The fix is available in v1.10.1. Exploits seem to require structured cloning, replacing the 0x70 extension with your own (that throws an error or does something other than recursive referencing) should mitigate the issue.	6.8	More Details
CVE-2023-32884	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011.	6.7	More Details
CVE-2023-49794	KernelSU is a Kernel-based root solution for Android devices. In versions 0.7.1 and prior, the logic of get apk path in KernelSU kernel module can be bypassed, which causes any malicious apk named `me.weishu.kernelsu` get root permission. If a KernelSU module installed device try to install any not checked apk which package name equal to the official KernelSU Manager, it can take over root privileges on the device. As of time of publication, a patched version is not available.	6.7	More Details
CVE-2023-32872	In keyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607.	6.7	More Details
CVE-2023-32877	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070.	6.7	More Details
CVE-2023-32879	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064.	6.7	More Details
CVE-2023-32882	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616.	6.7	More Details
CVE-2023-33038	Memory corruption while receiving a message in Bus Socket Transport Server.	6.7	More Details
CVE-2023-32885	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685.	6.7	More Details
CVE-2023-32891	In bluetooth service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559.	6.7	More Details
CVE-2023-28583	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	6.7	More Details
CVE-2023-32883	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249.	6.7	More Details
CVE-2023-23426	Some Honor products are affected by file writing vulnerability, successful exploitation could cause information disclosure.	6.6	More Details
CVE-2023-36381	Deserialization of Untrusted Data vulnerability in Gesundheit Bewegt GmbH Zippy.This issue affects Zippy: from n/a through 1.6.5.	6.6	More Details
CVE-2023-51541	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aleksandar Urošević Stock Ticker allows Stored XSS.This issue affects Stock Ticker: from n/a through 3.23.4.	6.5	More Details
CVE-2023-50448	In ActiveAdmin (aka Active Admin) before 2.12.0, a concurrency issue allows a malicious actor to access potentially private data (that belongs to another user) by making CSV export requests at certain specific times.	6.5	More Details
CVE-2023-51399	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Back Button Widget allows Stored XSS.This issue affects Back Button Widget: from n/a through 1.6.3.	6.5	More Details
CVE-2023-50891	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoho Forms Form plugin for WordPress – Zoho Forms allows Stored XSS.This issue affects Form plugin for WordPress – Zoho Forms: from n/a through 3.0.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The Beaver Builder Team Beaver Builder – WordPress Page Builder allows Stored XSS.This issue affects Beaver Builder – WordPress Page Builder: from n/a through 2.7.2.	6.5	More Details
CVE-2023-51397	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force WP Remote Site Search allows Stored XSS.This issue affects WP Remote Site Search: from n/a through 1.0.4.	6.5	More Details
CVE-2023-50881	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AAM Advanced Access Manager – Restricted Content, Users & Roles, Enhanced Security and More allows Stored XSS.This issue affects Advanced Access Manager – Restricted Content, Users & Roles, Enhanced Security and More: from n/a through 6.9.15.	6.5	More Details
CVE-2023-51396	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brizy.Io Brizy – Page Builder allows Stored XSS.This issue affects Brizy – Page Builder: from n/a through 2.4.29.	6.5	More Details
CVE-2023-23424	Some Honor products are affected by file writing vulnerability, successful exploitation could cause code execution	6.5	More Details
CVE-2023-50880	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The BuddyPress Community BuddyPress allows Stored XSS.This issue affects BuddyPress: from n/a through 11.3.1.	6.5	More Details
CVE-2023-50874	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Darren Cooney WordPress Infinite Scroll – Ajax Load More allows Stored XSS.This issue affects WordPress Infinite Scroll – Ajax Load More: from n/a through 6.1.0.1.	6.5	More Details
CVE-2023-50859	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum WP Crowdfunding allows Stored XSS.This issue affects WP Crowdfunding: from n/a through 2.1.6.	6.5	More Details
CVE-2023-50860	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TMS Booking for Appointments and Events Calendar – Amelia allows Stored XSS.This issue affects Booking for Appointments and Events Calendar – Amelia: from n/a through 1.0.85.	6.5	More Details
CVE-2023-50879	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WordPress.Com Editing Toolkit allows Stored XSS.This issue affects WordPress.Com Editing Toolkit: from n/a through 3.78784.	6.5	More Details
CVE-2023-34829	Incorrect access control in TP-Link Tapo before v3.1.315 allows attackers to access user credentials in plaintext.	6.5	More Details
CVE-2023-7079	Sending specially crafted HTTP requests and inspector messages to Wrangler's dev server could result in any file on the user's computer being accessible over the local network. An attacker that could trick any user on the local network into opening a malicious website could also read any file.	6.4	More Details
CVE-2023-49228	An issue was discovered in Peplink Balance Two before 8.4.0. Console port authentication uses hard-coded credentials, which allows an attacker with physical access and sufficient knowledge to execute arbitrary commands as root.	6.4	More Details
CVE-2023-51700	Unofficial Mobile BankID Integration for WordPress lets users employ Mobile BankID to authenticate themselves on your WordPress site. Prior to 1.0.1, WP-Mobile-BankID-Integration is affected by a vulnerability classified as a Deserialization of Untrusted Data vulnerability, specifically impacting scenarios where an attacker can manipulate the database. If unauthorized actors gain access to the database, they could exploit this vulnerability to execute object injection attacks. This could lead to unauthorized code execution, data manipulation, or data exfiltration within the WordPress environment. Users of the plugin should upgrade to version 1.0.1 (or later), where the serialization and deserialization of OrderResponse objects have been switched out to an array stored as JSON. A possible workaround for users unable to upgrade immediately is to enforce stricter access controls on the database, ensuring that only trusted and authorized entities can modify data. Additionally, implementing monitoring tools to detect unusual database activities could help identify and mitigate potential exploitation attempts.	6.4	More Details
CVE-2023-7130	A vulnerability has been found in code-projects College Notes Gallery 2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument user leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249133 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7116	A vulnerability, which was classified as critical, has been found in WeiYe-Jing datax-web 2.1.2. Affected by this issue is some unknown functionality of the file /api/log/killJob of the component HTTP POST Request Handler. The manipulation of the argument processId leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249086 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-7123	A vulnerability, which was classified as critical, has been found in SourceCodester Medicine Tracking System 1.0. This issue affects some unknown processing of the file /classes/Master.php? f=save_medicine. The manipulation of the argument id/name/description 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-249095.	6.3	More Details
CVE-2023-7126	A vulnerability classified as critical has been found in code-projects Automated Voting System 1.0. This affects an unknown part of the file /admin/ of the component Admin Login. The manipulation of the argument username leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249129 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0196	A vulnerability has been found in Magic-Api up to 2.0.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /resource/file/api/save?auto=1. The manipulation leads to code 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-249511.	6.3	More Details
CVE-2024-0192	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file downloadable.php of the component Add Downloadable. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249505 was assigned to this vulnerability.	6.3	More Details
