SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 May 2023

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-2023-1778	This vulnerability exists in GajShield Data Security Firewall firmware versions prior to v4.28 (except v4.21) due to insecure default credentials which allows remote attacker to login as superuser by using default username/password via web-based management interface and/or exposed SSH port thereby enabling remote attackers to execute arbitrary commands with administrative/superuser privileges on the targeted systems. The vulnerability has been addressed by forcing the user to change their default password to a new non-default password.	10.0	More Details
CVE-2023-1968	Instruments with Illumina Universal Copy Service v2.x are vulnerable due to binding to an unrestricted IP address. An unauthenticated malicious actor could use UCS to listen on all IP addresses, including those capable of accepting remote communications.	10.0	More Details
CVE-2012-5872	ARC (aka ARC2) through 2011-12-01 allows blind SQL Injection in getTriplePatternSQL in ARC2_StoreSelectQueryHandler.php via comments in a SPARQL WHERE clause.	9.8	More Details
CVE-2023-31470	SmartDNS through 41 before 56d0332 allows an out-of-bounds write because of a stack-based buffer overflow in the _dns_encode_domain function in the dns.c file, via a crafted DNS request.	9.8	More Details
CVE-2022-41400	Sage 300 through 2022 uses a hard-coded 40-byte blowfish key to encrypt and decrypt user passwords and SQL connection strings stored in ISAM database files in the shared data directory. This issue could allow attackers to decrypt user passwords and SQL connection strings.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27971	Certain HP LaserJet Pro print products are potentially vulnerable to Buffer Overflow and/or Elevation of Privilege.	9.8	More Details
CVE-2023-27972	Certain HP LaserJet Pro print products are potentially vulnerable to Buffer Overflow and/or Remote Code Execution.	9.8	More Details
CVE-2023-27973	Certain HP LaserJet Pro print products are potentially vulnerable to Heap Overflow and/or Remote Code Execution.	9.8	More Details
CVE-2023-26781	SQL injection vulnerability in mccms 2.6 allows remote attackers to run arbitrary SQL commands via Author Center ->Reader Comments ->Search.	9.8	More Details
CVE-2023-26813	SQL injection vulnerability in com.xnx3.wangmarket.plugin.dataDictionary.controller.DataDictionaryPluginController.java in wangmarket CMS 4.10 allows remote attackers to run arbitrary SQL commands via the TableName parameter to /plugin/dataDictionary/tableView.do.	9.8	More Details
CVE-2023-2429	Improper Access Control in GitHub repository thorsten/phpmyfaq prior to 3.1.13.	9.8	More Details
CVE-2023-30466	This vulnerability exists in Milesight 4K/H.265 Series NVR models (MS-Nxxxx-xxG, MS-Nxxxx-xxE, MS-Nxxxx-xxT, MS-Nxxxx-xxH and MS-Nxxxx-xxC), due to a weak password reset mechanism at the Milesight NVR web-based management interface. A remote attacker could exploit this vulnerability by sending a specially crafted http requests on the targeted device. Successful exploitation of this vulnerability could allow remote attacker to account takeover on the targeted device.	9.8	More Details
CVE-2022-45802	Streampark allows any users to upload a jar as application, but there is no mandatory verification of the uploaded file type, causing users to upload some high-risk files, and may upload them to any directory, Users of the affected versions should upgrade to Apache StreamPark 2.0.0 or later	9.8	More Details
CVE-2023-29635	File upload vulnerability in Antabot White-Jotter v0.2.2, allows remote attackers to execute malicious code via the file parameter to function coversUpload.	9.8	More Details
CVE-2022-35898	OpenText BizManager before 16.6.0.1 does not perform proper validation during the change-password operation. This allows any authenticated user to change the password of any other user, including the Administrator account.	9.8	More Details
CVE-2023-1730	The SupportCandy WordPress plugin before 3.1.5 does not validate and escape user input before using it in an SQL statement, which could allow unauthenticated attackers to perform SQL injection attacks	9.8	More Details
CVE-2023-30869	Improper Authentication vulnerability in Easy Digital Downloads plugin allows unauth. Privilege Escalation. This issue affects Easy Digital Downloads: from 3.1 through 3.1.1.4.1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29856	D-Link DIR-868L Hardware version A1, firmware version 1.12 is vulnerable to Buffer Overflow. The vulnerability is in scandir.sgi binary.	9.8	More Details
CVE-2023-2479	OS Command Injection in GitHub repository appium/appium-desktop prior to v1.22.3-4.	9.8	More Details
CVE-2023-26089	European Chemicals Agency IUCLID 6.x before 6.27.6 allows authentication bypass because a weak hard-coded secret is used for JWT signing. The affected versions are 5.15.0 through 6.27.5.	9.8	More Details
CVE-2022-41397	The optional Web Screens and Global Search features for Sage 300 through version 2022 use a hard-coded 40-byte blowfish key ("LandlordPassKey") to encrypt and decrypt secrets stored in configuration files and in database tables.	9.8	More Details
CVE-2023-1967	Keysight N8844A Data Analytics Web Service deserializes untrusted data without sufficiently verifying the resulting data will be valid.	9.8	More Details
CVE-2023-27843	SQL injection vulnerability found in PrestaShop askforaquote v.5.4.2 and before allow a remote attacker to gain privileges via the QuotesProduct::deleteProduct component.	9.8	More Details
CVE-2023-2158	Code Dx versions prior to 2023.4.2 are vulnerable to user impersonation attack where a malicious actor is able to gain access to another user's account by crafting a custom "Remember Me" token. This is possible due to the use of a hard-coded cipher which was used when generating the token. A malicious actor who creates this token can supply it to a separate Code Dx system, provided they know the username they want to impersonate, and impersonate the user. Score 6.7 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	9.8	More Details
CVE-2023-30404	Aigital Wireless-N Repeater Mini_Router v0.131229 was discovered to contain a remote code execution (RCE) vulnerability via the sysCmd parameter in the formSysCmd function. This vulnerability is exploited via a crafted HTTP request.	9.8	More Details
CVE-2023-24796	Password vulnerability found in Vinga WR-AC1200 81.102.1.4370 and before allows a remote attacker to execute arbitrary code via the password parameter at the /goform/sysTools and /adm/systools.asp endpoints.	9.8	More Details
CVE-2022-39989	An issue was discovered in Fighting Cock Information System 1.0, which uses default credentials, but does not force nor prompt the administrators to change the credentials.	9.8	More Details
CVE-2023-30211	OURPHP <= 7.2.0 is vulnerable to SQL Injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29268	The Splus Server component of TIBCO Software Inc.'s TIBCO Spotfire Statistics Services contains a vulnerability that allows an unauthenticated remote attacker to upload or modify arbitrary files within the web server directory on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Statistics Services: versions 11.4.10 and below, versions 11.5.0, 11.6.0, 11.6.1, 11.6.2, 11.7.0, 11.8.0, 11.8.1, 12.0.0, 12.0.1, and 12.0.2, versions 12.1.0 and 12.2.0.	9.8	More Details
CVE-2023-30546	Contiki-NG is an operating system for Internet of Things devices. An off-by-one error can be triggered in the Antelope database management system in the Contiki-NG operating system in versions 4.8 and prior. The problem exists in the Contiki File System (CFS) backend for the storage of data (file os/storage/antelope/storage-cfs.c). In the functions `storage_get_index` and `storage_put_index`, a buffer for merging two strings is allocated with one byte less than the maximum size of the merged strings, causing subsequent function calls to the cfs_open function to read from memory beyond the buffer size. The vulnerability has been patched in the "develop" branch of Contiki-NG, and is expected to be included in the next release. As a workaround, the problem can be fixed by applying the patch in Contiki-NG pull request #2425.	9.8	More Details
CVE-2020-36070	Insecure Permission vulnerability found in Yoyager v.1.4 and before allows a remote attacker to execute arbitrary code via a crafted .php file to the media component.	9.8	More Details
CVE-2023-30280	Buffer Overflow vulnerability found in Netgear R6900 v.1.0.2.26, R6700v3 v.1.0.4.128, R6700 v.1.0.0.26 allows a remote attacker to execute arbitrary code and cause a denial ofservice via the getInputData parameter of the fwSchedule.cgi page.	9.8	More Details
CVE-2023-30363	vConsole v3.15.0 was discovered to contain a prototype pollution due to incorrect key and value resolution in setOptions in core.ts.	9.8	More Details
CVE-2023-2297	The Profile Builder – User Profile & User Registration Forms plugin for WordPress is vulnerable to unauthorized password resets in versions up to, and including 3.9.0. This is due to the plugin using native password reset functionality, with insufficient validation on the password reset function (wppb_front_end_password_recovery). The function uses the plaintext value of a password reset key instead of a hashed value which means it can easily be retrieved and subsequently used. An attacker can leverage CVE-2023-0814, or another vulnerability like SQL Injection in another plugin or theme installed on the site to successfully exploit this vulnerability.	9.8	More Details
CVE-2022-47758	Nanoleaf firmware v7.1.1 and below is missing TLS verification, allowing attackers to execute arbitrary code via a DNS hijacking attack.	9.8	More Details
CVE-2023-20852	aEnrich Technology a+HRD has a vulnerability of Deserialization of Untrusted Data within its MSMQ interpreter. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands to perform arbitrary system operation or disrupt service.	9.8	More Details
CVE-2023-20853	aEnrich Technology a+HRD has a vulnerability of Deserialization of Untrusted Data within its MSMQ asynchronized message process. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands to perform arbitrary system operation or disrupt service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28697	Moxa MiiNePort E1 has a vulnerability of insufficient access control. An unauthenticated remote user can exploit this vulnerability to perform arbitrary system operation or disrupt service.	9.8	More Details
CVE-2023-28769	The buffer overflow vulnerability in the library “libclinkc.so” of the web server “zhttpd” in Zyxel DX5401-B0 firmware versions prior to V5.17(ABYO.1)C0 could allow a remote unauthenticated attacker to execute some OS commands or to cause denial-of-service (DoS) conditions on a vulnerable device.	9.8	More Details
CVE-2023-30349	JFinal CMS v5.1.0 was discovered to contain a remote code execution (RCE) vulnerability via the ActionEnter function.	9.8	More Details
CVE-2023-29778	GL.iNET MT3000 4.1.0 Release 2 is vulnerable to OS Command Injection via /usr/lib/oui-httpd/rpc/logread.	9.8	More Details
CVE-2023-30846	typed-rest-client is a library for Node Rest and Http Clients with typings for use with TypeScript. Users of the typed-rest-client library version 1.7.3 or lower are vulnerable to leak authentication data to 3rd parties. The flow of the vulnerability is as follows: First, send any request with `BasicCredentialHandler`, `BearerCredentialHandler` or `PersonalAccessTokenCredentialHandler`. Second, the target host may return a redirection (3xx), with a link to a second host. Third, the next request will use the credentials to authenticate with the second host, by setting the `Authorization` header. The expected behavior is that the next request will *NOT* set the `Authorization` header. The problem was fixed in version 1.8.0. There are no known workarounds.	9.1	More Details
CVE-2022-46365	Apache StreamPark 1.0.0 before 2.0.0 When the user successfully logs in, to modify his profile, the username will be passed to the server-layer as a parameter, but not verified whether the user name is the currently logged user and whether the user is legal, This will allow malicious attackers to send any username to modify and reset the account, Users of the affected versions should upgrade to Apache StreamPark 2.0.0 or later.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-30854	AVideo is an open source video platform. Prior to version 12.4, an OS Command Injection vulnerability in an authenticated endpoint `/plugin/CloneSite/cloneClient.json.php` allows attackers to achieve Remote Code Execution. This issue is fixed in version 12.4.	8.8	More Details
CVE-2023-29815	mccms v2.6.3 is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Details
CVE-2023-29150	mySCADA myPRO versions 8.26.0 and prior has parameters which an authenticated user could exploit to inject arbitrary operating system commands.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28716	mySCADA myPRO versions 8.26.0 and prior has parameters which an authenticated user could exploit to inject arbitrary operating system commands.	8.8	More Details
