SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 March 2022

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-2020-10640	Emerson OpenEnterprise versions through 3.3.4 may allow an attacker to run an arbitrary commands with system privileges or perform remote code execution via a specific communication service.	10.0	More Details
CVE-2021-42952	Zepl Notebooks before 2021-10-25 are affected by a sandbox escape vulnerability. Upon launching Remote Code Execution from the Notebook, users can then use that to subsequently escape the running context sandbox and proceed to access internal Zepl assets including cloud metadata services.	9.9	More Details
CVE-2021-4039	A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device.	9.8	More Details
CVE-2021-22432	There is a vulnerability when configuring permission isolation in smartphones. Successful exploitation of this vulnerability may cause out-of-bounds access.	9.8	More Details
CVE-2021-22431	There is a vulnerability when configuring permission isolation in smartphones. Successful exploitation of this vulnerability may cause out-of-bounds access.	9.8	More Details
CVE-2021-22430	There is a logic bypass vulnerability in smartphones. Successful exploitation of this vulnerability may cause code injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22429	There is a memory address out of bounds in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	9.8	More Details
CVE-2021-22426	There is a memory address out of bounds in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	9.8	More Details
CVE-2022-24340	In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible.	9.8	More Details
CVE-2021-22434	There is a memory address out of bounds vulnerability in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	9.8	More Details
CVE-2022-24331	In JetBrains TeamCity before 2021.1.4, GitLab authentication impersonation was possible.	9.8	More Details
CVE-2021-45977	JetBrains IntelliJ IDEA 2021.3.1 Preview, IntelliJ IDEA 2021.3.1 RC, PyCharm Professional 2021.3.1 RC, GoLand 2021.3.1, PhpStorm 2021.3.1 Preview, PhpStorm 2021.3.1 RC, RubyMine 2021.3.1 Preview, RubyMine 2021.3.1 RC, CLion 2021.3.1, WebStorm 2021.3.1 Preview, and WebStorm 2021.3.1 RC (used as Remote Development backend IDEs) bind to the 0.0.0.0 IP address. The fixed versions are: IntelliJ IDEA 2021.3.1, PyCharm Professional 2021.3.1, GoLand 2021.3.2, PhpStorm 2021.3.1 (213.6461.83), RubyMine 2021.3.1, CLion 2021.3.2, and WebStorm 2021.3.1.	9.8	More Details
CVE-2021-36166	An improper authentication vulnerability in FortiMail before 7.0.1 may allow a remote attacker to efficiently guess one administrative account's authentication token by means of the observation of certain system's properties.	9.8	More Details
CVE-2022-25149	The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the IP parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.5.	9.8	More Details
CVE-2022-25148	The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the current_page_id parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.5.	9.8	More Details
CVE-2022-25004	Hospital Patient Record Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in /admin/doctors/manage_doctor.php.	9.8	More Details
CVE-2021-22433	There is a memory address out of bounds in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	9.8	More Details
CVE-2021-39363	Honeywell HDZP252DI 1.00.HW02.4 and HBW2PER1 1.000.HW01.3 devices allow a video replay attack after ARP cache poisoning has been achieved.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25003	Hospital Patient Record Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in /admin/doctors/view_doctor.php.	9.8	More Details
CVE-2021-40046	PCManager versions 11.1.1.95 has a privilege escalation vulnerability. Successful exploit could allow the attacker to access certain resource beyond its privilege.	9.8	More Details
CVE-2022-24442	JetBrains YouTrack before 2021.4.40426 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates.	9.8	More Details
CVE-2022-25060	TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain a command injection vulnerability via the component oal_startPing.	9.8	More Details
CVE-2022-25061	TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain a command injection vulnerability via the component oal_setIp6DefaultRoute.	9.8	More Details
CVE-2022-25064	TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain a remote code execution (RCE) vulnerability via the function oal_wan6_setIpAddr.	9.8	More Details
CVE-2020-12775	Hicos citizen certificate client-side component does not filter special characters for command parameters in specific web URLs. An unauthenticated remote attacker can exploit this vulnerability to perform command injection attack to execute arbitrary system command, disrupt system or terminate service.	9.8	More Details
CVE-2022-25262	In JetBrains Hub before 2022.1.14434, SAML request takeover was possible.	9.8	More Details
CVE-2022-25263	JetBrains TeamCity before 2021.2.3 was vulnerable to OS command injection in the Agent Push feature configuration.	9.8	More Details
CVE-2022-25095	Home Owners Collection Management System v1.0 allows unauthenticated attackers to compromise user accounts via a crafted POST request.	9.8	More Details
CVE-2022-25096	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in /members/view_member.php.	9.8	More Details
CVE-2022-25411	A Remote Code Execution (RCE) vulnerability at /admin/options in Maxsite CMS v180 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-0412	The TI WooCommerce Wishlist WordPress plugin before 1.40.1, TI WooCommerce Wishlist Pro WordPress plugin before 1.40.1 do not sanitise and escape the item_id parameter before using it in a SQL statement via the wishlist/remove_product REST endpoint, allowing unauthenticated attackers to perform SQL injection attacks	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45414	A Remote Code Execution (RCE) vulnerability exists in DataRobot through 2021-10-28 because it allows submission of a Docker environment or Java driver.	9.8	More Details
CVE-2022-24571	Car Driving School Management System v1.0 is affected by SQL injection in the login page. An attacker can use simple SQL login injection payload to get admin access.	9.8	More Details
CVE-2021-22480	The interface of a certain HarmonyOS module has an integer overflow vulnerability. Successful exploitation of this vulnerability may lead to heap memory overflow.	9.8	More Details
CVE-2022-0651	The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the current_page_type parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.5.	9.8	More Details
CVE-2022-25080	TOTOLink A830R V5.9c.4729_B20191112 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25072	TP-Link Archer A54 Archer A54(US)_V1_210111 routers were discovered to contain a stack overflow in the function DM_ Fillobjbystr(). This vulnerability allows unauthenticated attackers to execute arbitrary code.	9.8	More Details
CVE-2022-25078	TOTOLink A3600R V4.1.2cu.5182_B20201102 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25077	TOTOLink A3100R V4.1.2cu.5050_B20200504 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25076	TOTOLink A800R V4.1.2cu.5137_B20200730 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25075	TOTOLink A3000RU V5.9c.2280_B20180512 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25074	TP-Link TL-WR902AC(US)_V3_191209 routers were discovered to contain a stack overflow in the function DM_ Fillobjbystr(). This vulnerability allows unauthenticated attackers to execute arbitrary code.	9.8	More Details
CVE-2022-25073	TL-WR841Nv14_US_0.9.1_4.18 routers were discovered to contain a stack overflow in the function dm_fillObjByStr(). This vulnerability allows unauthenticated attackers to execute arbitrary code.	9.8	More Details
CVE-2022-21142	Authentication bypass vulnerability in a-blog cms Ver.2.8.x series versions prior to Ver.2.8.74, Ver.2.9.x series versions prior to Ver.2.9.39, Ver.2.10.x series versions prior to Ver.2.10.43, and Ver.2.11.x series versions prior to Ver.2.11.41 allows a remote unauthenticated attacker to bypass authentication under the specific condition.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44663	A Remote Code Execution (RCE) vulnerability exists in the Xerte Project Xerte through 3.8.4 via a crafted php file through elfinder in connetor.php.	9.8	More Details