CVE-2023-46919	Phlox com.phlox.simpleserver (aka Simple HTTP Server) 1.8 and com.phlox.simpleserver.plus (aka Simple HTTP Server PLUS) 1.8.1-plus have a hardcoded aKySWb2jjrr4dzkYXczKRt7K (AES) encryption key. An attacker with physical access to the application's source code or binary can extract this key & use it decrypt the TLS secret.	6.3	More Details
CVE-2023-7144	A vulnerability classified as critical has been found in gopeak MasterLab up to 3.3.10. This affects the function sqlInject of the file app/ctrl/framework/Feature.php of the component HTTP POST Request Handler. The manipulation of the argument pwd leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249147.	6.3	More Details
CVE-2024-0195	A vulnerability, which was classified as critical, was found in spider-flow 0.4.3. Affected is the function FunctionService.saveFunction of the file src/main/java/org/spiderflow/controller/FunctionController.java. The manipulation leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249510 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0194	A vulnerability, which was classified as critical, has been found in CodeAstro Internet Banking System up to 1.0. This issue affects some unknown processing of the file pages_account.php of the component Profile Picture Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249509 was assigned to this vulnerability.	6.3	More Details
CVE-2023-7127	A vulnerability classified as critical was found in code-projects Automated Voting System 1.0. This vulnerability affects unknown code of the component Login. The manipulation of the argument idno leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-249130 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-7128	A vulnerability, which was classified as critical, has been found in code-projects Voting System 1.0. This issue affects some unknown processing of the file /admin/ of the component Admin Login. The manipulation of the argument username leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249131.	6.3	More Details
CVE-2023-7134	A vulnerability was found in SourceCodester Medicine Tracking System 1.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument page 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-249137 was assigned to this vulnerability.	6.3	More Details
CVE-2023-7138	A vulnerability, which was classified as critical, was found in code-projects Client Details System 1.0. This affects an unknown part of the file /admin of the component HTTP POST Request Handler. The manipulation of the argument username leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249141 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7137	A vulnerability, which was classified as critical, has been found in code-projects Client Details System 1.0. Affected by this issue is some unknown functionality of the component HTTP POST Request Handler. The manipulation of the argument uemail leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249140.	6.3	More Details
CVE-2023-7131	A vulnerability was found in code-projects Intern Membership Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user_registration/ of the component User Registration. The manipulation of the argument userName leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-249134 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-7146	A vulnerability, which was classified as critical, has been found in gopeak MasterLab up to 3.3.10. This issue affects the function sqlInjectDelete of the file app/ctrl/framework/Feature.php of the component HTTP POST Request Handler. The manipulation of the argument phone leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249149 was assigned to this vulnerability.	6.3	More Details
CVE-2023-7145	A vulnerability classified as critical was found in gopeak MasterLab up to 3.3.10. This vulnerability affects the function sqlInject of the file app/ctrl/Framework.php of the component HTTP POST Request Handler. The manipulation of the argument pwd leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249148.	6.3	More Details
CVE-2023-7147	A vulnerability, which was classified as critical, was found in gopeak MasterLab up to 3.3.10. Affected is the function base64ImageContent of the file app/ctrl/User.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. VDB-249150 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-7155	A vulnerability, which was classified as critical, was found in SourceCodester Free and Open Source Inventory Management System 1.0. This affects an unknown part of the file /ample/app/action/edit_product.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 identifier VDB-249177 was assigned to this vulnerability.	6.3	More Details
CVE-2023-7157	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /app/ajax/sell_return_data.php. The manipulation of the argument columns[0][data] 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-249179.	6.3	More Details
CVE-2023-45702	An HCL UrbanCode Deploy Agent installed as a Windows service in a non-standard location could be subject to a denial of service attack by local accounts..	6.2	More Details
CVE-2023-4467	A vulnerability was found in Poly Trio 8800 7.2.6.0019 and classified as critical. Affected by this issue is some unknown functionality of the component Test Automation Mode. The manipulation leads to backdoor. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249260.	6.2	More Details
CVE-2023-31302	Cross Site Scripting (XSS) vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) 6.3.8.6 (#718), allows remote attackers to execute arbitrary code via the Teller field.	6.1	More Details
CVE-2023-52264	The beesblog (aka Bees Blog) component before 1.6.2 for thirty bees allows Reflected XSS because controllers/front/post.php sharing_url is mishandled.	6.1	More Details
CVE-2023-52263	Brave Browser before 1.59.40 does not properly restrict the schema for WebUI factory and redirect. This is related to browser/brave_content_browser_client.cc and browser/ui/webui/brave_web_ui_controller_factory.cc.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51652	OWASP AntiSamy .NET is a library for performing cleansing of HTML coming from untrusted sources. Prior to version 1.2.0, there is a potential for a mutation cross-site scripting (mXSS) vulnerability in AntiSamy caused by flawed parsing of the HTML being sanitized. To be subject to this vulnerability the `preserveComments` directive must be enabled in your policy file and also allow for certain tags at the same time. As a result, certain crafty inputs can result in elements in comment tags being interpreted as executable when using AntiSamy's sanitized output. This is patched in OWASP AntiSamy .NET 1.2.0 and later. See important remediation details in the reference given below. As a workaround, manually edit the AntiSamy policy file (e.g., antisamy.xml) by deleting the `preserveComments` directive or setting its value to `false`, if present. Also it would be useful to make AntiSamy remove the `noscript` tag by adding a line described in the GitHub Security Advisory to the tag definitions under the `<tagrules>` node, or deleting it entirely if present. As the previously mentioned policy settings are preconditions for the mXSS attack to work, changing them as recommended should be sufficient to protect you against this vulnerability when using a vulnerable version of this library. However, the existing bug would still be present in AntiSamy or its parser dependency (HtmlAgilityPack). The safety of this workaround relies on configurations that may change in the future and don't address the root cause of the vulnerability. As such, it is strongly recommended to upgrade to a fixed version of AntiSamy.	6.1	More Details
CVE-2023-52257	LogoBee 0.2 allows updates.php?id= XSS.	6.1	More Details
CVE-2023-52240	The Kantega SAML SSO OIDC Kerberos Single Sign-on apps before 6.20.0 for Atlassian products allow XSS if SAML POST Binding is enabled. This affects 4.4.2 through 4.14.8 before 4.14.9, 5.0.0 through 5.11.4 before 5.11.5, and 6.0.0 through 6.19.0 before 6.20.0. The full product names are Kantega SAML SSO OIDC Kerberos Single Sign-on for Jira Data Center & Server (Kantega SSO Enterprise), Kantega SAML SSO OIDC Kerberos Single Sign-on for Confluence Data Center & Server (Kantega SSO Enterprise), Kantega SAML SSO OIDC Kerberos Single Sign-on for Bitbucket Data Center & Server (Kantega SSO Enterprise), Kantega SAML SSO OIDC Kerberos Single Sign-on for Bamboo Data Center & Server (Kantega SSO Enterprise), and Kantega SAML SSO OIDC Kerberos Single Sign-on for FeCru Server (Kantega SSO Enterprise). (Here, FeCru refers to the Atlassian Fisheye and Crucible products running together.)	6.1	More Details