CVE-2023-28400	mySCADA myPRO versions 8.26.0 and prior has parameters which an authenticated user could exploit to inject arbitrary operating system commands.	8.8	More Details
CVE-2023-28384	mySCADA myPRO versions 8.26.0 and prior has parameters which an authenticated user could exploit to inject arbitrary operating system commands.	8.8	More Details
CVE-2023-25437	An issue was discovered in vTech VCS754 version 1.1.1.A before 1.1.1.H, allows attackers to gain escalated privileges and gain sensitive information due to cleartext passwords passed in the raw HTML.	8.8	More Details
CVE-2023-26546	European Chemicals Agency IUCLID before 6.27.6 allows remote authenticated users to execute arbitrary code via Server Side Template Injection (SSTI) with a crafted template file. The attacker must have template manager permission.	8.8	More Details
CVE-2022-47878	Incorrect input validation for the default-storage-path in the settings page in Jedox 2020.2.5 allows remote, authenticated users to specify the location as Webroot directory. Consecutive file uploads can lead to the execution of arbitrary code.	8.8	More Details
CVE-2023-1196	The Advanced Custom Fields (ACF) Free and Pro WordPress plugins 6.x before 6.1.0 and 5.x before 5.12.5 unserialize user controllable data, which could allow users with a role of Contributor and above to perform PHP Object Injection when a suitable gadget is present.	8.8	More Details
CVE-2022-47876	The integrator in Jedox GmbH Jedox 2020.2.5 allows remote authenticated users to create Jobs to execute arbitrary code via Groovy-scripts.	8.8	More Details
CVE-2022-47875	A Directory Traversal vulnerability in /be/erpc.php in Jedox GmbH Jedox 2020.2.5 allows remote authenticated users to execute arbitrary code.	8.8	More Details
CVE-2023-32007	** UNSUPPORTED WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022-33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30850	Pimcore is an open source data and experience management platform. Prior to version 10.5.21, a SQL Injection vulnerability exists in the admin translations API. Users should update to version 10.5.21 to receive a patch or, as a workaround, or apply the patch manually.	8.8	More Details
CVE-2023-30849	Pimcore is an open source data and experience management platform. Prior to version 10.5.21, A SQL injection vulnerability exists in the translation export API. Users should update to version 10.5.21 to receive a patch or, as a workaround, or apply the patch manually.	8.8	More Details
CVE-2023-30848	Pimcore is an open source data and experience management platform. Prior to version 10.5.21, the admin search find API has a SQL injection vulnerability. Users should upgrade to version 10.5.21 to receive a patch or, as a workaround, apply the patch manually.	8.8	More Details
CVE-2023-2338	SQL Injection in GitHub repository pimcore/pimcore prior to 10.5.21.	8.8	More Details
CVE-2023-24836	SUNNET CTMS has vulnerability of path traversal within its file uploading function. An authenticated remote attacker with general user privilege can exploit this vulnerability to upload and execute scripts onto arbitrary directories to perform arbitrary system operation or disrupt service.	8.8	More Details
CVE-2023-27107	Incorrect access control in the runReport function of MyQ Solution Print Server before 8.2 Patch 32 and Central Server before 8.2 Patch 22 allows users who do not have appropriate access rights to generate internal reports using a direct URL.	8.8	More Details
CVE-2023-31433	A SQL injection issue in Logbuch in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allows authenticated attackers to execute SQL statements via the welche parameter.	8.8	More Details
CVE-2023-29169	mySCADA myPRO versions 8.26.0 and prior has parameters which an authenticated user could exploit to inject arbitrary operating system commands.	8.8	More Details
CVE-2023-22919	The post-authentication command injection vulnerability in the Zyxel NBG6604 firmware version V1.01(ABIR.0)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request.	8.8	More Details
CVE-2023-24269	An arbitrary file upload vulnerability in the plugin upload function of Textpattern v4.8.8 allows attackers to execute arbitrary code via a crafted Zip file.	8.8	More Details
CVE-2022-30759	In Nokia One-NDS (aka Network Directory Server) through 20.9, some Sudo permissions can be exploited by some users to escalate to root privileges and execute arbitrary commands.	8.8	More Details
CVE-2023-0896	A default password was reported in Lenovo Smart Clock Essential with Alexa Built In that could allow unauthorized device access to an attacker with local network access.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30266	CLTPHP <=6.0 is vulnerable to Unrestricted Upload of File with Dangerous Type.	8.8	More Details
CVE-2023-21642	Memory corruption in HAB Memory management due to broad system privileges via physical address.	8.4	More Details
CVE-2023-21665	Memory corruption in Graphics while importing a file.	8.4	More Details
CVE-2023-21666	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	8.4	More Details
CVE-2023-28528	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands. IBM X-Force ID: 251207.	8.4	More Details
CVE-2022-41736	IBM Spectrum Scale Container Native Storage Access 5.1.2.1 through 5.1.6.0 contains an unspecified vulnerability that could allow a local user to obtain root privileges. IBM X-Force ID: 237810.	8.4	More Details
CVE-2023-26286	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX runtime services library to execute arbitrary commands. IBM X-Force ID: 248421.	8.4	More Details
CVE-2023-0683	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	8.3	More Details
CVE-2023-30856	eDEX-UI is a science fiction terminal emulator. Versions 2.2.8 and prior are vulnerable to cross-site websocket hijacking. When running eDEX-UI and browsing the web, a malicious website can connect to eDEX's internal terminal control websocket, and send arbitrary commands to the shell. The project has been archived since 2021, and as of time of publication there are no plans to patch this issue and release a new version. Some workarounds are available, including shutting down eDEX-UI when browsing the web and ensuring the eDEX terminal runs with lowest possible privileges.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30845	ESPv2 is a service proxy that provides API management capabilities using Google Service Infrastructure. ESPv2 2.20.0 through 2.42.0 contains an authentication bypass vulnerability. API clients can craft a malicious `X-HTTP-Method-Override` header value to bypass JWT authentication in specific cases. ESPv2 allows malicious requests to bypass authentication if both the conditions are true: The requested HTTP method is **not** in the API service definition (OpenAPI spec or gRPC `google.api.http` proto annotations, and the specified `X-HTTP-Method-Override` is a valid HTTP method in the API service definition. ESPv2 will forward the request to your backend without checking the JWT. Attackers can craft requests with a malicious `X-HTTP-Method-Override` value that allows them to bypass specifying JWTs. Restricting API access with API keys works as intended and is not affected by this vulnerability. Upgrade deployments to release v2.43.0 or higher to receive a patch. This release ensures that JWT authentication occurs, even when the caller specifies `x-http-method-override`. `x-http-method-override` is still supported by v2.43.0+. API clients can continue sending this header to ESPv2.	8.2	More Details
CVE-2022-40505	Information disclosure due to buffer over-read in Modem while parsing DNS hostname.	8.2	More Details
CVE-2023-30847	H2O is an HTTP server. In versions 2.3.0-beta2 and prior, when the reverse proxy handler tries to processes a certain type of invalid HTTP request, it tries to build an upstream URL by reading from uninitialized pointer. This behavior can lead to crashes or leak of information to back end HTTP servers. Pull request number 3229 fixes the issue. The pull request has been merged to the `master` branch in commit f010336. Users should upgrade to commit f010336 or later.	8.2	More Details
CVE-2023-31435	Multiple components (such as Onlinetemplate-Verwaltung, Liste aller Teilbereiche, Umfragen anzeigen, and questionnaire previews) in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allow authenticated attackers to read and write to unauthorized data by accessing functions directly.	8.1	More Details
CVE-2023-31484	CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.	8.1	More Details
CVE-2023-31486	HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN, has an insecure default TLS configuration where users must opt in to verify certificates.	8.1	More Details
CVE-2023-30269	CLTPHP <=6.0 is vulnerable to Improper Input Validation via application/admin/controller/Template.php.	8.1	More Details
CVE-2023-21712	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-26567	Sangoma FreePBX 1805 through 2302 (when obtained as a ,.ISO file) places AMPDBUSER, AMPDBPASS, AMPMGRUSER, and AMPMGRPASS in the list of global variables. This exposes cleartext authentication credentials for the Asterisk Database (MariaDB/MySQL) and Asterisk Manager Interface. For example, an attacker can make a /ari/asterisk/variable?variable=AMPDBPASS API call.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41739	IBM Spectrum Scale (IBM Spectrum Scale Container Native Storage Access 5.1.2.1 through 5.1.6.0) could allow programs running inside the container to overcome isolation mechanism and gain additional capabilities or access sensitive information on the host. IBM X-Force ID: 237815.	7.9	More Details
CVE-2023-2331	Unquoted service Path or Element vulnerability in 42Gears Surelock Windows SureLock Service (NixService.Exe) on Windows application will allows to insert arbitrary code into the service. This issue affects Surelock Windows : from 2.3.12 through 2.40.0.	7.8	More Details
CVE-2023-2236	A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Both io_install_fixed_file and its callers call fput in a file in case of an error, causing a reference underflow which leads to a use-after-free vulnerability. We recommend upgrading past commit 9d94c04c0db024922e886c9fd429659f22f48ea4.	7.8	More Details
CVE-2023-31287	An issue was discovered in Serenity Serene (and StartSharp) before 6.7.0. Password reset links are sent by email. A link contains a token that is used to reset the password. This token remains valid even after the password reset and can be used a second time to change the password of the corresponding user. The token expires only 3 hours after issuance and is sent as a query parameter when resetting. An attacker with access to the browser history can thus use the token again to change the password in order to take over the account.	7.8	More Details
CVE-2023-26246	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The AppUpgrade binary file, which is used during the firmware installation process, can be modified by an attacker to bypass the digital signature check. This indirectly allows an attacker to install custom firmware in the IVI system.	7.8	More Details
CVE-2023-26245	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The AppUpgrade binary file, which is used during the firmware installation process, can be modified by an attacker to bypass the version check in order to install any firmware version (e.g., newer, older, or customized). This indirectly allows an attacker to install custom firmware in the IVI system.	7.8	More Details
CVE-2022-37326	Docker Desktop for Windows before 4.6.0 allows attackers to delete (or create) any file through the dockerBackendV2 windowscontainers/start API by controlling the pidfile field inside the DaemonJSON field in the WindowsContainerStartRequest class. This can indirectly lead to privilege escalation.	7.8	More Details
CVE-2023-2235	A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation. The perf_group_detach function did not check the event's siblings' attach_state before calling add_event_to_groups(), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a dangling pointer causing a use-after-free vulnerability. We recommend upgrading past commit fd0815f632c24878e325821943edccc7fde947a2.	7.8	More Details
CVE-2023-2355	Local privilege escalation due to a DLL hijacking vulnerability. The following products are affected: Acronis Snap Deploy (Windows) before build 3900.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25496	A privilege escalation vulnerability was reported in Lenovo Drivers Management Lenovo Driver Manager that could allow a local user to execute code with elevated privileges.	7.8	More Details
CVE-2022-25713	Memory corruption in Automotive due to Improper Restriction of Operations within the Bounds of a Memory Buffer while exporting a shared key.	7.8	More Details
CVE-2022-33292	Memory corruption in Qualcomm IPC due to use after free while receiving the incoming packet and reposting it.	7.8	More Details