CVE-2021-44610	Multiple SQL Injection vulnerabilities exist in bloofoxCMS 0.5.2.1 - 0.5.1 via the (1) URLs, (2) lang_id, (3) tmpl_id, (4) mod_rewrite (5) eta_doctype. (6) meta_charset, (7) default_group, and (8) page group parameters in the settings mode in admin/index.php.	9.8	More Details
CVE-2021-44567	An unauthenticated SQL Injection vulnerability exists in RosarioSIS before 7.6.1 via the votes parameter in ProgramFunctions/PortalPollsNotes.fnc.php.	9.8	More Details
CVE-2021-44550	An Incorrect Access Control vulnerability exists in CoreNLP 4.3.2 via the classifier in NERServlet.java (lines 158 and 159).	9.8	More Details
CVE-2022-25330	Integer overflow conditions that exist in Trend Micro ServerProtect 6.0/5.8 Information Server could allow a remote attacker to crash the process or achieve remote code execution.	9.8	More Details
CVE-2022-25329	Trend Micro ServerProtect 6.0/5.8 Information Server uses a static credential to perform authentication when a specific command is typed in the console. An unauthenticated remote attacker with access to the Information Server could exploit this to register to the server and perform authenticated actions.	9.8	More Details
CVE-2021-35689	A potential vulnerability in the Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. This high severity potential vulnerability allows attackers to perform remote code execution on Taleo Enterprise Edition system. Successful attacks of this vulnerability can result in unauthorized remote code execution within Taleo Enterprise Edition and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. All affected customers were notified of CVE-2021-35689 by Oracle.	9.8	More Details
CVE-2022-25079	TOTOLink A810R V4.1.2cu.5182_B20201026 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2021-43086	ARM astcenc 3.2.0 is vulnerable to Buffer Overflow. When the compression function of the astc-encoder project with -cl option was used, a stack-buffer-overflow occurred in function encode_ise() in function compress_symbolic_block_for_partition_2planes() in "/Source/astcenc_compress_symbolic.cpp".	9.8	More Details
CVE-2022-25405	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in change_box.php via the DELETE_STR parameter.	9.8	More Details
CVE-2022-25809	Improper Neutralization of audio output from 3rd and 4th Generation Amazon Echo Dot devices allows arbitrary voice command execution on these devices via a malicious skill (in the case of remote attackers) or by pairing a malicious Bluetooth device (in the case of physically proximate attackers), aka an "Alexa versus Alexa (AvA)" attack.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25082	TOTOLink A950RG V5.9c.4050_B20190424 and V4.1.2cu.5204_B20210112 were discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25083	TOTOLink A860R V4.1.2cu.5182_B20201027 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25084	TOTOLink T6 V5.9c.4085_B20190428 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-24720	image_processing is an image processing wrapper for libvips and ImageMagick/GraphicsMagick. Prior to version 1.12.2, using the `#apply` method from image_processing to apply a series of operations that are coming from unsanitized user input allows the attacker to execute shell commands. This method is called internally by Active Storage variants, so Active Storage is vulnerable as well. The vulnerability has been fixed in version 1.12.2 of image_processing. As a workaround, users who process based on user input should always sanitize the user input by allowing only a constrained set of operations.	9.8	More Details
CVE-2021-41193	wire-avs is the audio visual signaling (AVS) component of Wire, an open-source messenger. A remote format string vulnerability in versions prior to 7.1.12 allows an attacker to cause a denial of service or possibly execute arbitrary code. The issue has been fixed in wire-avs 7.1.12. There are currently no known workarounds.	9.8	More Details
CVE-2022-25403	HMS v1.0 was discovered to contain a SQL injection vulnerability via the component admin.php.	9.8	More Details
CVE-2022-25404	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in delete.php via the DELETE_STR parameter.	9.8	More Details
CVE-2022-25081	TOTOLink T10 V5.9c.5061_B20200511 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2022-25406	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in delete_query.php via the DELETE_STR parameter.	9.8	More Details
CVE-2022-25414	Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the parameter NPTR.	9.8	More Details
CVE-2022-25417	Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the function saveparentcontrolinfo.	9.8	More Details
CVE-2022-25418	Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the function openSchedWifi.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25643	seatd-launch in seatd 0.6.x before 0.6.4 allows removing files with escalated privileges when installed setuid root. The attack vector is a user-supplied socket pathname.	9.8	More Details
CVE-2021-25010	The Post Snippets WordPress plugin before 3.1.4 does not have CSRF check when importing files, allowing attacker to make a logged In admin import arbitrary snippets. Furthermore, imported snippers are not sanitised and escaped, which could lead to Stored Cross-Site Scripting issues	9.6	More Details
CVE-2022-24711	CodeIgniter4 is the 4.x branch of CodeIgniter, a PHP full-stack web framework. Prior to version 4.1.9, an improper input validation vulnerability allows attackers to execute CLI routes via HTTP request. Version 4.1.9 contains a patch. There are currently no known workarounds for this vulnerability.	9.4	More Details
CVE-2021-42767	A directory traversal vulnerability in the apoc plugins in Neo4J Graph database before 4.4.0.1 allows attackers to read local files, and sometimes create local files. This is fixed in 3.5.17, 4.2.10, 4.3.0.4, and 4.4.0.1.	9.1	More Details
CVE-2022-0717	Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2.	9.1	More Details
CVE-2022-0768	Server-Side Request Forgery (SSRF) in GitHub repository rudloff/alltube prior to 3.0.2.	9.1	More Details
CVE-2022-25359	On ICL ScadaFlex II SCADA Controller SC-1 and SC-2 1.03.07 devices, unauthenticated remote attackers can overwrite, delete, or create files.	9.1	More Details
CVE-2022-25260	JetBrains Hub before 2021.1.14276 was vulnerable to blind Server-Side Request Forgery (SSRF).	9.1	More Details
CVE-2021-22448	There is an improper verification vulnerability in smartphones. Successful exploitation of this vulnerability may cause unauthorized read and write of some files.	9.1	More Details
CVE-2021-22394	There is a buffer overflow vulnerability in smartphones. Successful exploitation of this vulnerability may cause DoS of the apps during Multi-Screen Collaboration.	9.1	More Details
CVE-2021-4070	Off-by-one Error in GitHub repository v2fly/v2ray-core prior to 4.44.0.	9.1	More Details
CVE-2022-25402	An incorrect access control issue in HMS v1.0 allows unauthenticated attackers to read and modify all PHP files.	9.1	More Details
CVE-2022-25098	ECTouch v2 suffers from arbitrary file deletion due to insufficient filtering of the filename parameter.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25010	The component /rootfs in RageFile of Stepmania v5.1b2 and below allows attackers access to the entire file system.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-25094	Home Owners Collection Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the parameter "cover" in SystemSettings.php.	8.8	More Details
CVE-2022-25291	An integer overflow in WatchGuard Firebox and XTM appliances allows an authenticated remote attacker to trigger a heap-based buffer overflow and potentially execute arbitrary code by initiating a firmware update with a malicious upgrade image. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	8.8	More Details
CVE-2022-24288	In Apache Airflow, prior to version 2.2.4, some example DAGs did not properly sanitize user-provided params, making them susceptible to OS Command Injection from the web UI.	8.8	More Details
CVE-2022-25018	Pluxml v5.8.7 was discovered to allow attackers to execute arbitrary code via crafted PHP code inserted into static pages.	8.8	More Details
CVE-2022-24947	Apache JSPWiki user preferences form is vulnerable to CSRF attacks, which can lead to account takeover. Apache JSPWiki users should upgrade to 2.11.2 or later.	8.8	More Details
CVE-2021-42951	A Remote Code Execution (RCE) vulnerability exists in Algorithmia MSOL all versions before October 10 2021 of SaaS. Users can register for an account and are allocated a set number of credits to try the product. Once users authenticate, they can proceed to create a new, specially crafted Algorithm and subsequently launch remote code execution with their desired result.	8.8	More Details