CVE-2024-21732	FlyCms through abbaa5a allows XSS via the permission management feature.	6.1	More Details
CVE-2023-50069	WireMock with GUI versions 3.2.0.0 through 3.0.4.0 are vulnerable to stored cross-site scripting (SXSS) through the recording feature. An attacker can host a malicious payload and perform a test mapping pointing to the attacker's file, and the result will render on the Matched page in the Body area, resulting in the execution of the payload. This occurs because the response body is not validated or sanitized.	6.1	More Details
CVE-2023-44089	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). It was possible to execute malicious JS code on Visual Consoles. This issue affects Pandora FMS: from 700 through 774.	6.1	More Details
CVE-2023-6000	The Popup Builder WordPress plugin before 4.2.3 does not prevent simple visitors from updating existing popups, and injecting raw JavaScript in them, which could lead to Stored XSS attacks.	6.1	More Details
CVE-2023-31301	Stored Cross Site Scripting (XSS) Vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows remote attackers to execute arbitrary code and obtain sensitive information via the Username field of the login form and application log.	6.1	More Details
CVE-2023-49469	Reflected Cross Site Scripting (XSS) vulnerability in Shaarli v0.12.2, allows remote attackers to execute arbitrary code via search tag function.	6.1	More Details
CVE-2023-4672	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Talent Software ECOP allows Reflected XSS.This issue affects ECOP: before 32255.	6.1	More Details
CVE-2023-31299	Cross Site Scripting (XSS) vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows remote attackers to execute arbitrary code via the Barcode field of a container.	6.1	More Details
CVE-2023-51429	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause information leak.	6.0	More Details
CVE-2023-23441	Some Honor products are affected by out of bounds read vulnerability, successful exploitation could cause information leak.	6.0	More Details
CVE-2023-51372	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes HashBar – WordPress Notification Bar allows Stored XSS.This issue affects HashBar – WordPress Notification Bar: from n/a through 1.4.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51371	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bit Assist Chat Widget: WhatsApp Chat, Facebook Messenger Chat, Telegram Chat Bubble, Line Messenger, Live Chat Support Chat Button, WeChat, SMS, Call Button, Customer Support Button with floating Chat Widget allows Stored XSS.This issue affects Chat Widget: WhatsApp Chat, Facebook Messenger Chat, Telegram Chat Bubble, Line Messenger, Live Chat Support Chat Button, WeChat, SMS, Call Button, Customer Support Button with floating Chat Widget: from n/a through 1.1.9.	5.9	More Details
CVE-2023-44088	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pandora FMS on all allows SQL Injection. Arbitrary SQL queries were allowed to be executed using any account with low privileges. This issue affects Pandora FMS: from 700 through 774.	5.9	More Details
CVE-2023-51361	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ginger Plugins Sticky Chat Widget: Click to chat, SMS, Email, Messages, Call Button, Live Chat and Live Support Button allows Stored XSS.This issue affects Sticky Chat Widget: Click to chat, SMS, Email, Messages, Call Button, Live Chat and Live Support Button: from n/a through 1.1.8.	5.9	More Details
CVE-2023-51503	Authorization Bypass Through User-Controlled Key vulnerability in Automattic WooPayments – Fully Integrated Solution Built and Supported by Woo.This issue affects WooPayments – Fully Integrated Solution Built and Supported by Woo: from n/a through 6.9.2.	5.9	More Details
CVE-2023-50896	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weForms weForms – Easy Drag & Drop Contact Form Builder For WordPress allows Stored XSS.This issue affects weForms – Easy Drag & Drop Contact Form Builder For WordPress: from n/a through 1.6.17.	5.9	More Details
CVE-2023-50836	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ibericode HTML Forms allows Stored XSS.This issue affects HTML Forms: from n/a through 1.3.28.	5.9	More Details
CVE-2024-21629	Rust EVM is an Ethereum Virtual Machine interpreter. In `rust-evm`, a feature called `record_external_operation` was introduced, allowing library users to record custom gas changes. This feature can have some bogus interactions with the call stack. In particular, during finalization of a `CREATE` or `CREATE2`, in the case that the substack execution happens successfully, `rust-evm` will first commit the substate, and then call `record_external_operation(Write(out_code.len()))`. If `record_external_operation` later fails, this error is returned to the parent call stack, instead of `Succeeded`. Yet, the substate commitment already happened. This causes smart contracts able to commit state changes, when the parent caller contract receives zero address (which usually indicates that the execution has failed). This issue only impacts library users with custom `record_external_operation` that returns errors. The issue is patched in release 0.41.1. No known workarounds are available.	5.9	More Details
CVE-2023-51374	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZeroBounce ZeroBounce Email Verification & Validation allows Stored XSS.This issue affects ZeroBounce Email Verification & Validation: from n/a through 1.0.11.	5.9	More Details
CVE-2023-50019	An issue was discovered in open5gs v2.6.6. InitialUEMessage, Registration request sent at a specific time can crash AMF due to incorrect error handling of Nudm_UECM_Registration response.	5.9	More Details
CVE-2023-50711	vmm-sys-util is a collection of modules that provides helpers and utilities used by multiple rust-vmm components. Starting in version 0.5.0 and prior to version 0.12.0, an issue in the `FamStructWrapper::deserialize` implementation provided by the crate for `vmm_sys_util::fam::FamStructWrapper` can lead to out of bounds memory accesses. The deserialization does not check that the length stored in the header matches the flexible array length. Mismatch in the lengths might allow out of bounds memory access through Rust-safe methods. The issue was corrected in version 0.12.0 by inserting a check that verifies the lengths of compared flexible arrays are equal for any deserialized header and aborting deserialization otherwise. Moreover, the API was changed so that header length can only be modified through Rust-unsafe code. This ensures that users cannot trigger out-of-bounds memory access from Rust-safe code.	5.7	More Details
CVE-2023-26157	Versions of the package libredwg before 0.12.5.6384 are vulnerable to Denial of Service (DoS) due to an out-of-bounds read involving section->num_pages in decode_r2007.c.	5.5	More Details
CVE-2023-7129	A vulnerability, which was classified as critical, was found in code-projects Voting System 1.0. Affected is an unknown function of the component Voters Login. The manipulation of the argument voter leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249132.	5.5	More Details
CVE-2023-52284	Bytecode Alliance wasm-micro-runtime (aka WebAssembly Micro Runtime or WAMR) before 1.3.0 can have an "double free or corruption" error for a valid WebAssembly module because push_pop_frame_ref_offset is mishandled.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50570	An issue in the component IPAddressBitsDivision of IPAddress v5.1.0 leads to an infinite loop. This is disputed because an infinite loop occurs only for cases in which the developer supplies invalid arguments. The product is not intended to always halt for contrived inputs.	5.5	More Details
CVE-2023-31292	An issue was discovered in Sesami Cash Point & Transport Optimizer (CPTO) 6.3.8.6 (#718), allows local attackers to obtain sensitive information and bypass authentication via "Back Button Refresh" attack.	5.5	More Details
CVE-2023-7180	A vulnerability has been found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/project/proj/delete.php. The manipulation of the argument PROJ_ID_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-249367. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-50572	An issue in the component GroovyEngine.execute of jline-groovy v3.24.1 allows attackers to cause an OOM (OutofMemory) error.	5.5	More Details