CVE-2023-26243	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The decryption binary used to decrypt firmware files has an information leak that allows an attacker to read the AES key and initialization vector from memory. An attacker may exploit this to create custom firmware that may be installed in the IVI system. Then, an attacker may be able to install a backdoor in the IVI system that may allow him to control it, if it is connected to the Internet through Wi-Fi.	7.8	More Details
CVE-2022-38583	On versions of Sage 300 2017 - 2022 (6.4.x - 6.9.x) which are setup in a "Windows Peer-to-Peer Network" or "Client Server Network" configuration, a low-privileged Sage 300 workstation user could abuse their access to the "SharedData" folder on the connected Sage 300 server to view and/or modify the credentials associated with Sage 300 users and SQL accounts to impersonate users and/or access the SQL database as a system administrator. With system administrator-level access to the Sage 300 MS SQL database it would be possible to create, update, and delete all records associated with the program and, depending on the configuration, execute code on the underlying database server.	7.8	More Details
CVE-2023-26244	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The AppDMClient binary file, which is used during the firmware installation process, can be modified by an attacker to bypass the digital signature check of AppUpgrade and .lge.upgrade.xml files, which are used during the firmware installation process. This indirectly allows an attacker to use a custom version of AppUpgrade and .lge.upgrade.xml files.	7.8	More Details
CVE-2023-31436	qfq_change_class in net/sched/sch_qfq.c in the Linux kernel before 6.2.13 allows an out-of-bounds write because lmax can exceed QFQ_MIN_LMAX.	7.8	More Details
CVE-2023-2291	Static credentials exist in the PostgreSQL data used in ManageEngine Access Manager Plus (AMP) build 4309, ManageEngine Password Manager Pro, and ManageEngine PAM360. These credentials could allow a malicious actor to modify configuration data that would escalate their permissions from that of a low-privileged user to an Administrative user.	7.8	More Details
CVE-2023-29835	Insecure Permission vulnerability found in Wondershare Dr.Fone v.12.9.6 allows a remote attacker to escalate privileges via the service permission function.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29596	Buffer Overflow vulnerability found in ByronKnoll Cmix v.19 allows an attacker to execute arbitrary code and cause a denial of service via the paq8 function.	7.8	More Details
CVE-2023-30853	Gradle Build Action allows users to execute a Gradle Build in their GitHub Actions workflow. A vulnerability impacts GitHub workflows using the Gradle Build Action prior to version 2.4.2 that have executed the Gradle Build Tool with the configuration cache enabled, potentially exposing secrets configured for the repository. Secrets configured for GitHub Actions are normally passed to the Gradle Build Tool via environment variables. Due to the way that the Gradle Build Tool records these environment variables, they may be persisted into an entry in the GitHub Actions cache. This data stored in the GitHub Actions cache can be read by a GitHub Actions workflow running in an untrusted context, such as that running for a Pull Request submitted by a developer via a repository fork. This vulnerability was discovered internally through code review, and we have not seen any evidence of it being exploited in the wild. However, in addition to upgrading the Gradle Build Action, affected users should delete any potentially vulnerable cache entries and may choose to rotate any potentially affected secrets. Gradle Build Action v2.4.2 and newer no longer saves this sensitive data for later use, preventing ongoing leakage of secrets via the GitHub Actions Cache. While upgrading to the latest version of the Gradle Build Action will prevent leakage of secrets going forward, additional actions may be required due to current or previous GitHub Actions Cache entries containing this information. Current cache entries will remain vulnerable until they are forcibly deleted or they expire naturally after 7 days of not being used. Potentially vulnerable entries can be easily identified in the GitHub UI by searching for a cache entry with key matching `configuration-cache-*`. The maintainers recommend that users of the Gradle Build Action inspect their list of cache entries and manually delete any that match this pattern. While maintainers have not seen any evidence of this vulnerability being exploited, they recommend cycling any repository secrets if you cannot be certain that these have not been compromised. Compromise could occur if a user runs a GitHub Actions workflow for a pull request attempting to exploit this data. Warning signs to look for in a pull request include: - Making changes to GitHub Actions workflow files in a way that may attempt to read/extract data from the Gradle User Home or `<project-root>/.gradle` directories. - Making changes to Gradle build files or other executable files that may be invoked by a GitHub Actions workflow, in a way that may attempt to read/extract information from these locations. Some workarounds to limit the impact of this vulnerability are available: - If the Gradle project does not opt-in to using the configuration cache, then it is not vulnerable. - If the Gradle project does opt-in to using the configuration-cache by default, then the `--no-configuration-cache` command-line argument can be used to disable this feature in a GitHub Actions workflow. In any case, we recommend that users carefully inspect any pull request before approving the execution of GitHub Actions workflows. It may be prudent to require approval for all PRs from external contributors.	7.6	More Details
CVE-2023-2360	Sensitive information disclosure due to CORS misconfiguration. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.2.0-135.	7.5	More Details
CVE-2022-33304	Transient DOS due to NULL pointer dereference in Modem while performing pullup for received TCP/UDP packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48483	3CX before 18 Hotfix 1 build 18.0.3.461 on Windows allows unauthenticated remote attackers to read %WINDIR%\system32 files via /Electron/download directory traversal in conjunction with a path component that has a drive letter and uses backslash characters. NOTE: this issue exists because of an incomplete fix for CVE-2022-28005.	7.5	More Details
CVE-2023-30467	This vulnerability exists in Milesight 4K/H.265 Series NVR models (MS-Nxxxx-xxG, MS-Nxxxx-xxE, MS-Nxxxx-xxT, MS-Nxxxx-xxH and MS-Nxxxx-xxC), due to improper authorization at the Milesight NVR web-based management interface. A remote attacker could exploit this vulnerability by sending a specially crafted http requests on the targeted device. Successful exploitation of this vulnerability could allow remote attacker to perform unauthorized activities on the targeted device.	7.5	More Details
CVE-2022-25275	In some situations, the Image module does not correctly check access to image files not stored in the standard public files directory when generating derivative images using the image styles system. Access to a non-public file is checked only if it is stored in the "private" file system. However, some contributed modules provide additional file systems, or schemes, which may lead to this vulnerability. This vulnerability is mitigated by the fact that it only applies when the site sets (Drupal 9) $config['image.settings']['allow_insecure_derivatives'] or (Drupal 7) $conf['image_allow_insecure_derivatives'] to TRUE. The recommended and default setting is FALSE, and Drupal core does not provide a way to change that in the admin UI. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing files or image styles after updating.	7.5	More Details
CVE-2023-31444	In Talend Studio before 7.3.1-R2022-10 and 8.x before 8.0.1-R2022-09, microservices allow unauthenticated access to the Jolokia endpoint of the microservice. This allows for remote access to the JVM via the Jolokia JMX-HTTP bridge.	7.5	More Details
CVE-2022-34144	Transient DOS due to reachable assertion in Modem during OSI decode scheduling.	7.5	More Details
CVE-2022-33305	Transient DOS due to NULL pointer dereference in Modem while sending invalid messages in DCCH.	7.5	More Details
CVE-2023-22921	A cross-site scripting (XSS) vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to store malicious scripts using a web management interface parameter, resulting in denial-of-service (DoS) conditions on an affected device.	7.5	More Details
CVE-2023-28882	Trustwave ModSecurity 3.0.5 through 3.0.8 before 3.0.9 allows a denial of service (worker crash and unresponsiveness) because some inputs cause a segfault in the Transaction class for some configurations.	7.5	More Details
CVE-2022-40508	Transient DOS due to reachable assertion in Modem while processing config related to cross carrier scheduling, which is not supported.	7.5	More Details
CVE-2022-45456	Denial of service due to unauthenticated API endpoint. The following products are affected: Acronis Agent (Windows, macOS, Linux) before build 30161.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22922	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote unauthenticated attacker to cause DoS conditions by sending crafted packets if Telnet is enabled on a vulnerable device.	7.5	More Details
CVE-2023-30112	Medicine Tracker System in PHP 1.0.0 is vulnerable to SQL Injection.	7.5	More Details
CVE-2023-30455	An issue was discovered in ebankIT before 7. A Denial-of-Service attack is possible through the GET parameter EStatementsIds located on the /Controls/Generic/EBMK/Handlers/EStatements/DownloadEStatement.ashx endpoint. The GET parameter accepts over 100 comma-separated e-statement IDs without throwing an error. When this many IDs are supplied, the server takes around 60 seconds to respond and successfully generate the expected ZIP archive (during this time period, no other pages load). A threat actor could issue a request to this endpoint with 100+ statement IDs every 30 seconds, potentially resulting in an overload of the server for all users.	7.5	More Details
CVE-2023-1809	The Download Manager WordPress plugin before 6.3.0 leaks master key information without the need for a password, allowing attackers to download arbitrary password-protected package files.	7.5	More Details
CVE-2023-2356	Relative Path Traversal in GitHub repository mlflow/mlflow prior to 2.3.1.	7.5	More Details
CVE-2023-30403	An issue in the time-based authentication mechanism of Aigital Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to bypass login by connecting to the web app after a successful attempt by a legitimate user.	7.5	More Details
CVE-2022-48482	3CX before 18 Update 2 Security Hotfix build 18.0.2.315 on Windows allows unauthenticated remote attackers to read certain files via /Electron/download directory traversal. Files may have credentials, full backups, call recordings, and chat logs.	7.5	More Details
CVE-2022-44232	libming 0.4.8 0.4.8 is vulnerable to Buffer Overflow. In getInt() in decompile.c unknown type may lead to denial of service. This is a different vulnerability than CVE-2018-9132 and CVE-2018-20427.	7.5	More Details
CVE-2023-30380	An issue in the component /dialog/select_media.php of DedeCMS v5.7.107 allows attackers to execute a directory traversal.	7.5	More Details
CVE-2023-2379	A vulnerability classified as critical has been found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6. This affects an unknown part of the component Web Service. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227655.	7.5	More Details
CVE-2023-26021	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to a denial of service as the server may crash when compiling a specially crafted SQL query using a LIMIT clause. IBM X-Force ID: 247864.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41398	The optional Global Search feature for Sage 300 through version 2022 uses a set of hard-coded credentials for the accompanying Apache Solr instance. This issue could allow attackers to login to the Solr dashboard with admin privileges and access sensitive information.	7.5	More Details
CVE-2023-29255	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as it may trap when compiling a variation of an anonymous block. IBM X-Force ID: 251991.	7.5	More Details
CVE-2023-31483	tar/TarFileReader.cpp in Cauldron cbang before bastet-v8.1.17 has a directory traversal during extraction that allows the attacker to create or write to files outside the current directory via a crafted tar archive.	7.5	More Details
CVE-2023-30441	IBM Runtime Environment, Java Technology Edition IBMJCEPlus and JSSE 8.0.7.0 through 8.0.7.11 components could expose sensitive information using a combination of flaws and configurations. IBM X-Force ID: 253188.	7.5	More Details
CVE-2022-27978	Tooljet v1.6 does not properly handle missing values in the API, allowing attackers to arbitrarily reset passwords via a crafted HTTP request.	7.5	More Details