CVE-2022-25360	WatchGuard Firebox and XTM appliances allow an authenticated remote attacker with unprivileged credentials to upload files to arbitrary locations. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	8.8	More Details
CVE-2022-25023	Audio File commit 004065d was discovered to contain a heap-buffer overflow in the function fouBytesToInt():AudioFile.h.	8.8	More Details
CVE-2022-25293	A systemd stack-based buffer overflow in WatchGuard Firebox and XTM appliances allows an authenticated remote attacker to potentially execute arbitrary code by initiating a firmware update with a malicious upgrade image. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25292	A wgagent stack-based buffer overflow in WatchGuard Firebox and XTM appliances allows an authenticated remote attacker to potentially execute arbitrary code by initiating a firmware update with a malicious upgrade image. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	8.8	More Details
CVE-2022-24342	In JetBrains TeamCity before 2021.2.1, URL injection leading to CSRF was possible.	8.8	More Details
CVE-2022-24709	@awsui/components-react is the main AWS UI package which contains React components, with TypeScript definitions designed for user interface development. Multiple components in versions before 3.0.367 have been found to not properly neutralize user input and may allow for javascript injection. Users are advised to upgrade to version 3.0.367 or later. There are no known workarounds for this issue.	8.8	More Details
CVE-2022-0411	The Asgaros Forum WordPress plugin before 2.0.0 does not sanitise and escape the post_id parameter before using it in a SQL statement via a REST route of the plugin (accessible to any authenticated user), leading to a SQL injection	8.8	More Details
CVE-2021-24864	The WP Cloudy, weather plugin WordPress plugin before 4.4.9 does not escape the post_id parameter before using it in a SQL statement in the admin dashboard, leading to a SQL Injection issue	8.8	More Details
CVE-2021-24803	The Core Tweaks WP Setup WordPress plugin through 4.1 allows to bulk-set many settings in WordPress, including the admin email, as well as creating a new admin account. There is no CSRF protection in place, allowing an attacker to arbitrary change the admin email or create another admin account and takeover the website via CSRF attacks	8.8	More Details
CVE-2021-24704	In the Orange Form WordPress plugin through 1.0, the process_bulk_action() function in "admin/orange-form-email.php" performs an unprepared SQL query with an unsanitized parameter ($id). Only admin can access the page that invokes the function, but because of lack of CSRF protection, it is actually exploitable and could allow attackers to make a logged in admin delete arbitrary posts for example	8.8	More Details
CVE-2021-3967	Improper Access Control in GitHub repository zulip/zulip prior to 4.10.	8.8	More Details
CVE-2021-44967	A Remote Code Execution (RCE) vulnerabilty exists in LimeSurvey 5.2.4 via the upload and install plugins function, which could let a remote malicious user upload an arbitrary PHP code file.	8.8	More Details
CVE-2021-4029	A command injection vulnerability in the CGI program of the Zyxel ARMOR Z1/Z2 firmware could allow an attacker to execute arbitrary OS commands via a LAN interface.	8.8	More Details
CVE-2022-24407	In Cyrus SASL 2.1.17 through 2.1.27 before 2.1.28, plugins/sql.c does not escape the password for a SQL INSERT or UPDATE statement.	8.8	More Details
CVE-2021-44664	An Authenticated Remote Code Exection (RCE) vulnerability exists in Xerte through 3.9 in website_code/php/import/fileupload.php by uploading a maliciously crafted PHP file though the project interface disguised as a language file to bypasses the upload filters. Attackers can manipulate the files destination by abusing path traversal in the 'mediapath' variable.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23176	WatchGuard Firebox and XTM appliances allow a remote attacker with unprivileged credentials to access the system with a privileged management session via exposed management access. This vulnerability impacts Fireware OS before 12.7.2_U1, 12.x before 12.1.3_U3, and 12.2.x through 12.5.x before 12.5.7_U3.	8.8	More Details
CVE-2021-41282	diag_routes.php in pfSense 2.5.2 allows sed data injection. Authenticated users are intended to be able to view data about the routes set in the firewall. The data is retrieved by executing the netstat utility, and then its output is parsed via the sed utility. Although the common protection mechanisms against command injection (i.e., the usage of the escapeshellarg function for the arguments) are used, it is still possible to inject sed-specific code and write an arbitrary file in an arbitrary location.	8.8	More Details
CVE-2022-24252	An unrestricted file upload vulnerability in the FileTransferServlet component of Extensis Portfolio v4.0 allows remote attackers to execute arbitrary code via a crafted file.	8.8	More Details
CVE-2022-23380	There is a SQL injection vulnerability in the background of taocms 3.0.2 in parameter id:action=admin&id=2&ctrl=edit.	8.8	More Details
CVE-2022-24251	Extensis Portfolio v4.0 was discovered to contain an authenticated unrestricted file upload vulnerability via the Catalog Asset Upload function.	8.8	More Details
CVE-2022-0729	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440.	8.8	More Details
CVE-2022-24255	Extensis Portfolio v4.0 was discovered to contain hardcoded credentials which allows attackers to gain administrator privileges.	8.8	More Details
CVE-2020-10632	Inadequate folder security permissions in Emerson OpenEnterprise versions through 3.3.4 may allow modification of important configuration files, which could cause the system to fail or behave in an unpredictable manner.	8.8	More Details
CVE-2022-24253	Extensis Portfolio v4.0 was discovered to contain an authenticated unrestricted file upload vulnerability via the component AdminFileTransferServlet.	8.8	More Details
CVE-2021-43075	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.2 and below, version 8.5.2 and below, version 8.4.2 and below, version 8.3.2 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests to the alarm dashboard and controller config handlers.	8.8	More Details
CVE-2021-43077	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiWLM version 8.6.2 and below, version 8.5.2 and below, version 8.4.2 and below, version 8.3.2 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests to the AP monitor handlers.	8.8	More Details
CVE-2022-24254	An unrestricted file upload vulnerability in the Backup/Restore Archive component of Extensis Portfolio v4.0 allows remote attackers to execute arbitrary code via a crafted ZIP file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20650	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation of user supplied data that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP POST request to the NX-API of an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. Note: The NX-API feature is disabled by default.	8.8	More Details
CVE-2022-24610	Settings/network settings/wireless settings on the Alecto DVC-215IP camera version 63.1.1.173 and below shows the Wi-Fi passphrase hidden, but by editing/removing the style of the password field the password becomes visible which grants access to an internal network connected to the camera.	8.6	More Details
CVE-2022-20623	A vulnerability in the rate limiter for Bidirectional Forwarding Detection (BFD) traffic of Cisco NX-OS Software for Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause BFD traffic to be dropped on an affected device. This vulnerability is due to a logic error in the BFD rate limiter functionality. An attacker could exploit this vulnerability by sending a crafted stream of traffic through the device. A successful exploit could allow the attacker to cause BFD traffic to be dropped, resulting in BFD session flaps. BFD session flaps can cause route instability and dropped traffic, resulting in a denial of service (DoS) condition. This vulnerability applies to both IPv4 and IPv6 traffic.	8.6	More Details