CVE-2023-7183	A vulnerability has been found in 7-card Fakabao up to 1.0_build20230805 and classified as critical. Affected by this vulnerability is an unknown functionality of the file shop/alipay_notify.php. The manipulation of the argument out_trade_no leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249385 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-7184	A vulnerability was found in 7-card Fakabao up to 1.0_build20230805 and classified as critical. Affected by this issue is some unknown functionality of the file shop/notify.php. The manipulation of the argument out_trade_no leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-249386 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-2023-7104	A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.	5.5	More Details
CVE-2023-7186	A vulnerability was found in 7-card Fakabao up to 1.0_build20230805. It has been declared as critical. This vulnerability affects unknown code of the file member/notify.php. The manipulation of the argument out_trade_no leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249388. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-7187	A vulnerability was found in Totolink N350RT 9.3.5u.6139_B20201216. It has been rated as critical. This issue affects some unknown processing of the file /cgi-bin/cstecgi.cgi?action=login&flag=ie8 of the component HTTP POST Request Handler. The manipulation leads to stack-based buffer overflow. The exploit has been disclosed to the public and may be used. The identifier VDB-249389 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-7189	A vulnerability classified as critical was found in S-CMS up to 2.0_build20220529-20231006. Affected by this vulnerability is an unknown functionality of the file /s/index.php?action=statistics. The manipulation of the argument lid leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249391. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-7190	A vulnerability, which was classified as critical, has been found in S-CMS up to 2.0_build20220529-20231006. Affected by this issue is some unknown functionality of the file /member/ad.php?action=ad. The manipulation of the argument A_text/A_url/A_contact leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249392. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-7191	A vulnerability, which was classified as critical, was found in S-CMS up to 2.0_build20220529-20231006. This affects an unknown part of the file member/reg.php. The manipulation of the argument M_login/M_email leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249393 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-32831	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7192	A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Linux Kernel. This issue may allow a local attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow.	5.5	More Details
CVE-2023-38023	An issue was discovered in SCONE Confidential Computing Platform before 5.8.0 for Intel SGX. Lack of pointer-alignment logic in __scone_dispatch and other entry functions allows a local attacker to access unauthorized information, aka an "AEPIC Leak."	5.5	More Details
CVE-2023-38022	An issue was discovered in Fortanix EnclaveOS Confidential Computing Manager (CCM) Platform before 3.29 for Intel SGX. Insufficient pointer validation allows a local attacker to access unauthorized information. This relates to strlen and sgx_is_within_user.	5.5	More Details
CVE-2023-38021	An issue was discovered in Fortanix EnclaveOS Confidential Computing Manager (CCM) Platform before 3.32 for Intel SGX. Lack of pointer-alignment validation logic in entry functions allows a local attacker to access unauthorized information. This relates to the enclave_ecall function and system call layer.	5.5	More Details
CVE-2022-46486	A lack of pointer-validation logic in the __scone_dispatch component of SCONE before v5.8.0 for Intel SGX allows attackers to access sensitive information.	5.5	More Details
CVE-2023-50559	An issue was discovered in XiangShan v2.1, allows local attackers to obtain sensitive information via the L1D cache.	5.5	More Details
CVE-2023-7152	A vulnerability, which was classified as critical, has been found in MicroPython 1.21.0/1.22.0-preview. Affected by this issue is the function poll_set_add_fd of the file extmod/modselect.c. The manipulation leads to use after free. The exploit has been disclosed to the public and may be used. The patch is identified as 8b24aa36ba978eafc6114b6798b47b7bfecdca26. It is recommended to apply a patch to fix this issue. VDB-249158 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-7185	A vulnerability was found in 7-card Fakabao up to 1.0_build20230805. It has been classified as critical. This affects an unknown part of the file shop/wxpay_notify.php. The manipulation of the argument out_trade_no leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249387. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-50470	A cross-site scripting (XSS) vulnerability in the component admin_ Video.php of SeaCMS v12.8 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-6485	The Html5 Video Player WordPress plugin before 2.5.19 does not sanitise and escape some of its player settings, which combined with missing capability checks around the plugin could allow any authenticated users, such as low as subscribers to perform Stored Cross-Site Scripting attacks against high privilege users like admins	5.4	More Details
CVE-2023-50858	Cross-Site Request Forgery (CSRF) vulnerability in Bill Minozzi Disable Json API, Login Lockdown, XMLRPC, Pingback, Stop User Enumeration Anti Hacker Scan.This issue affects Disable Json API, Login Lockdown, XMLRPC, Pingback, Stop User Enumeration Anti Hacker Scan: from n/a through 4.34.	5.4	More Details
CVE-2023-52265	IDURAR (aka idurar-erp-crm) through 2.0.1 allows stored XSS via a PATCH request with a crafted JSON email template in the /api/email/update data.	5.4	More Details
CVE-2024-21628	PrestaShop is an open-source e-commerce platform. Prior to version 8.1.3, the isCleanHtml method is not used on this this form, which makes it possible to store a cross-site scripting payload in the database. The impact is low because the HTML is not interpreted in BO, thanks to twig's escape mechanism. In FO, the cross-site scripting attack is effective, but only impacts the customer sending it, or the customer session from which it was sent. This issue affects those who have a module fetching these messages from the DB and displaying it without escaping HTML. Version 8.1.3 contains a patch for this issue.	5.4	More Details
CVE-2023-51378	Cross-Site Request Forgery (CSRF) vulnerability in Rise Themes Rise Blocks – A Complete Gutenberg Page Builder.This issue affects Rise Blocks – A Complete Gutenberg Page Builder: from n/a through 3.1.	5.4	More Details
CVE-2023-51358	Cross-Site Request Forgery (CSRF) vulnerability in Bright Plugins Block IPs for Gravity Forms.This issue affects Block IPs for Gravity Forms: from n/a through 1.0.1.	5.4	More Details
CVE-2023-50878	Cross-Site Request Forgery (CSRF) vulnerability in InspireUI MStore API.This issue affects MStore API: from n/a through 4.10.1.	5.4	More Details
CVE-2023-50550	layui up to v2.74 was discovered to contain a cross-site scripting (XSS) vulnerability via the data-content parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31296	CSV Injection vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows attackers to obtain sensitive information via the User Name field.	5.3	More Details
CVE-2023-51527	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Senol Sahin AI Power: Complete AI Pack – Powered by GPT-4.This issue affects AI Power: Complete AI Pack – Powered by GPT-4: from n/a through 1.8.2.	5.3	More Details
CVE-2023-51687	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in impleCode Product Catalog Simple.This issue affects Product Catalog Simple: from n/a through 1.7.6.	5.3	More Details
CVE-2023-51688	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in impleCode eCommerce Product Catalog Plugin for WordPress.This issue affects eCommerce Product Catalog Plugin for WordPress: from n/a through 3.3.26.	5.3	More Details
CVE-2023-51663	Hail is an open-source, general-purpose, Python-based data analysis tool with additional data types and methods for working with genomic data. Hail relies on OpenID Connect (OIDC) email addresses from ID tokens to verify the validity of a user's domain, but because users have the ability to change their email address, they could create accounts and use resources in clusters that they should not have access to. For example, a user could create a Microsoft or Google account and then change their email to `test@example.org`. This account can then be used to create a Hail Batch account in Hail Batch clusters whose organization domain is `example.org`. The attacker is not able to access private data or impersonate another user, but they would have the ability to run jobs if Hail Batch billing projects are enabled and create Azure Tenants if they have Azure Active Directory Administrator access.	5.3	More Details