CVE-2022-40504	Transient DOS due to reachable assertion in Modem when UE received Downlink Data Indication message from the network.	7.5	More Details
CVE-2023-26735	blackbox_exporter v0.23.0 was discovered to contain an access control issue in its probe interface. This vulnerability allows attackers to detect intranet ports and services, as well as download resources. NOTE: this is disputed by third parties because authentication can be configured.	7.5	More Details
CVE-2023-30061	D-Link DIR-879 v105A1 is vulnerable to Authentication Bypass via phpcgi.	7.5	More Details
CVE-2023-30861	Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response containing data intended for one client may be cached and subsequently sent by the proxy to other clients. If the proxy also caches `Set-Cookie` headers, it may send one client's `session` cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior regarding cookies. The risk depends on all these conditions being met. 1. The application must be hosted behind a caching proxy that does not strip cookies or ignore responses with cookies. 2. The application sets `session.permanent = True` 3. The application does not access or modify the session at any point during a request. 4. `SESSION_REFRESH_EACH_REQUEST` enabled (the default). 5. The application does not set a `Cache-Control` header to indicate that a page is private or should not be cached. This happens because vulnerable versions of Flask only set the `Vary: Cookie` header when the session is accessed or modified, not when it is refreshed (re-sent to update the expiration) without being accessed or modified. This issue has been fixed in versions 2.3.2 and 2.2.5.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25273	Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.	7.5	More Details
CVE-2023-30063	D-Link DIR-890L FW1.10 A1 is vulnerable to Authentication bypass.	7.5	More Details
CVE-2022-41399	The optional Web Screens feature for Sage 300 through version 2022 uses a hard-coded 40-byte blowfish key ("PASS_KEY") to encrypt and decrypt the database connection string for the PORTAL database found in the "dbconfig.xml". This issue could allow attackers to obtain access to the SQL database.	7.5	More Details
CVE-2023-28770	The sensitive information exposure vulnerability in the CGI “Export_Log” and the binary “zcmd” in Zyxel DX5401-B0 firmware versions prior to V5.17(ABYO.1)C0 could allow a remote unauthenticated attacker to read the system files and to retrieve the password of the supervisor from the encrypted file.	7.5	More Details
CVE-2023-30843	Payload is a free and open source headless content management system. In versions prior to 1.7.0, if a user has access to documents that contain hidden fields or fields they do not have access to, the user could reverse-engineer those values via brute force. Version 1.7.0 contains a patch. As a workaround, write a `beforeOperation` hook to remove `where` queries that attempt to access hidden field data.	7.4	More Details
CVE-2023-1966	Instruments with Illumina Universal Copy Service v1.x and v2.x contain an unnecessary privileges vulnerability. An unauthenticated malicious actor could upload and execute code remotely at the operating system level, which could allow an attacker to change settings, configurations, software, or access sensitive data on the affected product.	7.4	More Details
CVE-2022-33273	Information disclosure due to buffer over-read in Trusted Execution Environment while QRKS report generation.	7.3	More Details
CVE-2023-29057	A valid XCC user's local account permissions overrides their active directory permissions under specific configurations. This could lead to a privilege escalation. To be vulnerable, LDAP must be configured for authentication/authorization and logins configured as “Local First, then LDAP”.	7.3	More Details
CVE-2022-36769	IBM Cloud Pak for Data 4.5 and 4.6 could allow a privileged user to upload malicious files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 232034.	7.2	More Details
CVE-2023-1477	Improper Authentication vulnerability in HYPR Keycloak Authenticator Extension allows Authentication Abuse.This issue affects HYPR Keycloak Authenticator Extension: before 7.10.2, before 8.0.3.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25277	Drupal core sanitizes filenames with dangerous extensions upon upload (reference: SA-CORE-2020-012) and strips leading and trailing dots from filenames to prevent uploading server configuration files (reference: SA-CORE-2019-010). However, the protections for these two vulnerabilities previously did not work correctly together. As a result, if the site were configured to allow the upload of files with an htaccess extension, these files' filenames would not be properly sanitized. This could allow bypassing the protections provided by Drupal core's default .htaccess files and possible remote code execution on Apache web servers. This issue is mitigated by the fact that it requires a field administrator to explicitly configure a file field to allow htaccess as an extension (a restricted permission), or a contributed module or custom code that overrides allowed file uploads.	7.2	More Details
CVE-2023-0924	The ZYREX POPUP WordPress plugin through 1.0 does not validate the type of files uploaded when creating a popup, allowing a high privileged user (such as an Administrator) to upload arbitrary files, even when modifying the file system is disallowed, such as in a multisite install.	7.2	More Details
CVE-2023-29257	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to remote code execution as a database administrator of one database may execute code or read/write files from another database within the same instance. IBM X-Force ID: 252011.	7.2	More Details
CVE-2023-1669	The SEOPress WordPress plugin before 6.5.0.3 unserializes user input provided via the settings, which could allow high-privilege users such as admin to perform PHP Object Injection when a suitable gadget is present.	7.2	More Details
CVE-2023-30859	Triton is a Minecraft plugin for Spigot and BungeeCord that helps you translate your Minecraft server. The CustomPayload packet allows you to execute commands on the spigot/bukkit console. When you enable bungee mode in the config it will enable the bungee bridge and the server will begin to broadcast the 'triton:main' plugin channel. Using this plugin channel you are able to send a payload packet containing a byte (2) and a string (any spigot command). This could be used to make yourself a server operator and be used to extract other user information through phishing (pretending to be an admin), many servers use essentials so the /geoip command could be available to them, etc. This could also be modified to allow you to set the servers language, set another players language, etc. This issue affects those who have bungee enabled in config. This issue has been fixed in version 3.8.4.	7.2	More Details
CVE-2022-31647	Docker Desktop before 4.6.0 on Windows allows attackers to delete any file through the hyperv/destroy dockerBackendV2 API via a symlink in the DataFolder parameter, a different vulnerability than CVE-2022-26659.	7.1	More Details
CVE-2022-34292	Docker Desktop for Windows before 4.6.0 allows attackers to overwrite any file through a symlink attack on the hyperv/create dockerBackendV2 API by controlling the DataFolder parameter for DockerDesktop.vhdx, a similar issue to CVE-2022-31647.	7.1	More Details
CVE-2023-28008	HCL Workload Automation 9.4, 9.5, and 10.1 are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30639	Archer Platform 6.8 before 6.12 P6 HF1 (6.12.0.6.1) contains a stored XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. 6.11.P4 (6.11.0.4) is also a fixed release.	7.1	More Details
CVE-2023-30444	IBM Watson Machine Learning on Cloud Pak for Data 4.0 and 4.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 253350.	7.1	More Details
CVE-2023-0834	Incorrect Permission Assignment for Critical Resource vulnerability in HYPR Workforce Access on MacOS allows Privilege Escalation.This issue affects Workforce Access: from 6.12 before 8.1.	7.0	More Details
CVE-2022-4568	A directory permissions management vulnerability in Lenovo System Update may allow elevation of privileges.	7.0	More Details
CVE-2022-33281	Memory corruption due to improper validation of array index in computer vision while testing EVA kernel without sending any frames.	6.7	More Details
CVE-2023-30024	The MagicJack device, a VoIP solution for internet phone calls, contains a hidden NAND flash memory partition allowing unauthorized read/write access. Attackers can exploit this by replacing the original software with a malicious version, leading to ransomware deployment on the host computer. Affected devices have firmware versions prior to magicJack A921 USB Phone Jack Rev 3.0 V1.4.	6.6	More Details
CVE-2023-30943	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system.	6.5	More Details
CVE-2023-29867	Zammad 5.3.x (Fixed 5.4.0) is vulnerable to Incorrect Access Control. An authenticated attacker could gain information about linked accounts of users involved in their tickets using the Zammad API.	6.5	More Details
CVE-2022-47874	Improper Access Control in /tc/rpc in Jedox GmbH Jedox 2020.2.5 allows remote authenticated users to view details of database connections via class 'com.jedox.etl.mngr.Connections' and method 'getGlobalConnection'.	6.5	More Details
CVE-2023-2336	Path Traversal in GitHub repository pimcore/pimcore prior to 10.5.21.	6.5	More Details
CVE-2023-1125	The Ruby Help Desk WordPress plugin before 1.3.4 does not ensure that the ticket being modified belongs to the user making the request, allowing an attacker to close and/or add files and replies to tickets other than their own.	6.5	More Details
CVE-2023-26560	Northern.tech CFEngine Enterprise before 3.21.1 allows a subset of authenticated users to leverage the Scheduled Reports feature to read arbitrary files and potentially discover credentials.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26782	An issue discovered in mccms 2.6.1 allows remote attackers to cause a denial of service via Backend management interface ->System Configuration->Cache Configuration->Cache security characters.	6.5	More Details
CVE-2023-2380	A vulnerability, which was classified as problematic, was found in Netgear SRX5308 up to 4.3.5-3. Affected is an unknown function. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-227658 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2023-29868	Zammad 5.3.x (Fixed in 5.4.0) is vulnerable to Incorrect Access Control. An authenticated attacker with agent and customer roles could perform unauthorized changes on articles where they only have customer permissions.	6.5	More Details
CVE-2023-27035	An issue discovered in Obsidian Canvas 1.1.9 allows remote attackers to send desktop notifications, record user audio and other unspecified impacts via embedded website on the canvas page.	6.5	More Details
CVE-2023-28009	HCL Workload Automation is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	6.5	More Details
CVE-2023-30265	CLTPHP <=6.0 is vulnerable to Directory Traversal.	6.5	More Details
CVE-2023-2335	Plaintext Password in Registry vulnerability in 42gears surelock windows surelockwinsetupv2.40.0.Exe on Windows (Registery modules) allows Retrieve Admin user credentials This issue affects surelock windows: from 2.3.12 through 2.40.0.	6.5	More Details
CVE-2022-25278	Under certain circumstances, the Drupal core form API evaluates form element access incorrectly. This may lead to a user being able to alter data they should not have access to. No forms provided by Drupal core are known to be vulnerable. However, forms added through contributed or custom modules or themes may be affected.	6.5	More Details
CVE-2023-27556	IBM Counter Fraud Management for Safer Payments 6.1.0.00, 6.2.0.00, 6.3.0.00 through 6.3.1.03, 6.4.0.00 through 6.4.2.02 and 6.5.0.00 does not properly allocate resources without limits or throttling which could allow a remote attacker to cause a denial of service. IBM X-Force ID: 249190.	6.5	More Details
CVE-2023-22923	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker to cause denial-of-service (DoS) conditions on an affected device.	6.5	More Details
CVE-2023-26987	An issue discovered in Konga 0.14.9 allows remote attackers to manipulate user accounts regardless of privilege via crafted POST request.	6.5	More Details
CVE-2023-31250	The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29058	A valid, authenticated XCC user with read-only permissions can modify custom user roles on other user accounts and the user trespass message through the XCC CLI. There is no exposure if SSH is disabled or if there are no users assigned optional read-only permissions.	6.4	More Details
CVE-2023-2377	A vulnerability was found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Web Management Interface. The manipulation of the argument name leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227653 was assigned to this vulnerability.	6.3	More Details