CVE-2022-20624	A vulnerability in the Cisco Fabric Services over IP (CFSoIP) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of incoming CFSoIP packets. An attacker could exploit this vulnerability by sending crafted CFSoIP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2022-21824	Due to the formatting logic of the "console.table()" function it was not safe to allow user controlled input to be passed to the "properties" parameter while simultaneously passing a plain object with at least one property as the first parameter, which could be "__proto__". The prototype pollution has very limited control, in that it only allows an empty string to be assigned to numerical keys of the object prototype.Node.js >= 12.22.9, >= 14.18.3, >= 16.13.2, and >= 17.3.1 use a null protoype for the object these properties are being assigned to.	8.2	More Details
CVE-2021-21708	In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits.	8.2	More Details
CVE-2022-24335	JetBrains TeamCity before 2021.2 was vulnerable to a Time-of-check/Time-of-use (TOCTOU) race-condition attack in agent registration via XML-RPC.	8.1	More Details
CVE-2022-23835	The Visual Voice Mail (VVM) application through 2022-02-24 for Android allows persistent access if an attacker temporarily controls an application that has the READ_SMS permission, and reads an IMAP credentialing message that is (by design) not displayed to the victim within the AOSP SMS/MMS messaging application. (Often, the IMAP credentials are usable to listen to voice mail messages sent before the vulnerability was exploited, in addition to new ones.) NOTE: some vendors characterize this as not a "concrete and exploitable risk.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41112	Rundeck is an open source automation service with a web console, command line tools and a WebAPI. In versions prior to 3.4.5, authenticated users could craft a request to modify or delete System or Project level Calendars, without appropriate authorization. Modifying or removing calendars could cause Scheduled Jobs to execute, or not execute on desired calendar days. Severity depends on trust level of authenticated users and impact of running or not running scheduled jobs on days governed by calendar definitions. Version 3.4.5 contains a patch for this issue. There are currently no known workarounds.	8.1	More Details
CVE-2022-25412	Maxsite CMS v180 was discovered to contain multiple arbitrary file deletion vulnerabilities in /admin_page/all-files-update-ajax.php via the dir and deletefile parameters.	8.1	More Details
CVE-2021-24823	The Support Board WordPress plugin before 3.3.6 does not have any CSRF checks in actions handled by the include/ajax.php file, which could allow attackers to make logged in users do unwanted actions. For example, make an admin delete arbitrary files	8.1	More Details
CVE-2021-36171	The use of a cryptographically weak pseudo-random number generator in the password reset feature of FortiPortal before 6.0.6 may allow a remote unauthenticated attacker to predict parts of or the whole newly generated password within a given time frame.	8.1	More Details
CVE-2022-25838	Laravel Fortify before 1.11.1 allows reuse within a short time window, thus calling into question the "OT" part of the "TOTP" concept.	8.1	More Details
CVE-2021-26617	This issues due to insufficient verification of the various input values from user's input. The vulnerability allows remote attackers to execute malicious code in Firstmall via navercheckout_add function.	8.1	More Details
CVE-2021-4030	A cross-site request forgery vulnerability in the HTTP daemon of the Zyxel ARMOR Z1/Z2 firmware could allow an attacker to execute arbitrary commands if they coerce or trick a local user to visit a compromised website with malicious scripts.	8.0	More Details
CVE-2021-40043	The laser command injection vulnerability exists on AIS-BW80H-00 versions earlier than AIS-BW80H-00 9.0.3.4(H100SP13C00). The devices cannot effectively defend against external malicious interference. Attackers need the device to be visually exploitable and successful triggering of this vulnerability could execute voice commands on the device.	7.8	More Details
CVE-2022-21209	The affected product is vulnerable to an out-of-bounds read while processing project files, which allows an attacker to craft a project file that would allow arbitrary code execution.	7.8	More Details
CVE-2022-24232	A local file inclusion in Hospital Patient Record Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24346	In JetBrains IntelliJ IDEA before 2021.3.1, local code execution via RLO (Right-to-Left Override) characters was possible.	7.8	More Details
CVE-2022-24345	In JetBrains IntelliJ IDEA before 2021.2.4, local code execution (without permission from a user) upon opening a project was possible.	7.8	More Details
CVE-2022-25099	A vulnerability in the component /languages/index.php of WBCE CMS v1.5.2 allows attackers to execute arbitrary code via a crafted PHP file.	7.8	More Details
CVE-2022-25101	A vulnerability in the component /templates/install.php of WBCE CMS v1.5.2 allows attackers to execute arbitrary code via a crafted PHP file.	7.8	More Details
CVE-2022-0545	An integer overflow in the processing of loaded 2D images leads to a write-what-where vulnerability and an out-of-bounds read vulnerability, allowing an attacker to leak sensitive information or achieve code execution in the context of the Blender process when a specially crafted image file is loaded. This flaw affects Blender versions prior to 2.83.19, 2.93.8 and 3.1.	7.8	More Details
CVE-2022-23985	The affected product is vulnerable to an out-of-bounds write while processing project files, which allows an attacker to craft a project file that would allow arbitrary code execution.	7.8	More Details
CVE-2022-0546	A missing bounds check in the image loader used in Blender 3.x and 2.93.8 leads to out-of-bounds heap access, allowing an attacker to cause denial of service, memory corruption or potentially code execution.	7.8	More Details
CVE-2022-25636	net/netfilter/nf_dup_netdev.c in the Linux kernel 5.4 through 5.6.10 allows local users to gain privileges because of a heap out-of-bounds write. This is related to nf_tables_offload.	7.8	More Details
CVE-2021-26252	A flaw was found in htmldoc in v1.9.12. Heap buffer overflow in pspdf_prepare_page(),in ps-pdf.cxx may lead to execute arbitrary code and denial of service.	7.8	More Details
CVE-2022-25170	The affected product is vulnerable to a stack-based buffer overflow while processing project files, which may allow an attacker to execute arbitrary code	7.8	More Details
CVE-2019-25058	An issue was discovered in USBGuard before 1.1.0. On systems with the usbguard-dbus daemon running, an unprivileged user could make USBGuard allow all USB devices to be connected in the future.	7.8	More Details
CVE-2022-26181	Dropbox Lepton v1.2.1-185-g2a08b77 was discovered to contain a heap-buffer-overflow in the function aligned_dealloc():src/lepton/bitops.cc:108.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24680	A security link following local privilege escalation vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service, Trend Micro Worry-Free Business Security 10.0 SP1 and Trend Micro Worry-Free Business Security Services agents could allow a local attacker to create a mount point and leverage this for arbitrary folder deletion, leading to escalated privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-24679	A security link following local privilege escalation vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service, Trend Micro Worry-Free Business Security 10.0 SP1 and Trend Micro Worry-Free Business Security Services agents could allow a local attacker to create an writable folder in an arbitrary location and escalate privileges affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-43619	Trusted Firmware M 1.4.x through 1.4.1 has a buffer overflow issue in the Firmware Update partition. In the IPC model, a psa_fwu_write caller from SPE or NSPE can overwrite stack memory locations.	7.8	More Details
CVE-2021-44342	David Brackeen ok-file-formats 203defd is vulnerable to Buffer Overflow via function ok_png_transform_scanline() in "/ok_png.c:494".	7.8	More Details
CVE-2021-44331	ARM astcenc 3.2.0 is vulnerable to Buffer Overflow in function encode_ise().	7.8	More Details
CVE-2021-44340	David Brackeen ok-file-formats dev version is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurred in function ok_jpg_generate_huffman_table() in "/ok_jpg.c:403".	7.8	More Details
CVE-2021-44339	David Brackeen ok-file-formats 203defd is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurred in function ok_png_transform_scanline() in "/ok_png.c:712".	7.8	More Details