CVE-2023-52081	ffcss is a CLI interface to apply and configure Firefox CSS themes. Prior to 0.2.0, the function `lookupPreprocess()` is meant to apply some transformations to a string by disabling characters in the regex `[-_ .]`. However, due to the use of late Unicode normalization of type NFKD, it is possible to bypass that validation and re-introduce all the characters in the regex `[-_ .]`. The `lookupPreprocess()` can be easily bypassed with equivalent Unicode characters like U+FE4D (﹍), which would result in the omitted U+005F (_), for instance. The `lookupPreprocess()` function is only ever used to search for themes loosely (case insensitively, while ignoring dashes, underscores and dots), so the actual security impact is classified as low. This vulnerability is fixed in 0.2.0. There are no known workarounds.	5.3	More Details
CVE-2023-27447	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in VeronaLabs WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc.This issue affects WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc: from n/a through 6.0.4.	5.3	More Details
CVE-2023-51010	An issue in the export component AdSdkH5Activity of com.sdjictec.qdmetro v4.2.2 allows attackers to open a crafted URL without any filtering or checking.	5.3	More Details
CVE-2023-52185	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Everestthemes Everest Backup – WordPress Cloud Backup, Migration, Restore & Cloning Plugin.This issue affects Everest Backup – WordPress Cloud Backup, Migration, Restore & Cloning Plugin: from n/a through 2.1.9.	5.3	More Details
CVE-2023-51079	A long execution time can occur in the ParseTools.subCompileExpression method in MVEL 2.5.0.Final because of many Java class lookups. NOTE: the vendor disputes this because "the only thing that you could expect is that the parser will take a crazy amount of time to complete its task."	5.3	More Details
CVE-2023-51074	json-path v2.8.0 was discovered to contain a stack overflow via the Criteria.parse() method.	5.3	More Details
CVE-2023-45561	An issue in A-WORLD OIRASE BEER_waiting Line v.13.6.1 allows attackers to send crafted notifications via leakage of the channel access token.	5.3	More Details
CVE-2024-0191	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/uploads/. The manipulation leads to file and directory information exposure. 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-249504.	5.3	More Details
CVE-2023-4463	A vulnerability classified as problematic was found in Poly CCX 400, CCX 600, Trio 8800 and Trio C60. This vulnerability affects unknown code of the component HTTP Header Handler. The manipulation of the argument Cookie leads to denial of service. 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-249256.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6093	A clickjacking vulnerability has been identified in OnCell G3150A-LTE Series firmware versions v1.3 and prior. This vulnerability is caused by incorrectly restricts frame objects, which can lead to user confusion about which interface the user is interacting with. This vulnerability may lead the attacker to trick the user into interacting with the application.	5.3	More Details
CVE-2023-6094	A vulnerability has been identified in OnCell G3150A-LTE Series firmware versions v1.3 and prior. The vulnerability results from lack of protection for sensitive information during transmission. An attacker eavesdropping on the traffic between the web browser and server may obtain sensitive information. This type of attack could be executed to gather sensitive information or to facilitate a subsequent attack against the target.	5.3	More Details
CVE-2022-36399	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in BoxyStudio Booked - Appointment Booking for WordPress	Calendars.This issue affects Booked - Appointment Booking for WordPress	Calendars: from n/a before 2.4.4.	5.3	More Details
CVE-2023-49003	An issue in simplemobiletools Simple Dialer 5.18.1 allows an attacker to bypass intended access restrictions via interaction with com.simplemobiletools.dialer.activities.DialerActivity.	5.3	More Details
CVE-2023-7148	A vulnerability has been found in ShifuML shifu 0.12.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file src/main/java/ml/shifu/shifu/core/DataPurifier.java of the component Java Expression Language Handler. The manipulation of the argument FilterExpression leads to code injection. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249151.	5.0	More Details
CVE-2023-7188	A vulnerability classified as critical has been found in Shipping 100 Fahuo100 up to 1.1. Affected is an unknown function of the file member/login.php. The manipulation of the argument M_pwd leads to sql injection. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. VDB-249390 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2023-6693	A stack based buffer overflow was found in the virtio-net device of QEMU. This issue occurs when flushing TX in the virtio_net_flush_tx function if guest features VIRTIO_NET_F_HASH_REPORT, VIRTIO_F_VERSION_1 and VIRTIO_NET_F_MRG_RXBUF are enabled. This could allow a malicious user to overwrite local variables allocated on the stack. Specifically, the `out_sg` variable could be used to read a part of process memory and send it to the wire, causing an information leak.	4.9	More Details
CVE-2023-51676	Server-Side Request Forgery (SSRF) vulnerability in Leevio Happy Addons for Elementor.This issue affects Happy Addons for Elementor: from n/a through 3.9.1.1.	4.9	More Details
CVE-2023-31298	Cross Site Scripting (XSS) vulnerability in Sesami Cash Point & Transport Optimizer (CPTO) version 6.3.8.6 (#718), allows remote attackers to execute arbitrary code and obtain sensitive information via the User ID field when creating a new system user.	4.8	More Details
CVE-2023-52269	MDaemon SecurityGateway through 9.0.3 allows XSS via a crafted Message Content Filtering rule. This might allow domain administrators to conduct attacks against global administrators.	4.8	More Details
CVE-2023-6037	The WP TripAdvisor Review Slider WordPress plugin before 11.9 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-2024-0185	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file dasboard_teacher.php of the component Avatar Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249443.	4.7	More Details
CVE-2023-7181	A vulnerability was found in Muyun DedeBIZ up to 6.2.12 and classified as critical. Affected by this issue is some unknown functionality of the component Add Attachment Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249368. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-51675	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in AAM Advanced Access Manager – Restricted Content, Users & Roles, Enhanced Security and More.This issue affects Advanced Access Manager – Restricted Content, Users & Roles, Enhanced Security and More: from n/a through 6.9.18.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31095	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for HubSpot and Contact Form 7, WPForms, Elementor, Ninja Forms.This issue affects Integration for HubSpot and Contact Form 7, WPForms, Elementor, Ninja Forms: from n/a through 1.2.8.	4.7	More Details
CVE-2023-7177	A vulnerability classified as critical was found in Campcodes Online College Library System 1.0. This vulnerability affects unknown code of the file /admin/book_add.php of the component HTTP POST Request Handler. The manipulation of the argument category 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-249364.	4.7	More Details
CVE-2023-32101	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Pexle Chris Library Viewer.This issue affects Library Viewer: from n/a through 2.0.6.	4.7	More Details
CVE-2023-31229	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in WP Directory Kit.This issue affects WP Directory Kit: from n/a through 1.1.9.	4.7	More Details
CVE-2023-31237	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Dylan James Zephyr Project Manager.This issue affects Zephyr Project Manager: from n/a through 3.3.9.	4.7	More Details