CVE-2015-10105	A vulnerability, which was classified as critical, was found in IP Blacklist Cloud Plugin up to 3.42 on WordPress. This affects the function valid_js_identifier of the file ip_blacklist_cloud.php of the component CSV File Import. The manipulation of the argument filename leads to path traversal. It is possible to initiate the attack remotely. Upgrading to version 3.43 is able to address this issue. The identifier of the patch is 6e6fe8c6fda7cbc252eef083105e08d759c07312. It is recommended to upgrade the affected component. The identifier VDB-227757 was assigned to this vulnerability.	6.3	More Details
CVE-2023-25492	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	6.3	More Details
CVE-2023-2374	A vulnerability has been found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6 and classified as critical. This vulnerability affects unknown code of the component Web Management Interface. The manipulation of the argument ecn-down leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227650 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2375	A vulnerability was found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6 and classified as critical. This issue affects some unknown processing of the component Web Management Interface. The manipulation of the argument src leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227651.	6.3	More Details
CVE-2023-2376	A vulnerability was found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6. It has been classified as critical. Affected is an unknown function of the component Web Management Interface. The manipulation of the argument dpi leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227652.	6.3	More Details
CVE-2023-2420	A vulnerability was found in MLECMS 3.0. It has been rated as critical. This issue affects the function get_url in the library /upload/inc/lib/admin of the file upload\inc\include\common.func.php. The manipulation of the argument $_SERVER['REQUEST_URI'] 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-227717 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2378	A vulnerability was found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6. It has been rated as critical. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation of the argument suffix-rate-up leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-227654 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2424	A vulnerability was found in DedeCMS 5.7.106 and classified as critical. Affected by this issue is the function UpDateMemberModCache of the file uploads/dede/config.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-227750 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2451	A vulnerability was found in SourceCodester Online DJ Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/bookings/view_details.php of the component GET Parameter 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 associated identifier of this vulnerability is VDB-227795.	6.3	More Details
CVE-2023-2413	A vulnerability was found in SourceCodester AC Repair and Services System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/bookings/manage_booking.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227707.	6.3	More Details
CVE-2023-2412	A vulnerability was found in SourceCodester AC Repair and Services System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-227706 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2410	A vulnerability has been found in SourceCodester AC Repair and Services System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/bookings/view_booking.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227704.	6.3	More Details
CVE-2023-2409	A vulnerability, which was classified as critical, was found in SourceCodester AC Repair and Services System 1.0. This affects an unknown part of the file /admin/services/view_service.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227703.	6.3	More Details
CVE-2023-2408	A vulnerability, which was classified as critical, has been found in SourceCodester AC Repair and Services System 1.0. Affected by this issue is some unknown functionality of the file services/view.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-227702 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2411	A vulnerability was found in SourceCodester AC Repair and Services System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/inquiries/view_inquiry.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227705 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2371	A vulnerability classified as critical was found in SourceCodester Online DJ Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/inquiries/view_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227647.	6.3	More Details
CVE-2023-2344	A vulnerability has been found in SourceCodester Service Provider Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=save_service of the component HTTP POST Request Handler. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227587.	6.3	More Details
CVE-2023-2366	A vulnerability was found in SourceCodester Faculty Evaluation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file ajax.php?action=delete_class. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-227642 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2373	A vulnerability, which was classified as critical, was found in Ubiquiti EdgeRouter X up to 2.0.9-hotfix.6. This affects an unknown part of the component Web Management Interface. The manipulation of the argument ecn-up leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227649 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2370	A vulnerability classified as critical has been found in SourceCodester Online DJ Management System 1.0. Affected is an unknown function of the file admin/events/manage_event.php of the component GET Parameter 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-227646 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-38730	Docker Desktop for Windows before 4.6 allows attackers to overwrite any file through the windowscontainers/start dockerBackendV2 API by controlling the data-root field inside the DaemonJSON field in the WindowsContainerStartRequest class. This allows exploiting a symlink vulnerability in ..\dataRoot\network\files\local-kv.db because of a TOCTOU race condition.	6.3	More Details
CVE-2023-2348	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227591.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2363	A vulnerability, which was classified as critical, has been found in SourceCodester Resort Reservation System 1.0. This issue affects some unknown processing of the file view_room.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227639.	6.3	More Details
CVE-2023-2347	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/services/manage_service.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227590 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2346	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/inquiries/view_inquiry.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-227589 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2365	A vulnerability has been found in SourceCodester Faculty Evaluation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file ajax.php?action=delete_subject. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227641 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2345	A vulnerability was found in SourceCodester Service Provider Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=delete_inquiry. The manipulation leads to improper authorization. The attack may be launched remotely. The identifier of this vulnerability is VDB-227588.	6.3	More Details
CVE-2022-48186	A certificate validation vulnerability exists in the Baiying Android application which could lead to information disclosure.	6.2	More Details
CVE-2020-23647	Cross Site Scripting (XSS) vulnerability in BoxBilling 4.19, 4.19.1, 4.20, and 4.21 allows remote attackers to run arbitrary code via the message field on the submit new ticket form.	6.1	More Details
CVE-2023-30125	EyouCms V1.6.1-UTF8-sp1 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-29836	Cross Site Scripting vulnerability found in Exelysis Unified Communication Solutions (EUCS) v.1.0 allows a remote attacker to execute arbitrary code via the Username parameter of the eucsAdmin login form.	6.1	More Details
CVE-2023-29641	Cross Site Scripting (XSS) vulnerability in pandao editor.md thru 1.5.0 allows attackers to inject arbitrary web script or HTML via crafted markdown text.	6.1	More Details
CVE-2023-28286	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30454	An issue was discovered in ebankIT before 7. Document Object Model based XSS exists within the /Security/Transactions/Transactions.aspx endpoint. Users can supply their own JavaScript within the ctl100$ctl00MainContent$TransactionMainContent$accControl$hdnAccountsArray POST parameter that will be passed to an eval() function and executed upon pressing the continue button.	6.1	More Details
CVE-2023-2341	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.21.	6.1	More Details
CVE-2023-24966	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246904.	6.1	More Details
CVE-2023-29637	Cross Site Scripting (XSS) vulnerability in Qbian61 forum-java, allows attackers to inject arbitrary web script or HTML via editing the article content in the "article editor" page.	6.1	More Details
CVE-2023-28092	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	6.1	More Details
CVE-2023-30792	Anchor tag hrefs in Lexical prior to v0.10.0 would render javascript: URLs, allowing for cross-site scripting on link clicks in cases where input was being parsed from untrusted sources.	6.1	More Details
CVE-2023-29442	Zoho ManageEngine Applications Manager before 16400 allows proxy.html DOM XSS.	6.1	More Details
CVE-2023-30111	Medicine Tracker System in PHP 1.0.0 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-30106	Sourcecodester Medicine Tracker System in PHP 1.0.0 is vulnerable to Cross Site Scripting (XSS) via page=about.	6.1	More Details
CVE-2023-31285	An XSS issue was discovered in Serenity Serene (and StartSharp) before 6.7.0. When users upload temporary files, some specific file endings are not allowed, but it is possible to upload .html or .htm files containing an XSS payload. The resulting link can be sent to an administrator user.	6.1	More Details
CVE-2020-21643	Cross Site Scripting (XSS) vulnerability in HongCMS 3.0 allows attackers to run arbitrary code via the callback parameter to /ajax/myshop.	6.1	More Details
CVE-2023-25292	Reflected Cross Site Scripting (XSS) in Intermesh BV Group-Office version 6.6.145, allows attackers to gain escalated privileges and gain sensitive information via the GO_LANGUAGE cookie.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30267	CLTPHP <=6.0 is vulnerable to Cross Site Scripting (XSS) via application/home/controller/Changyan.php.	6.1	More Details
CVE-2023-30212	OURPHP <= 7.2.0 is vulnerale to Cross Site Scripting (XSS) via /client/manage/ourphp_out.php.	6.1	More Details
CVE-2023-1804	The Product Catalog Feed by PixelYourSite WordPress plugin before 2.1.1 does not sanitise and escape the edit parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as administrators.	6.1	More Details
CVE-2023-1546	The MyCryptoCheckout WordPress plugin before 2.124 does not escape some URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2023-28475	Concrete CMS (previously concrete5) versions 8.5.12 and below, and versions 9.0 through 9.1.3 is vulnerable to Reflected XSS on the Reply form because msgID was not sanitized.	6.1	More Details
CVE-2022-25276	The Media oEmbed iframe route does not properly validate the iframe domain setting, which allows embeds to be displayed in the context of the primary domain. Under certain circumstances, this could lead to cross-site scripting, leaked cookies, or other vulnerabilities.	6.1	More Details
CVE-2023-1805	The Product Catalog Feed by PixelYourSite WordPress plugin before 2.1.1 does not sanitise and escape the page parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-30210	OURPHP <= 7.2.0 is vulnerable to Cross Site Scripting (XSS) via ourphp_tz.php.	6.1	More Details
CVE-2023-30841	Baremetal Operator (BMO) is a bare metal host provisioning integration for Kubernetes. Prior to version 0.3.0, ironic and ironic-inspector deployed within Baremetal Operator using the included `deploy.sh` store their `.htpasswd` files as ConfigMaps instead of Secrets. This causes the plain-text username and hashed password to be readable by anyone having a cluster-wide read-access to the management cluster, or access to the management cluster's Etcd storage. This issue is patched in baremetal-operator PR#1241, and is included in BMO release 0.3.0 onwards. As a workaround, users may modify the kustomizations and redeploy the BMO, or recreate the required ConfigMaps as Secrets per instructions in baremetal-operator PR#1241.	6.0	More Details
CVE-2023-23723	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media WP Email Capture plugin <= 3.9.3 versions.	5.9	More Details