CVE-2021-44334	David Brackeen ok-file-formats 97f78ca is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurs in function ok_jpg_convert_YCbCr_to_RGB() in "/ok_jpg.c:513" .	7.8	More Details
CVE-2022-24671	A link following privilege escalation vulnerability in Trend Micro Antivirus for Max 11.0.2150 and below could allow a local attacker to modify a file during the update process and escalate their privileges. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-24986	KDE KCron through 21.12.2 uses a temporary file in /tmp when saving, but reuses the filename during an editing session. Thus, someone watching it be created the first time could potentially intercept the file the following time, enabling that person to run unauthorized commands.	7.8	More Details
CVE-2020-14481	The DeskLock tool provided with FactoryTalk View SE uses a weak encryption algorithm that may allow a local, authenticated attacker to decipher user credentials, including the Windows user or Windows DeskLock passwords. If the compromised user has an administrative account, an attacker could gain full access to the user's operating system and certain components of FactoryTalk View SE.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44132	A command injection vulnerability in the function formImportOMCIShell of C-DATA ONU4FERW V2.1.13_X139 allows attackers to execute arbitrary commands via a crafted file.	7.8	More Details
CVE-2021-32586	An improper input validation vulnerability in the web server CGI facilities of FortiMail before 7.0.1 may allow an unauthenticated attacker to alter the environment of the underlying script interpreter via specifically crafted HTTP requests.	7.7	More Details
CVE-2022-22262	ROG Live Service's function for deleting temp files created by installation has an improper link resolution before file access vulnerability. Since this function does not validate the path before deletion, an unauthenticated local attacker can create an unexpected symbolic link to system file path, to delete arbitrary system files and disrupt system service.	7.7	More Details
CVE-2022-24718	ssr-pages is an HTML page builder for the purpose of server-side rendering (SSR). In versions prior to 0.1.4, a path traversal issue can occur when providing untrusted input to the `svg` property as an argument to the `build(MessagePageOptions)` function. While there is no known workaround at this time, there is a patch in version 0.1.4.	7.6	More Details
CVE-2022-0777	Weak Password Recovery Mechanism for Forgotten Password in GitHub repository microweber/microweber prior to 1.3.	7.5	More Details
CVE-2022-23377	Archeevo below 5.0 is affected by local file inclusion through file=~/web.config to allow an attacker to retrieve local files.	7.5	More Details
CVE-2022-23387	An issue was discovered in taocms 3.0.2. This is a SQL blind injection that can obtain database data through the Comment Update field.	7.5	More Details
CVE-2021-39364	Honeywell HDZP252DI 1.00.HW02.4 and HBW2PER1 1.000.HW01.3 devices allow command spoofing (for camera control) after ARP cache poisoning has been achieved.	7.5	More Details
CVE-2021-4021	A vulnerability was found in Radare2 in versions prior to 5.6.2, 5.6.0, 5.5.4 and 5.5.2. Mapping a huge section filled with zeros of an ELF64 binary for MIPS architecture can lead to uncontrolled resource consumption and DoS.	7.5	More Details
CVE-2021-3610	A heap-based buffer overflow vulnerability was found in ImageMagick in versions prior to 7.0.11-14 in ReadTIFFImage() in coders/tiff.c. This issue is due to an incorrect setting of the pixel array size, which can lead to a crash and segmentation fault.	7.5	More Details
CVE-2021-41652	Insecure permissions in the file database.sdb of BatFlat CMS v1.3.6 allows attackers to dump the entire database.	7.5	More Details
CVE-2020-22845	A buffer overflow in Mikrotik RouterOS 6.47 allows unauthenticated attackers to cause a denial of service (DOS) via crafted FTP requests.	7.5	More Details
CVE-2022-0247	An issue exists in Fuchsia where VMO data can be modified through access to copy-on-write snapshots. A local attacker could modify objects in the VMO that they do not have permission to. We recommend upgrading past commit d97c05d2301799ed585620a9c5c739d36e7b5d3d or any of the listed versions.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25374	HashiCorp Terraform Enterprise v202112-1, v202112-2, v202201-1, and v202201-2 were configured to log inbound HTTP requests in a manner that may capture sensitive data. Fixed in v202202-1.	7.5	More Details
CVE-2022-24327	In JetBrains Hub before 2021.1.13890, integration with JetBrains Account exposed an API key with excessive permissions.	7.5	More Details
CVE-2022-23921	Exploitation of this vulnerability may result in local privilege escalation and code execution. GE maintains exploitation of this vulnerability is only possible if the attacker has login access to a machine actively running CIMPLICITY, the CIMPLICITY server is not already running a project, and the server is licensed for multiple projects.	7.5	More Details
CVE-2020-22844	A buffer overflow in Mikrotik RouterOS 6.47 allows unauthenticated attackers to cause a denial of service (DOS) via crafted SMB requests.	7.5	More Details
CVE-2022-24341	In JetBrains TeamCity before 2021.2.1, editing a user account to change its password didn't terminate sessions of the edited user.	7.5	More Details
CVE-2022-24685	HashiCorp Nomad and Nomad Enterprise 1.0.17, 1.1.11, and 1.2.5 allow invalid HCL for the jobs parse endpoint, which may cause excessive CPU usage. Fixed in 1.0.18, 1.1.12, and 1.2.6.	7.5	More Details
CVE-2021-22319	There is an improper verification vulnerability in smartphones. Successful exploitation of this vulnerability may cause integer overflows.	7.5	More Details
CVE-2022-0736	Insecure Temporary File in GitHub repository mlflow/mlflow prior to 1.23.1.	7.5	More Details
CVE-2022-23308	valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.	7.5	More Details
CVE-2021-22489	There is a DoS vulnerability in smartphones. Successful exploitation of this vulnerability may affect service availability.	7.5	More Details
CVE-2021-37027	There is a DoS vulnerability in smartphones. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2022-25264	In JetBrains TeamCity before 2021.2.3, environment variables of the "password" type could be logged in some cases.	7.5	More Details
CVE-2022-25062	TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain an integer overflow via the function dm_checkString. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21798	The affected product is vulnerable due to cleartext transmission of credentials seen in the CIMPLICITY network, which can be easily spoofed and used to log in to make operational changes to the system.	7.5	More Details
CVE-2022-0654	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository fgribreau/node-request-retry prior to 7.0.0.	7.5	More Details
CVE-2021-22395	There is a code injection vulnerability in smartphones. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2022-24678	An security agent resource exhaustion denial-of-service vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service, Trend Micro Worry-Free Business Security 10.0 SP1 and Trend Micro Worry-Free Business Security Services agents could allow an attacker to flood a temporary log location and consume all disk space on affected installations.	7.5	More Details
CVE-2022-25104	HorizontCMS v1.0.0-beta.2 was discovered to contain an arbitrary file download vulnerability via the component /admin/file-manager/.	7.5	More Details
CVE-2020-27467	A Directory Traversal vulnerability exits in Processwire CMS before 2.7.1 via the download parameter to index.php.	7.5	More Details
CVE-2022-25331	Uncaught exceptions that can be generated in Trend Micro ServerProtection 6.0/5.8 Information Server could allow a remote attacker to crash the process.	7.5	More Details
CVE-2022-23986	SQL injection vulnerability in the phpUploader v1.2 and earlier allows a remote unauthenticated attacker to obtain the information in the database via unspecified vectors.	7.5	More Details
CVE-2022-22336	IBM Sterling External Authentication Server and IBM Sterling Secure Proxy 6.0.3.0, 6.0.2.0, and 3.4.3.2 could allow a remote user to consume resources causing a denial of service due to a resource leak. IBM X-Force ID: 219395.	7.5	More Details