CVE-2023-7176	A vulnerability classified as critical has been found in Campcodes Online College Library System 1.0. This affects an unknown part of the file /admin/return_add.php of the component HTTP POST Request Handler. The manipulation of the argument student 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-249363.	4.7	More Details
CVE-2023-7150	A vulnerability classified as critical was found in Campcodes Chic Beauty Salon 20230703. Affected by this vulnerability is an unknown functionality of the file product-list.php of the component Product Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249157 was assigned to this vulnerability.	4.7	More Details
CVE-2023-32517	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in PluginOps MailChimp Subscribe Form, Optin Builder, PopUp Builder, Form Builder.This issue affects MailChimp Subscribe Form, Optin Builder, PopUp Builder, Form Builder: from n/a through 4.0.9.3.	4.7	More Details
CVE-2023-7159	A vulnerability was found in gopeak MasterLab up to 3.3.10. It has been declared as critical. Affected by this vulnerability is the function add/update of the file app/ctrl/admin/User.php. The manipulation of the argument avatar 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-249181 was assigned to this vulnerability.	4.7	More Details
CVE-2023-7179	A vulnerability, which was classified as critical, was found in Campcodes Online College Library System 1.0. Affected is an unknown function of the file /admin/category_row.php of the component HTTP POST Request Handler. 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-249366 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-7178	A vulnerability, which was classified as critical, has been found in Campcodes Online College Library System 1.0. This issue affects some unknown processing of the file /admin/book_row.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-249365 was assigned to this vulnerability.	4.7	More Details
CVE-2023-7175	A vulnerability was found in Campcodes Online College Library System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/borrow_add.php of the component HTTP POST Request Handler. The manipulation of the argument student leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249362 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-4641	A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.	4.7	More Details
CVE-2023-23443	Some Honor products are affected by type confusion vulnerability, successful exploitation could cause information leak.	4.6	More Details
CVE-2023-51428	Some Honor products are affected by type confusion vulnerability, successful exploitation could cause information leak.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51427	Some Honor products are affected by type confusion vulnerability, successful exploitation could cause information leak.	4.6	More Details
CVE-2023-51426	Some Honor products are affected by type confusion vulnerability, successful exploitation could cause information leak.	4.6	More Details
CVE-2023-46918	Phlox com.phlox.simpleserver.plus (aka Simple HTTP Server PLUS) 1.8.1-plus has an Android manifest file that contains an entry with the android:allowBackup attribute set to true. This could be leveraged by an attacker with physical access to the device.	4.6	More Details
CVE-2023-23442	Some Honor products are affected by type confusion vulnerability, successful exploitation could cause information leak.	4.6	More Details
CVE-2023-7193	A vulnerability was found in MTab Bookmark up to 1.2.6 and classified as critical. This issue affects some unknown processing of the file public/install.php of the component Installation. The manipulation leads to improper access controls. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249395. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.6	More Details
CVE-2023-32881	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080.	4.4	More Details
CVE-2023-51430	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause information leak.	4.4	More Details
CVE-2023-32878	In battery, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08307992.	4.4	More Details
CVE-2023-32876	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612.	4.4	More Details
CVE-2023-32875	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217.	4.4	More Details
CVE-2023-32880	In battery, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308076.	4.4	More Details
CVE-2023-48732	Mattermost fails to scope the WebSocket response around notified users to a each user separately resulting in the WebSocket broadcasting the information about who was notified about a post to everyone else in the channel.	4.3	More Details
CVE-2018-25096	A vulnerability was found in MdAlAmin-aol Own Health Record 0.1-alpha/0.2-alpha/0.3-alpha/0.3.1-alpha. It has been rated as problematic. This issue affects some unknown processing of the file includes/logout.php. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. Upgrading to version 0.4-alpha is able to address this issue. The patch is named 58b413aa40820b49070782c786c526850ab7748f. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-249191.	4.3	More Details
CVE-2023-7139	A vulnerability has been found in code-projects Client Details System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/regester.php of the component HTTP POST Request Handler. The manipulation of the argument fname/lname/email/contact leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-249142 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-51665	Audiobookshelf is a self-hosted audiobook and podcast server. Prior to 2.7.0, Audiobookshelf is vulnerable to unauthenticated blind server-side request (SSRF) vulnerability in Auth.js. This vulnerability has been addressed in version 2.7.0. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2023-45701	HCL Launch could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7124	A vulnerability, which was classified as problematic, was found in code-projects E-Commerce Site 1.0. Affected is an unknown function of the file search.php. The manipulation of the argument keyword with the input <video/src=x onerror=alert(document.cookie)> 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-249096.	4.3	More Details
CVE-2023-49229	An issue was discovered in Peplink Balance Two before 8.4.0. A missing authorization check in the administration web service allows read-only, unprivileged users to obtain sensitive information about the device configuration.	4.3	More Details
CVE-2023-7133	A vulnerability was found in y_project RuoYi 4.7.8. It has been declared as problematic. This vulnerability affects unknown code of the file /login of the component HTTP POST Request Handler. The manipulation of the argument rememberMe with the input falsen3f0m<script>alert(1)</script>p86o0 leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249136.	4.3	More Details
CVE-2023-7173	A vulnerability, which was classified as problematic, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file registration.php. The manipulation of the argument First Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249357 was assigned to this vulnerability.	4.3	More Details
CVE-2023-31293	An issue was discovered in Sesami Cash Point & Transport Optimizer (CPTO) 6.3.8.6 (#718), allows remote attackers to obtain sensitive information and bypass profile restriction via improper access control in the Reader system user's web browser, allowing the journal to be displayed, despite the option being disabled.	4.3	More Details
CVE-2023-7140	A vulnerability was found in code-projects Client Details System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/manage-users.php. The manipulation of the argument 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-249143.	4.3	More Details
CVE-2023-4468	A vulnerability was found in Poly Trio 8500, Trio 8800 and Trio C60. It has been classified as problematic. This affects an unknown part of the component Poly Lens Management Cloud Registration. The manipulation leads to missing authorization. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier VDB-249261 was assigned to this vulnerability.	4.3	More Details
CVE-2023-50902	Cross-Site Request Forgery (CSRF) vulnerability in WPExpertsio New User Approve.This issue affects New User Approve: from n/a through 2.5.1.	4.3	More Details
CVE-2023-50267	MeterSphere is a one-stop open source continuous testing platform. Prior to 2.10.10-lts, the authenticated attackers can update resources which don't belong to him if the resource ID is known. This issue if fixed in 2.10.10-lts. There are no known workarounds.	4.3	More Details
CVE-2023-47858	Mattermost fails to properly verify the permissions needed for viewing archived public channels, allowing a member of one team to get details about the archived public channels of another team via the GET /api/v4/teams/<team-id>/channels/deleted endpoint.	4.3	More Details