CVE-2023-25930	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 11.1, and 11.5 is vulnerable to a denial of service. Under rare conditions, setting a special register may cause the Db2 server to terminate abnormally. IBM X-Force ID: 247862.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26022	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server may crash when an Out of Memory occurs using the DBMS_OUTPUT module. IBM X-Force ID: 247868.	5.9	More Details
CVE-2023-27557	IBM Counter Fraud Management for Safer Payments 6.1.0.00 through 6.1.1.02, 6.2.0.00 through 6.2.2.02, 6.3.0.00 through 6.3.1.02, 6.4.0.00 through 6.4.2.01, and 6.5.0.00 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 249192.	5.9	More Details
CVE-2023-31485	GitLab::API::v4 through 0.26 does not verify TLS certificates when connecting to a GitLab server, enabling machine-in-the-middle attacks.	5.9	More Details
CVE-2023-31290	Trust Wallet Core before 3.1.1, as used in the Trust Wallet browser extension before 0.0.183, allows theft of funds because the entropy is 32 bits, as exploited in the wild in December 2022 and March 2023. This occurs because the mt19937 Mersenne Twister takes a single 32-bit value as an input seed, resulting in only four billion possible mnemonics. The affected versions of the browser extension are 0.0.172 through 0.0.182. To steal funds efficiently, an attacker can identify all Ethereum addresses created since the 0.0.172 release, and check whether they are Ethereum addresses that could have been created by this extension. To respond to the risk, affected users need to upgrade the product version and also move funds to a new wallet address.	5.9	More Details
CVE-2023-2273	Rapid7 Insight Agent token handler versions 3.2.6 and below, suffer from a Directory Traversal vulnerability whereby unsanitized input from a CLI argument flows into io.ioutil.WriteFile, where it is used as a path. This can result in a Path Traversal vulnerability and allow an attacker to write arbitrary files. This issue is remediated in version 3.3.0 via safe guards that reject inputs that attempt to do path traversal.	5.8	More Details
CVE-2023-29680	Cleartext Transmission in set-cookie:ecos_pw: Tenda N301 v6.0, Firmware v12.02.01.61_multi allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password.	5.7	More Details
CVE-2023-29681	Cleartext Transmission in cookie:ecos_pw: in Tenda N301 v6.0, firmware v12.03.01.06_pt allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password.	5.7	More Details
CVE-2023-28261	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	5.7	More Details
CVE-2023-30944	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database.	5.6	More Details
CVE-2023-29950	swfrender v0.9.2 was discovered to contain a heap buffer overflow in the function enumerateUsedIDs_fillstyle at modules/swftools.c	5.5	More Details
CVE-2023-29471	Lightbend Alpakka Kafka before 5.0.0 logs its configuration as debug information, and thus log files may contain credentials (if plain cleartext login is configured). This occurs in akka.kafka.internal.KafkaConsumerActor.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45876	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.	5.5	More Details
CVE-2023-2426	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 9.0.1499.	5.5	More Details
CVE-2023-26930	Buffer Overflow vulnerability found in XPDF v.4.04 allows an attacker to cause a Denial of Service via the PDFDoc malloc in the pdftotext.cc function. NOTE: Vendor states “it's an expected abort on out-of-memory error.”	5.5	More Details
CVE-2022-31643	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which may allow loss of integrity. HP is releasing firmware updates to mitigate the potential vulnerability.	5.5	More Details
CVE-2023-28477	Concrete CMS (previously concrete5) versions 8.5.12 and below, and 9.0 through 9.1.3 is vulnerable to stored XSS on API Integrations via the name parameter.	5.5	More Details
CVE-2023-1786	Sensitive data could be exposed in logs of cloud-init before version 23.1.2. An attacker could use this information to find hashed passwords and possibly escalate their privilege.	5.5	More Details
CVE-2023-29636	Cross site scripting (XSS) vulnerability in ZHENFENG13 My-Blog, allows attackers to inject arbitrary web script or HTML via the "title" field in the "blog management" page due to the the default configuration not using MyBlogUtils.cleanString.	5.4	More Details
CVE-2023-22729	Silverstripe Framework is the Model-View-Controller framework that powers the Silverstripe content management system. Prior to version 4.12.15, an attacker can display a link to a third party website on a login screen by convincing a legitimate content author to follow a specially crafted link. Users should upgrade to Silverstripe Framework 4.12.15 or above to address the issue.	5.4	More Details
CVE-2023-28474	Concrete CMS (previously concrete5) in versions 9.0 through 9.1.3 is vulnerable to Stored XSS on Saved Presets on search.	5.4	More Details
CVE-2023-29918	RosarioSIS 10.8.4 is vulnerable to CSV injection via the Periods Module.	5.4	More Details
CVE-2023-0891	The StagTools WordPress plugin before 2.3.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-2322	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-28476	Concrete CMS (previously concrete5) in versions 9.0 through 9.1.3 is vulnerable to Stored XSS on Tags on uploaded files.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2328	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-2327	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-2428	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.13.	5.4	More Details
CVE-2023-2323	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-2339	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2022-27979	A cross-site scripting (XSS) vulnerability in ToolJet v1.6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comment Body component.	5.4	More Details
CVE-2023-29638	Cross Site Scripting (XSS) vulnerability in WinterChenS my-site before commit 3f0423da6d5200c7a46e200da145c1f54ee18548, allows attackers to inject arbitrary web script or HTML via editing blog articles.	5.4	More Details
CVE-2023-29639	Cross site scripting (XSS) vulnerability in ZHENFENG13 My-Blog, allows attackers to inject arbitrary web script or HTML via editing an article in the "blog article" page due to the default configuration not utilizing MyBlogUtils.cleanString.	5.4	More Details
CVE-2022-45801	Apache StreamPark 1.0.0 to 2.0.0 have a LDAP injection vulnerability. LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements through techniques similar to SQL Injection. LDAP injection attacks could result in the granting of permissions to unauthorized queries, and content modification inside the LDAP tree. This risk may only occur when the user logs in with ldap, and the user name and password login will not be affected, Users of the affected versions should upgrade to Apache StreamPark 2.0.0 or later.	5.4	More Details
CVE-2023-1861	The Limit Login Attempts WordPress plugin through 1.7.2 does not sanitize and escape usernames when outputting them back in the logs dashboard, which could allow any authenticated users, such as subscriber to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-47877	A Stored cross-site scripting vulnerability in Jedox 2020.2.5 allows remote, authenticated users to inject arbitrary web script or HTML in the Logs page via the log module 'log'.	5.4	More Details
CVE-2023-2361	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30405	A cross-site scripting (XSS) vulnerability in Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the wl_ssid parameter at /boafrm/formHomeWlanSetup.	5.4	More Details
CVE-2023-2000	Mattermost Desktop App fails to validate a mattermost server redirection and navigates to an arbitrary website	5.4	More Details
CVE-2023-31434	The parameters nutzer_titel, nutzer_vn, and nutzer_nn in the user profile, and langID and ONLINEID in direct links, in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 do not validate input, which allows authenticated attackers to inject HTML Code and XSS payloads in multiple locations.	5.4	More Details
CVE-2023-30338	Multiple stored cross-site scripting (XSS) vulnerabilities in Emlog Pro v2.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Article Title or Article Summary parameters.	5.4	More Details
CVE-2022-25274	Drupal 9.3 implemented a generic entity access API for entity revisions. However, this API was not completely integrated with existing permissions, resulting in some possible access bypass for users who have access to use revisions of content generally, but who do not have access to individual items of node and media content. This vulnerability only affects sites using Drupal's revision system.	5.4	More Details
CVE-2023-27864	IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 249327.	5.4	More Details
CVE-2023-29643	Cross Site Scripting (XSS) vulnerability in PerfreeBlog 3.1.2 allows attackers to execute arbitrary code via the Post function.	5.4	More Details
CVE-2023-2343	Cross-site Scripting (XSS) - DOM in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-2342	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-28471	Concrete CMS (previously concrete5) in versions 9.0 through 9.1.3 is vulnerable to Stored XSS via a container name.	5.4	More Details
CVE-2023-2340	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-30123	wuzhicms v4.1.0 is vulnerable to Cross Site Scripting (XSS) in the Member Center, Account Settings.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22503	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0.	5.3	More Details
CVE-2023-27108	An issue was discovered in KaiOS 3.0. The pre-installed Communications application exposes a Web Activity that returns the user's call log without origin or permission checks. An attacker can inject a JavaScript payload that runs in a browser or app without user interaction or consent. This allows an attacker to send the user's call logs to a remote server via XMLHttpRequest or Fetch.	5.3	More Details
CVE-2023-2247	In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview function	5.3	More Details
CVE-2012-5873	ARC (aka ARC2) through 2011-12-01 allows reflected XSS via the end_point.php query parameter in an output=htmltab action.	5.3	More Details
CVE-2023-28472	Concrete CMS (previously concrete5) versions 8.5.12 and below, and 9.0 through 9.1.3 does not have Secure and HTTP only attributes set for ccmPoll cookies.	5.3	More Details
CVE-2023-0458	A speculative pointer dereference problem exists in the Linux Kernel on the do_prlimit() function. The resource argument value is controlled and is used in pointer arithmetic for the 'rlim' variable and can be used to leak the contents. We recommend upgrading past version 6.1.8 or commit 739790605705ddcf18f21782b9c99ad7d53a8c11	5.3	More Details
CVE-2022-25091	Infopop Ultimate Bulletin Board up to v5.47a was discovered to allow all messages posted inside private forums to be disclosed by unauthenticated users via the quote reply feature.	5.3	More Details
CVE-2023-31286	An issue was discovered in Serenity Serene (and StartSharp) before 6.7.0. When a password reset request occurs, the server response leaks the existence of users. If one tries to reset a password of a non-existent user, an error message indicates that this user does not exist.	5.3	More Details
CVE-2023-27559	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash when using a specially crafted subquery. IBM X-Force ID: 249196.	5.3	More Details
CVE-2023-30858	The Denosaurs emoji package provides emojis for dinosaurs. Starting in version 0.1.0 and prior to version 0.3.0, the reTrimSpace regex has 2nd degree polynomial inefficiency, leading to a delayed response given a big payload. The issue has been patched in 0.3.0. As a workaround, avoid using the `replace`, `unemojify`, or `strip` functions.	5.3	More Details
CVE-2023-29056	A valid LDAP user, under specific conditions, will default to read-only permissions when authenticating into XCC. To be vulnerable, XCC must be configured to use an LDAP server for Authentication/Authorization and have the login permission attribute not defined.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4729	IBM Counter Fraud Management for Safer Payments 5.7.0.00 through 5.7.0.10, 6.0.0.00 through 6.0.0.07, 6.1.0.00 through 6.1.0.05, and 6.2.0.00 through 6.2.1.00 could allow an authenticated attacker under special circumstances to send multiple specially crafted API requests that could cause the application to crash. IBM X-Force ID: 188052.	5.3	More Details
CVE-2023-29489	An issue was discovered in cPanel before 11.109.9999.116. XSS can occur on the cpsrvd error page via an invalid webcall ID, aka SEC-669. The fixed versions are 11.109.9999.116, 11.108.0.13, 11.106.0.18, and 11.102.0.31.	5.3	More Details