CVE-2021-25636	LibreOffice supports digital signatures of ODF documents and macros within documents, presenting visual aids that no alteration of the document occurred since the last signing and that the signature is valid. An Improper Certificate Validation vulnerability in LibreOffice allowed an attacker to create a digitally signed ODF document, by manipulating the documentsignatures.xml or macrosignatures.xml stream within the document to contain both "X509Data" and "KeyValue" children of the "KeyInfo" tag, which when opened caused LibreOffice to verify using the "KeyValue" but to report verification with the unrelated "X509Data" value. This issue affects: The Document Foundation LibreOffice 7.2 versions prior to 7.2.5.	7.5	More Details
CVE-2022-25640	In wolfSSL before 5.2.0, a TLS 1.3 server cannot properly enforce a requirement for mutual authentication. A client can simply omit the certificate_verify message from the handshake, and never present a certificate.	7.5	More Details
CVE-2021-45746	A Directory Traversal vulnerability exists in WeBankPartners wecube-platform 3.2.1 via the file variable in PluginPackageController.java.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0732	The backend infrastructure shared by multiple mobile device monitoring services does not adequately authenticate or authorize API requests, creating an IDOR (Insecure Direct Object Reference) vulnerability.	7.5	More Details
CVE-2022-25401	The copy function of the file manager in Cuppa CMS v1.0 allows any file to be copied to the current directory, granting attackers read access to arbitrary files.	7.5	More Details
CVE-2022-24707	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. UNION SQL injection and time-based blind injection vulnerabilities existed in Time Tracker Puncher plugin in versions of anuko timetracker prior to 1.20.0.5642. This was happening because the Puncher plugin was reusing code from other places and was relying on an unsanitized date parameter in POST requests. Because the parameter was not checked, it was possible to craft POST requests with malicious SQL for Time Tracker database. This issue has been resolved in in version 1.20.0.5642. Users unable to upgrade are advised to add their own checks to input.	7.4	More Details
CVE-2021-44531	Accepting arbitrary Subject Alternative Name (SAN) types, unless a PKI is specifically defined to use a particular SAN type, can result in bypassing name-constrained intermediates. Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 was accepting URI SAN types, which PKIs are often not defined to use. Additionally, when a protocol allows URI SANs, Node.js did not match the URI correctly.Versions of Node.js with the fix for this disable the URI SAN type when checking a certificate against a hostname. This behavior can be reverted through the --security-revert command-line option.	7.4	More Details
CVE-2022-0383	The WP Review Slider WordPress plugin before 11.0 does not sanitise and escape the pid parameter when copying a Twitter source, which could allow a high privilege users to perform SQL Injections attacks	7.2	More Details
CVE-2022-26149	MODX Revolution through 2.8.3-pl allows remote authenticated administrators to execute arbitrary code by uploading an executable file, because the Uploadable File Types setting can be changed by an administrator.	7.2	More Details
CVE-2022-25306	The WP Statistics WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the browser parameter found in the ~/includes/class-wp-statistics-visitor.php file which allows attackers to inject arbitrary web scripts onto several pages that execute when site administrators view a sites statistics, in versions up to and including 13.1.5.	7.2	More Details
CVE-2022-25305	The WP Statistics WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the IP parameter found in the ~/includes/class-wp-statistics-ip.php file which allows attackers to inject arbitrary web scripts onto several pages that execute when site administrators view a sites statistics, in versions up to and including 13.1.5.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21706	Zulip is an open-source team collaboration tool with topic-based threading. Zulip Server version 2.0.0 and above are vulnerable to insufficient access control with multi-use invitations. A Zulip Server deployment which hosts multiple organizations is vulnerable to an attack where an invitation created in one organization (potentially as a role with elevated permissions) can be used to join any other organization. This bypasses any restrictions on required domains on users' email addresses, may be used to gain access to organizations which are only accessible by invitation, and may be used to gain access with elevated privileges. This issue has been patched in release 4.10. There are no known workarounds for this issue. ### Patches _Has the problem been patched? What versions should users upgrade to?_ ### Workarounds _Is there a way for users to fix or remediate the vulnerability without upgrading?_ ### References _Are there any links users can visit to find out more?_ ### For more information If you have any questions or comments about this advisory, you can discuss them on the [developer community Zulip server](https://zulip.com/developer-community/), or email the [Zulip security team](mailto:security@zulip.com).	7.2	More Details
CVE-2022-23911	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not validate and escape the id parameter before using it in a SQL statement when retrieving a testimonial to edit, leading to a SQL Injection	7.2	More Details
CVE-2022-23906	CMS Made Simple v2.2.15 was discovered to contain a Remote Command Execution (RCE) vulnerability via the upload avatar function. This vulnerability is exploited via a crafted image file.	7.2	More Details
CVE-2022-25307	The WP Statistics WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the platform parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers to inject arbitrary web scripts onto several pages that execute when site administrators view a sites statistics, in versions up to and including 13.1.5.	7.2	More Details
CVE-2021-44238	AyaCMS 3.1.2 is vulnerable to Remote Code Execution (RCE) via /aya/module/admin/ust_tab_e.inc.php,	7.2	More Details
CVE-2022-21705	Octobercms is a self-hosted CMS platform based on the Laravel PHP Framework. In affected versions user input was not properly sanitized before rendering. An authenticated user with the permissions to create, modify and delete website pages can exploit this vulnerability to bypass `cms.safe_mode` / `cms.enableSafeMode` in order to execute arbitrary code. This issue only affects admin panels that rely on safe mode and restricted permissions. To exploit this vulnerability, an attacker must first have access to the backend area. The issue has been patched in Build 474 (v1.0.474) and v1.1.10. Users unable to upgrade should apply https://github.com/octobercms/library/commit/c393c5ce9ca2c5acc3ed6c9bb0dab5ffd61965fe to your installation manually.	7.2	More Details
CVE-2021-29220	Multiple buffer overflow security vulnerabilities have been identified in HPE iLO Amplifier Pack version(s): Prior to 2.12. These vulnerabilities could be exploited by a highly privileged user to remotely execute code that could lead to a loss of confidentiality, integrity, and availability. HPE has provided a software update to resolve this vulnerability in HPE iLO Amplifier Pack.	7.2	More Details
CVE-2022-23043	Zenario CMS 9.2 allows an authenticated admin user to bypass the file upload restriction by creating a new 'File/MIME Types' using the '.phar' extension. Then an attacker can upload a malicious file, intercept the request and change the extension to '.phar' in order to run commands on the server.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14478	A local, authenticated attacker could use an XML External Entity (XXE) attack to exploit weakly configured XML files to access local or remote content. A successful exploit could potentially cause a denial-of-service condition and allow the attacker to arbitrarily read any local file via system-level services.	7.1	More Details
CVE-2021-22437	There is a software integer overflow leading to a TOCTOU condition in smartphones. Successful exploitation of this vulnerability may cause random address access.	7.0	More Details
CVE-2021-34359	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Proxy Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Proxy Server: QTS 4.5.x: Proxy Server 1.4.2 (2021/12/30) and later	6.9	More Details