CVE-2023-51402	Cross-Site Request Forgery (CSRF) vulnerability in Brain Storm Force Ultimate Addons for WPBakery Page Builder.This issue affects Ultimate Addons for WPBakery Page Builder: from n/a through 3.19.17.	4.3	More Details
CVE-2023-50873	Cross-Site Request Forgery (CSRF) vulnerability in Marios Alexandrou Add Any Extension to Pages.This issue affects Add Any Extension to Pages: from n/a through 1.4.	4.3	More Details
CVE-2023-51697	Audiobookshelf is a self-hosted audiobook and podcast server. Prior to 2.7.0, Audiobookshelf is vulnerable to unauthenticated blind server-side request (SSRF) vulnerability in `podcastUtils.js`. This vulnerability has been addressed in version 2.7.0. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2023-7141	A vulnerability was found in code-projects Client Details System 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/update-clients.php. The manipulation of the argument uid leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249144.	4.3	More Details
CVE-2023-7142	A vulnerability was found in code-projects Client Details System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/clientview.php. The manipulation of the argument ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-249145 was assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51354	Cross-Site Request Forgery (CSRF) vulnerability in WebbaPlugins Appointment & Event Booking Calendar Plugin – Webba Booking.This issue affects Appointment & Event Booking Calendar Plugin – Webba Booking: from n/a through 4.5.33.	4.3	More Details
CVE-2023-51517	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CodePeople Calculated Fields Form.This issue affects Calculated Fields Form: from n/a through 1.2.28.	4.1	More Details
CVE-2023-23439	Some Honor products are affected by information leak vulnerability, successful exploitation could cause the information leak.	4.0	More Details
CVE-2023-47857	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia camera crash through modify a released pointer.	4.0	More Details
CVE-2023-49135	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia player crash through modify a released pointer.	4.0	More Details
CVE-2023-23427	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause device service exceptions.	4.0	More Details
CVE-2023-23429	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause device service exceptions.	4.0	More Details
CVE-2023-23438	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause device service exceptions	4.0	More Details
CVE-2023-49142	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia audio crash through modify a released pointer.	4.0	More Details
CVE-2023-48360	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia player crash through modify a released pointer.	4.0	More Details
CVE-2023-23433	Some Honor products are affected by signature management vulnerability, successful exploitation could cause the forged system file overwrite the correct system file.	4.0	More Details
CVE-2023-6939	Some Honor products are affected by type confusion vulnerability, successful exploitation could cause denial of service.	4.0	More Details
CVE-2023-23434	Some Honor products are affected by information leak vulnerability, successful exploitation could cause the information leak.	4.0	More Details
CVE-2023-23435	Some Honor products are affected by signature management vulnerability, successful exploitation could cause the forged system file overwrite the correct system file	4.0	More Details
CVE-2020-26624	A SQL injection vulnerability was discovered in Gila CMS 1.15.4 and earlier which allows a remote attacker to execute arbitrary web scripts via the ID parameter after the login portal.	3.8	More Details
CVE-2020-26625	A SQL injection vulnerability was discovered in Gila CMS 1.15.4 and earlier which allows a remote attacker to execute arbitrary web scripts via the 'user_id' parameter after the login portal.	3.8	More Details
CVE-2020-26623	SQL Injection vulnerability discovered in Gila CMS 1.15.4 and earlier allows a remote attacker to execute arbitrary web scripts via the Area parameter under the Administration>Widget tab after the login portal.	3.8	More Details
CVE-2023-28786	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in SolidWP Solid Security – Password, Two Factor Authentication, and Brute Force Protection.This issue affects Solid Security – Password, Two Factor Authentication, and Brute Force Protection: from n/a through 8.1.4.	3.7	More Details
CVE-2023-50333	Mattermost fails to update the permissions of the current session for a user who was just demoted to guest, allowing freshly demoted guests to change group names.	3.7	More Details
CVE-2023-41814	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). Through an HTML payload (iframe tag) it is possible to carry out XSS attacks when the user receiving the messages opens their notifications. This issue affects Pandora FMS: from 700 through 774.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4462	A vulnerability classified as problematic has been found in Poly Trio 8300, Trio 8500, Trio 8800, Trio C60, CCX 350, CCX 400, CCX 500, CCX 505, CCX 600, CCX 700, EDGE E100, EDGE E220, EDGE E300, EDGE E320, EDGE E350, EDGE E400, EDGE E450, EDGE E500, EDGE E550, VVX 101, VVX 150, VVX 201, VVX 250, VVX 300, VVX 301, VVX 310, VVX 311, VVX 350, VVX 400, VVX 401, VVX 410, VVX 411, VVX 450, VVX 500, VVX 501, VVX 600 and VVX 601. This affects an unknown part of the component Web Configuration Application. The manipulation leads to insufficiently random values. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249255.	3.7	More Details
CVE-2023-7113	Mattermost version 8.1.6 and earlier fails to sanitize channel mention data in posts, which allows an attacker to inject markup in the web client.	3.7	More Details
CVE-2024-0186	A vulnerability classified as problematic has been found in HuiRan Host Reseller System up to 2.0.0. Affected is an unknown function of the file /user/index/findpass?do=4 of the component HTTP POST Request Handler. The manipulation leads to weak password recovery. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249444.	3.7	More Details
CVE-2024-0189	A vulnerability has been found in RRJ Nueva Ecija Engineer Online Portal 1.0 and classified as problematic. This vulnerability affects unknown code of the file teacher_message.php of the component Create Message Handler. The manipulation of the argument Content with the input </title><scRipt>alert(x)</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-249502 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0190	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file add_quiz.php of the component Quiz Handler. The manipulation of the argument Quiz Title/Quiz Description with the input </title><scRipt>alert(x)</scRipt> 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-249503.	3.5	More Details
CVE-2023-7132	A vulnerability was found in code-projects Intern Membership Management System 2.0. It has been classified as problematic. This affects an unknown part of the file /user_registration/ of the component User Registration. The manipulation of the argument userName/firstName/lastName/userEmail with the input "><ScRiPt>confirm(document.domain)</ScRiPt>h0la leads to cross site scripting. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249135.	3.5	More Details
CVE-2018-25097	A vulnerability, which was classified as problematic, was found in Acumos Design Studio up to 2.0.7. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.0.8 is able to address this issue. The name of the patch is 0df8a5e8722188744973168648e4c74c69ce67fd. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-249420.	3.5	More Details
CVE-2015-10128	A vulnerability was found in rt-prettyphoto Plugin up to 1.2 on WordPress and classified as problematic. Affected by this issue is the function royal_prettyphoto_plugin_links of the file rt-prettyphoto.php. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.3 is able to address this issue. The patch is identified as 0d3d38cfa487481b66869e4212df1cefc281ecb7. It is recommended to upgrade the affected component. VDB-249422 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-7166	A vulnerability classified as problematic has been found in Novel-Plus up to 4.2.0. This affects an unknown part of the file /user/updateUserInfo of the component HTTP POST Request Handler. The manipulation of the argument nickName 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 of the patch is c62da9bb3a9b3603014d0edb436146512631100d. It is recommended to apply a patch to fix this issue. The identifier VDB-249201 was assigned to this vulnerability.	3.5	More Details