CVE-2023-2417	A vulnerability was found in ks-soft Advanced Host Monitor up to 12.56 and classified as problematic. Affected by this issue is some unknown functionality of the file C:\Program Files (x86)\HostMonitor\RMA-Win\rma_active.exe. The manipulation leads to unquoted search path. It is possible to launch the attack on the local host. Upgrading to version 12.60 is able to address this issue. It is recommended to upgrade the affected component. VDB-227714 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-28821	Concrete CMS (previously concrete5) before 9.1 did not have a rate limit for password resets.	5.3	More Details
CVE-2023-27860	IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 could disclose sensitive information in an error message. This information could be used in further attacks against the system. IBM X-Force ID: 249207.	5.3	More Details
CVE-2022-48481	In JetBrains Toolbox App before 1.28 a DYLIB injection on macOS was possible	5.2	More Details
CVE-2023-29772	A Cross-site scripting (XSS) vulnerability in the System Log/General Log page of the administrator web UI in ASUS RT-AC51U wireless router firmware version up to and including 3.0.0.4.380.8591 allows remote attackers to inject arbitrary web script or HTML via a malicious network request.	5.2	More Details
CVE-2023-27555	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 is vulnerable to a denial of service when attempting to use ACR client affinity for unfenced DRDA federation wrappers. IBM X-Force ID: 249187.	5.1	More Details
CVE-2023-25495	A valid, authenticated administrative user can query a web interface API to reveal the configured LDAP client password used by XCC to authenticate to an external LDAP server in certain configurations. There is no exposure where no LDAP client password is configured	4.9	More Details
CVE-2023-29443	Zoho ManageEngine ServiceDesk Plus before 14105, ServiceDesk Plus MSP before 14200, SupportCenter Plus before 14200, and AssetExplorer before 6989 allow SDAdmin attackers to conduct XXE attacks via a crafted server that sends malformed XML from a Reports integration API endpoint.	4.9	More Details
CVE-2023-22924	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing crafted CLI commands on a vulnerable device.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22901	ChangingTec MOTP system has a path traversal vulnerability. A remote attacker with administrator's privilege can exploit this vulnerability to access arbitrary system files.	4.9	More Details
CVE-2023-2445	Improper access control in Subscriptions Folder path filter in Devolutions Server 2023.1.1 and earlier allows attackers with administrator privileges to retrieve usage information on folders in user vaults via a specific folder name.	4.9	More Details
CVE-2023-1614	The WP Custom Author URL WordPress plugin before 1.0.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-1554	The Quick Paypal Payments WordPress plugin before 5.7.26.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-1525	The Site Reviews WordPress plugin before 6.7.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-1090	The SMTP Mailing Queue WordPress plugin before 2.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-1021	The amr ical events lists WordPress plugin through 6.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-2419	A vulnerability was found in Zhong Bang CRMEB 4.6.0. It has been declared as critical. This vulnerability affects the function videoUpload of the file \crmeb\app\services\system\attachment\SystemAttachmentServices.php. The manipulation of the argument filename leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227716.	4.7	More Details
CVE-2023-2367	A vulnerability was found in SourceCodester Faculty Evaluation System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/manage_academic.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227643.	4.7	More Details
CVE-2023-2369	A vulnerability was found in SourceCodester Faculty Evaluation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin/manage_restriction.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227645 was assigned to this vulnerability.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2368	A vulnerability was found in SourceCodester Faculty Evaluation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file index.php?page=manage_questionnaire. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227644.	4.7	More Details
CVE-2023-2307	Cross-Site Request Forgery (CSRF) in GitHub repository builderio/qwik prior to 0.104.0.	4.7	More Details
CVE-2022-43871	IBM Financial Transaction Manager for SWIFT Services 3.2.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 239707.	4.6	More Details
CVE-2023-1526	Certain DesignJet and PageWide XL TAA compliant models may have risk of potential information disclosure if the hard disk drive is physically removed from the printer.	4.6	More Details
CVE-2023-31207	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log.	4.4	More Details
CVE-2023-26268	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when using these design document functions: * validate_doc_update * list * filter * filter views (using view functions as filters) * rewrite * update This doesn't affect map/reduce or search (Dreyfus) index functions. Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3). Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store data in the Javascript environment.	4.4	More Details
CVE-2023-30852	Pimcore is an open source data and experience management platform. Prior to version 10.5.21, the `/admin/misc/script-proxy` API endpoint that is accessible by an authenticated administrator user is vulnerable to arbitrary JavaScript and CSS file read via the `scriptPath` and `scripts` parameters. The `scriptPath` parameter is not sanitized properly and is vulnerable to path traversal attack. Any JavaScript/CSS file from the application server can be read by specifying sufficient number of `../` patterns to go out from the application webroot followed by path of the folder where the file is located in the "scriptPath" parameter and the file name in the "scripts" parameter. The JavaScript file is successfully read only if the web application has read access to it. Users should update to version 10.5.21 to receive a patch or, as a workaround, apply the patch manual.	4.4	More Details
CVE-2023-22728	Silverstripe Framework is the Model-View-Controller framework that powers the Silverstripe content management system. Prior to version 4.12.15, the GridField print view incorrectly validates the permission of DataObjects potentially allowing a content author to view records they are not authorised to access. Users should upgrade to Silverstripe Framework 4.12.15 or above to address the issue.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2473	A vulnerability was found in Dreamer CMS up to 4.1.3. It has been declared as problematic. This vulnerability affects the function updatePwd of the file UserController.java of the component Password Hash Calculation. The manipulation leads to inefficient algorithmic complexity. The attack can be initiated remotely. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-227860.	4.3	More Details
CVE-2023-2364	A vulnerability, which was classified as problematic, was found in SourceCodester Resort Reservation System 1.0. Affected is an unknown function of the file registration.php. The manipulation of the argument fullname 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-227640.	4.3	More Details
CVE-2023-29334	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2023-2396	A vulnerability classified as problematic was found in Netgear SRX5308 up to 4.3.5-3. This vulnerability affects unknown code of the component Web Management Interface. The manipulation of the argument USERDBUsers.Password leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227674 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-2395	A vulnerability classified as problematic has been found in Netgear SRX5308 up to 4.3.5-3. This affects an unknown part of the component Web Management Interface. The manipulation of the argument Login.userAgent 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-227673 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-1911	The Blocksy Companion WordPress plugin before 1.8.82 does not ensure that posts to be accessed via a shortcode are already public and can be viewed, allowing any authenticated users, such as subscriber to access draft posts for example	4.3	More Details
CVE-2023-2474	A vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-227866 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-1387	Grafana is an open-source platform for monitoring and observability. Starting with the 9.1 branch, Grafana introduced the ability to search for a JWT in the URL query parameter auth_token and use it as the authentication token. By enabling the "url_login" configuration option (disabled by default), a JWT might be sent to data sources. If an attacker has access to the data source, the leaked token could be used to authenticate to Grafana.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30624	Wasmtime is a standalone runtime for WebAssembly. Prior to versions 6.0.2, 7.0.1, and 8.0.1, Wasmtime's implementation of managing per-instance state, such as tables and memories, contains LLVM-level undefined behavior. This undefined behavior was found to cause runtime-level issues when compiled with LLVM 16 which causes some writes, which are critical for correctness, to be optimized away. Vulnerable versions of Wasmtime compiled with Rust 1.70, which is currently in beta, or later are known to have incorrectly compiled functions. Versions of Wasmtime compiled with the current Rust stable release, 1.69, and prior are not known at this time to have any issues, but can theoretically exhibit potential issues. The underlying problem is that Wasmtime's runtime state for an instance involves a Rust-defined structure called `Instance` which has a trailing `VMContext` structure after it. This `VMContext` structure has a runtime-defined layout that is unique per-module. This representation cannot be expressed with safe code in Rust so `unsafe` code is required to maintain this state. The code doing this, however, has methods which take `&self` as an argument but modify data in the `VMContext` part of the allocation. This means that pointers derived from `&self` are mutated. This is typically not allowed, except in the presence of `UnsafeCell`, in Rust. When compiled to LLVM these functions have `noalias readonly` parameters which means it's UB to write through the pointers. Wasmtime's internal representation and management of `VMContext` has been updated to use `&mut self` methods where appropriate. Additionally verification tools for `unsafe` code in Rust, such as `cargo miri`, are planned to be executed on the `main` branch soon to fix any Rust-level issues that may be exploited in future compiler versions. Precomplied binaries available for Wasmtime from GitHub releases have been compiled with at most LLVM 15 so are not known to be vulnerable. As mentioned above, however, it's still recommended to update. Wasmtime version 6.0.2, 7.0.1, and 8.0.1 have been issued which contain the patch necessary to work correctly on LLVM 16 and have no known UB on LLVM 15 and earlier. If Wasmtime is compiled with Rust 1.69 and prior, which use LLVM 15, then there are no known issues. There is a theoretical possibility for undefined behavior to exploited, however, so it's recommended that users upgrade to a patched version of Wasmtime. Users using beta Rust (1.70 at this time) or nightly Rust (1.71 at this time) must update to a patched version to work correctly.	3.9	More Details
CVE-2023-27892	Insufficient length checks in the ShapeShift KeepKey hardware wallet firmware before 7.7.0 allow a global buffer overflow via crafted messages. Flaws in cf_confirmExecTx() in ethereum_contracts.c can be used to reveal arbitrary microcontroller memory on the device screen or crash the device. With physical access to a PIN-unlocked device, attackers can extract the BIP39 mnemonic secret from the hardware wallet.	3.8	More Details
CVE-2023-30857	@aedart/support is the support package for Ion, a monorepo for JavaScript/TypeScript packages. Prior to version `0.6.1`, there is a possible prototype pollution issue for the `MetadataRecord`, when merged with a base class' metadata object, in `meta` decorator from the `@aedart/support` package. The likelihood of exploitation is questionable, given that a class's metadata can only be set or altered when the class is decorated via `meta()`. Furthermore, object(s) of sensitive nature would have to be stored as metadata, before this can lead to a security impact. The issue has been patched in version `0.6.1`.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-10026	A vulnerability, which was classified as problematic, has been found in Mail Subscribe List Plugin up to 2.0.10 on WordPress. This issue affects some unknown processing of the file index.php. The manipulation of the argument sml_name/sml_email leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2.1 is able to address this issue. The identifier of the patch is 484970ef8285cae51d2de3bd4e4684d33c956c28. It is recommended to upgrade the affected component. The identifier VDB-227765 was assigned to this vulnerability.	3.5	More Details