CVE-2022-22794	Cybonet - PineApp Mail Relay Unauthenticated Sql Injection. Attacker can send a request to: /manage/emailrichment/userlist.php?CUSTOMER_ID_INNER=1 /admin/emailrichment/userlist.php?CUSTOMER_ID_INNER=1 /manage/emailrichment/usersunlist.php?CUSTOMER_ID_INNER=1 /admin/emailrichment/usersunlist.php?CUSTOMER_ID_INNER=1 and by doing that, the attacker can run Remote Code Execution in one liner.	6.8	More Details
CVE-2022-0764	Arbitrary Command Injection in GitHub repository strapi/strapi prior to 4.1.0.	6.7	More Details
CVE-2022-23810	Template injection (Improper Neutralization of Special Elements Used in a Template Engine) vulnerability in a-blog cms Ver.2.8.x series versions prior to Ver.2.8.75, Ver.2.9.x series versions prior to Ver.2.9.40, Ver.2.10.x series versions prior to Ver.2.10.44, Ver.2.11.x series versions prior to Ver.2.11.42, and Ver.3.0.x series versions prior to Ver.3.0.1 allows a remote authenticated attacker to obtain an arbitrary file on the server via unspecified vectors.	6.5	More Details
CVE-2022-24333	In JetBrains TeamCity before 2021.2, blind SSRF via an XML-RPC call was possible.	6.5	More Details
CVE-2022-0721	Insertion of Sensitive Information Into Debugging Code in GitHub repository microweber/microweber prior to 1.3.	6.5	More Details
CVE-2022-25363	WatchGuard Firebox and XTM appliances allow an authenticated remote attacker with unprivileged credentials to modify privileged management user credentials. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	6.5	More Details
CVE-2022-0724	Insecure Storage of Sensitive Information in GitHub repository microweber/microweber prior to 1.3.	6.5	More Details
CVE-2022-24328	In JetBrains Hub before 2021.1.13956, an unprivileged user could perform DoS.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0731	Improper Access Control (IDOR) in GitHub repository dolibarr/dolibarr prior to 16.0.	6.5	More Details
CVE-2022-25290	WatchGuard Firebox and XTM appliances allow an authenticated remote attacker with unprivileged credentials to retrieve certificate private keys. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	6.5	More Details
CVE-2022-24337	In JetBrains TeamCity before 2021.2, health items of pull requests were shown to users who lacked appropriate permissions.	6.5	More Details
CVE-2022-22333	IBM Sterling Secure Proxy 6.0.3.0, 6.0.2.0, and 3.4.3.2 and IBM Sterling External Authentication Server are vulnerable a buffer overflow, due to the Jetty based GUI in the Secure Zone not properly validating the sizes of the form content and/or HTTP headers submitted. A local attacker positioned inside the Secure Zone could submit a specially crafted HTTP request to disrupt service. IBM X-Force ID: 219133.	6.5	More Details
CVE-2022-24599	In autofile Audio File Library 0.3.6, there exists one memory leak vulnerability in printfileinfo, in printinfo.c, which allows an attacker to leak sensitive information via a crafted file. The printfileinfo function calls the copyrightstring function to get data, however, it dosn't use zero bytes to truncate the data.	6.5	More Details
CVE-2021-35036	A cleartext storage of information vulnerability in the Zyxel VMG3625-T50B firmware version V5.50(ABTL.0)b2k could allow an authenticated attacker to obtain sensitive information from the configuration file.	6.5	More Details
CVE-2021-25081	The Maps Plugin using Google Maps for WordPress plugin before 1.8.4 does not have CSRF checks in most of its AJAX actions, which could allow attackers to make logged in admins delete arbitrary posts and update the plugin's settings via a CSRF attack	6.5	More Details
CVE-2022-25638	In wolfSSL before 5.2.0, certificate validation may be bypassed during attempted authentication by a TLS 1.3 client to a TLS 1.3 server. This occurs when the sig_algo field differs between the certificate_verify message and the certificate message.	6.5	More Details
CVE-2021-24820	The Cost Calculator WordPress plugin through 1.6 allows authenticated users (Contributor+ in versions < 1.5, and Admin+ in versions <= 1.6) to perform path traversal and local PHP file inclusion on Windows Web Servers via the Cost Calculator post's Layout	6.5	More Details
CVE-2020-10636	Inadequate encryption may allow the passwords for Emerson OpenEnterprise versions through 3.3.4 user accounts to be obtained.	6.5	More Details
CVE-2022-23135	There is a directory traversal vulnerability in some home gateway products of ZTE. Due to the lack of verification of user modified destination path, an attacker with specific permissions could modify the FTP access path to access and modify the system path contents without authorization, which will cause information leak and affect device operation.	6.5	More Details
CVE-2022-24687	HashiCorp Consul and Consul Enterprise 1.9.0 through 1.9.14, 1.10.7, and 1.11.2 clusters with at least one Ingress Gateway allow a user with service:write to register a specifically-defined service that can cause Consul servers to panic. Fixed in 1.9.15, 1.10.8, and 1.11.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44665	A Directory Traversal vulnerability exists in the Xerte Project Xerte through 3.10.3 when downloading a project file via download.php.	6.5	More Details
CVE-2021-3596	A NULL pointer dereference flaw was found in ImageMagick in versions prior to 7.0.10-31 in ReadSVGImage() in coders/svg.c. This issue is due to not checking the return value from libxml2's xmlCreatePushParserCtxt() and uses the value directly, which leads to a crash and segmentation fault.	6.5	More Details
CVE-2022-24708	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. ttUser.class.php in Time Tracker versions prior to 1.20.0.5646 was not escaping primary group name for display. Because of that, it was possible for a logged in user to modify primary group name with elements of JavaScript. Such script could then be executed in user browser on subsequent requests on pages where primary group name was displayed. This is vulnerability has been fixed in version 1.20.0.5646. Users who are unable to upgrade may modify ttUser.class.php to use an additional call to htmlspecialchars when printing group name.	6.5	More Details
CVE-2021-41111	Rundeck is an open source automation service with a web console, command line tools and a WebAPI. Prior to versions 3.4.5 and 3.3.15, an authenticated user with authorization to read webhooks in one project can craft a request to reveal Webhook definitions and tokens in another project. The user could use the revealed webhook tokens to trigger webhooks. Severity depends on trust level of authenticated users and whether any webhooks exist that trigger sensitive actions. There are patches for this vulnerability in versions 3.4.5 and 3.3.15. There are currently no known workarounds.	6.4	More Details
CVE-2021-3700	A use-after-free vulnerability was found in usbredir in versions prior to 0.11.0 in the usbredirparser_serialize() in usbredirparser/usbredirparser.c. This issue occurs when serializing large amounts of buffered write data in the case of a slow or blocked destination.	6.4	More Details
CVE-2022-24712	CodeIgniter4 is the 4.x branch of CodeIgniter, a PHP full-stack web framework. A vulnerability in versions prior to 4.1.9 might allow remote attackers to bypass the CodeIgniter4 Cross-Site Request Forgery (CSRF) protection mechanism. Users should upgrade to version 4.1.9. There are workarounds for this vulnerability, but users will still need to code as these after upgrading to v4.1.9. Otherwise, the CSRF protection may be bypassed. If auto-routing is enabled, check the request method in the controller method before processing. If auto-routing is disabled, either avoid using `$routes->add()` and instead use HTTP verbs in routes; or check the request method in the controller method before processing.	6.3	More Details
CVE-2022-0189	The WP RSS Aggregator WordPress plugin before 4.20 does not sanitise and escape the id parameter in the wprss_fetch_items_row_action AJAX action before outputting it back in the response, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-24435	Cross-site scripting vulnerability in phpUploader v1.2 and earlier allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-37504	A cross-site scripting (XSS) vulnerability in the fileNameStr parameter of jQuery-Upload-File v4.0.11 allows attackers to execute arbitrary web scripts or HTML via a crafted file with a Javascript payload in the file name.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0150	The WP Accessibility Helper (WAH) WordPress plugin before 0.6.0.7 does not sanitise and escape the wahi parameter before outputting back its base64 decode value in the page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-24948	A carefully crafted user preferences for submission could trigger an XSS vulnerability on Apache JSPWiki, related to the user preferences screen, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.2 or later.	6.1	More Details