CVE-2023-7149	A vulnerability was found in code-projects QR Code Generator 1.0. It has been classified as problematic. This affects an unknown part of the file /download.php?file=author.png. The manipulation of the argument file with the input "><iMg src=N onerror=alert(document.domain)> 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-249153 was assigned to this vulnerability.	3.5	More Details
CVE-2023-23437	Some Honor products are affected by information leak vulnerability, successful exploitation could cause the information leak	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52085	Winter is a free, open-source content management system. Users with access to backend forms that include a ColorPicker FormWidget can provide a value that would then be included without further processing in the compilation of custom stylesheets via LESS. This had the potential to lead to a Local File Inclusion vulnerability. This issue has been patched in v1.2.4.	3.3	More Details
CVE-2023-23428	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause device service exceptions.	3.3	More Details
CVE-2023-23430	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause device service exceptions.	3.3	More Details
CVE-2023-23440	Some Honor products are affected by information leak vulnerability, successful exploitation could cause the information leak.	3.3	More Details
CVE-2023-51432	Some Honor products are affected by out of bounds read vulnerability, successful exploitation could cause information leak.	3.2	More Details
CVE-2024-0188	A vulnerability, which was classified as problematic, was found in RRJ Nueva Ecija Engineer Online Portal 1.0. This affects an unknown part of the file change_password_teacher.php. The manipulation leads to weak password requirements. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-249501 was assigned to this vulnerability.	3.1	More Details
CVE-2023-22676	Missing Authorization vulnerability in Anders Thorborg.This issue affects Anders Thorborg: from n/a through 1.4.12.	3.1	More Details
CVE-2023-41813	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). Allows you to edit the Web Console user notification options. This issue affects Pandora FMS: from 700 through 774.	3.0	More Details
CVE-2023-51433	Some Honor products are affected by incorrect privilege assignment vulnerability, successful exploitation could cause information leak.	2.9	More Details
CVE-2023-47216	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause DOS through occupy all resources	2.9	More Details
CVE-2023-4466	A vulnerability has been found in Poly CCX 400, CCX 600, Trio 8800 and Trio C60 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Web Interface. The manipulation leads to protection mechanism failure. The attack can be launched remotely. The vendor explains that they do not regard this as a vulnerability as this is a feature that they offer to their customers who have a variety of environmental needs that are met through different firmware builds. To avoid potential roll-back attacks, they remove vulnerable builds from the public servers as a remediation effort. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249259.	2.7	More Details
CVE-2023-4465	A vulnerability, which was classified as problematic, was found in Poly Trio 8300, Trio 8500, Trio 8800, Trio C60, CCX 350, CCX 400, CCX 500, CCX 505, CCX 600, CCX 700, EDGE E100, EDGE E220, EDGE E300, EDGE E320, EDGE E350, EDGE E400, EDGE E450, EDGE E500, EDGE E550, VVX 101, VVX 150, VVX 201, VVX 250, VVX 300, VVX 301, VVX 310, VVX 311, VVX 350, VVX 400, VVX 401, VVX 410, VVX 411, VVX 450, VVX 500, VVX 501, VVX 600 and VVX 601. Affected is an unknown function of the component Configuration File Import. The manipulation of the argument device.auth.localAdminPassword leads to unverified password change. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249258 is the identifier assigned to this vulnerability.	2.7	More Details
CVE-2017-20188	A vulnerability has been found in Zimbra zm-ajax up to 8.8.1 and classified as problematic. Affected by this vulnerability is the function XFormItem.prototype.setError of the file WebRoot/js/ajax/dwt/xforms/XFormItem.js. The manipulation of the argument message leads to cross site scripting. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 8.8.2 is able to address this issue. The identifier of the patch is 8d039d6efe80780adc40c6f670c06d21de272105. It is recommended to upgrade the affected component. The identifier VDB-249421 was assigned to this vulnerability.	2.6	More Details
CVE-2023-7143	A vulnerability was found in code-projects Client Details System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/regester.php. The manipulation of the argument fname/lname/email/contact leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249146 is the identifier assigned to this vulnerability.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7171	A vulnerability was found in Novel-Plus up to 4.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file novel-admin/src/main/java/com/java2nb/novel/controller/FriendLinkController.java of the component Friendly Link 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 patch is named d6093d8182362422370d7eaf6c53afde9ee45215. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-249307.	2.4	More Details
CVE-2023-7135	A vulnerability classified as problematic has been found in code-projects Record Management System 1.0. Affected is an unknown function of the file /main/offices.php of the component Offices Handler. The manipulation of the argument officename with the input "><script src="https://js.rip/b23tmbxf49"></script> 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. VDB-249138 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-7136	A vulnerability classified as problematic was found in code-projects Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /main/doctype.php of the component Document Type Handler. The manipulation of the argument docname with the input "><script src="https://js.rip/b23tmbxf49"> </script> leads to cross site scripting. 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-249139.	2.4	More Details
CVE-2024-0183	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/students.php of the component NIA Office. The manipulation leads to basic 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-249441 was assigned to this vulnerability.	2.4	More Details
CVE-2024-0184	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/edit_teacher.php of the component Add Enginer. The manipulation of the argument Firstname/Lastname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249442 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-7160	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add Engineer Handler. The manipulation of the argument first name/last name with the input <script>alert(0)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249182 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2024-0181	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin_user.php of the component Admin Panel. The manipulation of the argument Firstname/Lastname/Username 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-249433 was assigned to this vulnerability.	2.4	More Details
CVE-2023-52275	Gallery3d on Tecno Camon X CA7 devices allows attackers to view hidden images by navigating to data/com.android.gallery3d/.privatealbum/.encryptfiles and guessing the correct image file extension.	2.1	More Details
CVE-2023-52084	Winter is a free, open-source content management system. Prior to 1.2.4, Users with access to backend forms that include a ColorPicker FormWidget can provide a value that would then be rendered unescaped in the backend form, potentially allowing for a stored XSS attack. This issue has been patched in v1.2.4.	2.0	More Details
CVE-2023-52083	Winter is a free, open-source content management system. Prior to 1.2.4, users with the `media.manage_media` permission can upload files to the Media Manager and rename them after uploading. Previously, media manager files were only sanitized on upload, not on renaming, which could have allowed a stored XSS attack. This issue has been patched in v1.2.4.	2.0	More Details
CVE-2023-6752	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-6747. Reason: This candidate is a reservation duplicate of CVE-2023-6747. Notes: All CVE users should reference CVE-2023-6747 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-48721	Rejected reason: Not used	N/A	More Details