CVE-2023-28819	Concrete CMS (previously concrete5) versions 8.5.12 and below, 9.0.0 through 9.0.2 is vulnerable to Stored XSS in uploaded file and folder names.	3.5	More Details
CVE-2015-10104	A vulnerability, which was classified as problematic, has been found in Icons for Features Plugin 1.0.0 on WordPress. Affected by this issue is some unknown functionality of the file classes/class-icons-for-features-admin.php. The manipulation of the argument redirect_url leads to open redirect. The attack may be launched remotely. Upgrading to version 1.0.1 is able to address this issue. The name of the patch is 63124c021ae24b68e56872530df26eb4268ad633. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-227756.	3.5	More Details
CVE-2023-2294	A vulnerability was found in UCMS 1.6.0. It has been classified as problematic. This affects an unknown part of the file saddpost.php of the component Column Configuration. The manipulation of the argument strorder 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-227481 was assigned to this vulnerability.	3.5	More Details
CVE-2023-2476	A vulnerability was found in Dromara J2eeFAST up to 2.6.0. It has been classified as problematic. Affected is an unknown function of the component Announcement Handler. The manipulation of the argument 系统工具/公告管理 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 name of the patch is 7a9e1a00e3329fdc0ae05f7a8257cce77037134d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-227868.	3.5	More Details
CVE-2023-2421	A vulnerability classified as problematic has been found in Control iD RHiD 23.3.19.0. Affected is an unknown function of the file /v2/#/add/department. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely. VDB-227718 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-2477	A vulnerability was found in Funadmin up to 3.2.3. It has been declared as problematic. Affected by this vulnerability is the function tagLoad of the file Cx.php. The manipulation of the argument file 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-227869 was assigned to this vulnerability.	3.5	More Details
CVE-2023-2475	A vulnerability was found in Dromara J2eeFAST up to 2.6.0 and classified as problematic. This issue affects some unknown processing of the component System Message Handler. The manipulation of the argument 主题 leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is named 7a9e1a00e3329fdc0ae05f7a8257cce77037134d. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-227867.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2350	A vulnerability classified as problematic was found in SourceCodester Service Provider Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Users.php. The manipulation of the argument id 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-227593 was assigned to this vulnerability.	3.5	More Details
CVE-2023-2349	A vulnerability classified as problematic has been found in SourceCodester Service Provider Management System 1.0. Affected is an unknown function of the file /admin/index.php. The manipulation of the argument page 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-227592.	3.5	More Details
CVE-2014-125100	A vulnerability classified as problematic was found in BestWebSoft Job Board Plugin 1.0.0 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.0.1 is able to address this issue. The name of the patch is dbb71deee071422ce3e663fbcdce3ad24886f940. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-227764.	3.5	More Details
CVE-2023-28473	Concrete CMS (previously concrete5) versions 8.5.12 and below, and 9.0 through 9.1.3 is vulnerable to possible Auth bypass in the jobs section.	3.3	More Details
CVE-2023-2418	A vulnerability was found in Konga 2.8.3 on Kong. It has been classified as problematic. This affects an unknown part of the component Login API. The manipulation leads to insufficiently random values. 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. It is recommended to change the configuration settings. The associated identifier of this vulnerability is VDB-227715.	3.1	More Details
CVE-2023-2197	HashiCorp Vault Enterprise 1.13.0 up to 1.13.1 is vulnerable to a padding oracle attack when using an HSM in conjunction with the CKM_AES_CBC_PAD or CKM_AES_CBC encryption mechanisms. An attacker with privileges to modify storage and restart Vault may be able to intercept or modify cipher text in order to derive Vault's root key. Fixed in 1.13.2	2.5	More Details
CVE-2018-25085	A vulnerability classified as problematic was found in Responsive Menus 7.x-1.x-dev on Drupal. Affected by this vulnerability is the function responsive_menus_admin_form_submit of the file responsive_menus.module of the component Configuration Setting Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 7.x-1.7 is able to address this issue. The patch is named 3c554b31d32a367188f44d44857b061eac949fb8. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-227755.	2.4	More Details
CVE-2023-2393	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file scgi-bin/platform.cgi?page=dmz_setup.htm of the component Web Management Interface. The manipulation of the argument ConfigPort.LogicalIfName 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-227671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2397	A vulnerability, which was classified as problematic, has been found in SourceCodester Simple Mobile Comparison Website 1.0. This issue affects some unknown processing of the file classes/Master.php?f=save_field. The manipulation of the argument Field Name 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-227675.	2.4	More Details
CVE-2023-2425	A vulnerability was found in SourceCodester Simple Student Information System 1.0. It has been classified as problematic. This affects an unknown part of the file /classes/Master.php?f=save_course of the component Add New Course. The manipulation of the argument name with the input <script>alert(document.cookie) </script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227751.	2.4	More Details
CVE-2023-2394	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation of the argument wanName leads to cross site scripting. 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-227672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2392	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been classified as problematic. Affected is an unknown function of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface. The manipulation of the argument ManualDate.minutes 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-227670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2391	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. This issue affects some unknown processing of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface. The manipulation of the argument ntp.server2 leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227669 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2383	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been classified as problematic. This affects an unknown part of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.fromAddr 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-227661 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2389	A vulnerability, which was classified as problematic, was found in Netgear SRX5308 up to 4.3.5-3. This affects an unknown part of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.emailServer leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2388	A vulnerability, which was classified as problematic, has been found in Netgear SRX5308 up to 4.3.5-3. Affected by this issue is some unknown functionality of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.fromAddr leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-227666 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2387	A vulnerability classified as problematic was found in Netgear SRX5308 up to 4.3.5-3. Affected by this vulnerability is an unknown functionality of the file scgi-bin/platform.cgi?page=dmz_setup.htm of the component Web Management Interface. The manipulation of the argument winsServer1 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-227665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2386	A vulnerability classified as problematic has been found in Netgear SRX5308 up to 4.3.5-3. Affected is an unknown function of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.toAddr 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-227664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2385	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been rated as problematic. This issue affects some unknown processing of the file scgi-bin/platform.cgi?page=ike_policies.htm of the component Web Management Interface. The manipulation of the argument IpsecIKEPolicy.IKEPolicyName 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-227663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2384	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been declared as problematic. This vulnerability affects unknown code of the file scgi-bin/platform.cgi?page=dmz_setup.htm of the component Web Management Interface. The manipulation of the argument dhcp.SecDnsIPByte2 leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227662 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2372	A vulnerability, which was classified as problematic, has been found in SourceCodester Online DJ Management System 1.0. Affected by this issue is some unknown functionality of the file classes/Master.php?f=save_event. The manipulation of the argument name leads to cross site scripting. 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-227648.	2.4	More Details
CVE-2023-2390	A vulnerability has been found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. This vulnerability affects unknown code of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface. The manipulation of the argument ntp.server1 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-227668. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2381	A vulnerability has been found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file scgi-bin/platform.cgi?page=bandwidth_profile.htm of the component Web Management Interface. The manipulation of the argument BandWidthProfile.ProfileName 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-227659. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-2382	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. Affected by this issue is some unknown functionality of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument sysLogInfo.serverName leads to cross site scripting. 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-227660. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-28820	Concrete CMS (previously concrete5) before 9.1 is vulnerable to stored XSS in RSS Displayer via the href attribute because the link element input was not sanitized.	2.0	More Details
CVE-2023-30183	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-30349. Reason: This record is a reservation duplicate of CVE-2023-30349. Notes: All CVE users should reference CVE-2023-30349 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-26936	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2019-9587. Reason: This record is a reservation duplicate of CVE-2019-9587. Notes: All CVE users should reference CVE-2019-9587 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-26931	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2022-30524. Reason: This record is a duplicate of CVE-2022-30524. Notes: All CVE users should reference CVE-2022-30524 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26934	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2019-9587. Reason: This record is a reservation duplicate of CVE-2019-9587. Notes: All CVE users should reference CVE-2019-9587 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-26935	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2019-9587. Reason: This record is a reservation duplicate of CVE-2019-9587. Notes: All CVE users should reference CVE-2019-9587 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-26937	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2019-9587. Reason: This record is a reservation duplicate of CVE-2019-9587. Notes: All CVE users should reference CVE-2019-9587 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-26938	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2019-9587. Reason: This record is a reservation duplicate of CVE-2019-9587. Notes: All CVE users should reference CVE-2019-9587 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-26812	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-26813. Reason: This record is a reservation duplicate of CVE-2023-26813. Notes: All CVE users should reference CVE-2023-26813 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-2248	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it was the duplicate of CVE-2023-31436.	N/A	More Details