CVE-2021-42244	A cross-site scripting (XSS) vulnerability in PaquitoSoftware Notimoo v1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted title or message in a notification.	6.1	More Details
CVE-2022-0385	The Crazy Bone WordPress plugin through 0.6.0 does not sanitise and escape the username submitted via the login from when displaying them back in the log dashboard, leading to an unauthenticated Stored Cross-Site scripting	6.1	More Details
CVE-2022-0683	The Essential Addons for Elementor Lite WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the settings parameter found in the ~/includes/Traits/Helper.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a user clicks on a specially crafted link by an attacker. This affects versions up to and including 5.0.8.	6.1	More Details
CVE-2022-22793	Cybonet - PineApp Mail Relay Local File Inclusion. Attacker can send a request to : /manage/mailpolicymtm/log/eml_viewer/email.content.body.php?filesystem_path=ENCDODED PATH and by doing that, the attacker can read Local Files inside the server.	6.1	More Details
CVE-2022-23916	Cross-site scripting vulnerability in a-blog cms Ver.2.8.x series versions prior to Ver.2.8.75, Ver.2.9.x series versions prior to Ver.2.9.40, Ver.2.10.x series versions prior to Ver.2.10.44, Ver.2.11.x series versions prior to Ver.2.11.42, and Ver.3.0.x series versions prior to Ver.3.0.1 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. This vulnerability is different from CVE-2022-24374.	6.1	More Details
CVE-2022-24374	Cross-site scripting vulnerability in a-blog cms Ver.2.8.x series versions prior to Ver.2.8.75, Ver.2.9.x series versions prior to Ver.2.9.40, Ver.2.10.x series versions prior to Ver.2.10.44, Ver.2.11.x series versions prior to Ver.2.11.42, and Ver.3.0.x series versions prior to Ver.3.0.1 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. This vulnerability is different from CVE-2022-23916.	6.1	More Details
CVE-2021-25112	The WHMCS Bridge WordPress plugin before 6.4b does not sanitise and escape the error parameter before outputting it back in admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2020-14502	The web interface of the 1734-AENTR communication module is vulnerable to stored XSS. A remote, unauthenticated attacker could store a malicious script within the web interface that, when executed, could modify some string values on the homepage of the web interface.	6.1	More Details
CVE-2022-0653	The Profile Builder – User Profile & User Registration Forms WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the site_url parameter found in the ~/assets/misc/fallback-page.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a user clicks on a specially crafted link by an attacker. This affects versions up to and including 3.6.1.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25034	The WP User WordPress plugin before 7.0 does not sanitise and escape some parameters in pages where the [wp_user] shortcode is used, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-25259	JetBrains Hub before 2021.1.14276 was vulnerable to reflected XSS.	6.1	More Details
CVE-2022-25261	JetBrains TeamCity before 2021.2.2 was vulnerable to reflected XSS.	6.1	More Details
CVE-2021-24994	The Migration, Backup, Staging WordPress plugin before 0.9.69 does not have authorisation when adding remote storages, and does not sanitise as well as escape a parameter from such unauthenticated requests before outputting it in admin page, leading to a Stored Cross-Site Scripting issue	6.1	More Details
CVE-2021-24977	The Use Any Font	Custom Font Uploader WordPress plugin before 6.2.1 does not have any authorisation checks when assigning a font, allowing unauthenticated users to sent arbitrary CSS which will then be processed by the frontend for all users. Due to the lack of sanitisation and escaping in the backend, it could also lead to Stored XSS issues	6.1	More Details
CVE-2022-24717	ssr-pages is an HTML page builder for the purpose of server-side rendering (SSR). In versions prior to 0.1.5, a cross site scripting (XSS) issue can occur when providing untrusted input to the `redirect.link` property as an argument to the `build(MessagePageOptions)` function. While there is no known workaround at this time, there is a patch in version 0.1.5.	6.1	More Details
CVE-2020-36510	The 15Zine WordPress theme before 3.3.0 does not sanitise and escape the cbi parameter before outputing it back in the response via the cb_s_a AJAX action, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-23912	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not sanitise and escape the id parameter before outputting it back in an attribute, leading to a Reflected cross-Site Scripting	6.1	More Details
CVE-2022-0710	The Header Footer Code Manager plugin <= 1.1.16 for WordPress is vulnerable to Reflected Cross-Site Scripting (XSS) via the $_REQUEST['page'] parameter.	6.1	More Details
CVE-2022-23988	The WS Form LITE and Pro WordPress plugins before 1.8.176 do not sanitise and escape submitted form data, allowing unauthenticated attacker to submit XSS payloads which will get executed when a privileged user will view the related submission	6.1	More Details
CVE-2021-44662	A Site Scripting (XSS) vulnerability exists in the Xerte Project Xerte through 3.8.4 via the link parameter in print.php.	6.1	More Details
CVE-2022-25028	Home Owners Collection Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the collected_by parameter under the List of Collections module.	6.1	More Details
CVE-2022-24330	In JetBrains TeamCity before 2021.2.1, a redirection to an external site was possible.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24572	Car Driving School Management System v1.0 is affected by Cross Site Scripting (XSS) in the User Enrollment Form (Username Field). To exploit this Vulnerability, an admin views the registered user details.	6.1	More Details
CVE-2022-25014	Ice Hrm 30.0.0.OS was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the "m" parameter in the Dashboard of the current user. This vulnerability allows attackers to compromise session credentials via user interaction with a crafted link.	6.1	More Details
CVE-2022-25013	Ice Hrm 30.0.0.OS was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities via the "key" and "fm" parameters in the component login.php.	6.1	More Details
CVE-2021-29217	A remote URL redirection vulnerability was discovered in HPE OneView Global Dashboard version(s): Prior to 2.5. HPE has provided a software update to resolve this vulnerability in HPE OneView Global Dashboard.	6.1	More Details
CVE-2022-24338	JetBrains TeamCity before 2021.2.1 was vulnerable to reflected XSS.	6.1	More Details
CVE-2021-46387	ZyXEL ZyWALL 2 Plus Internet Security Appliance is affected by Cross Site Scripting (XSS). Insecure URI handling leads to bypass security restriction to achieve Cross Site Scripting, which allows an attacker able to execute arbitrary JavaScript codes to perform multiple attacks such as clipboard hijacking and session hijacking.	6.1	More Details
CVE-2022-0776	Cross-site Scripting (XSS) - DOM in GitHub repository hakimel/reveal.js prior to 4.3.0.	6.1	More Details
CVE-2021-29216	A remote cross-site scripting vulnerability was discovered in HPE OneView Global Dashboard version(s): Prior to 2.5. HPE has provided a software update to resolve this vulnerability in HPE OneView Global Dashboard.	6.1	More Details
CVE-2022-26158	An issue was discovered in the web application in Cherwell Service Management (CSM) 10.2.3. It accepts and reflects arbitrary domains supplied via a client-controlled Host header. Injection of a malicious URL in the Host: header of the HTTP Request results in a 302 redirect to an attacker-controlled page.	6.1	More Details
CVE-2022-26156	An issue was discovered in the web application in Cherwell Service Management (CSM) 10.2.3. Injection of a malicious payload within the RelayState= parameter of the HTTP request body results in the hijacking of the form action. Form-action hijacking vulnerabilities arise when an application places user-supplied input into the action URL of an HTML form. An attacker can use this vulnerability to construct a URL that, if visited by another application user, will modify the action URL of a form to point to the attacker's server.	6.1	More Details
CVE-2022-26155	An issue was discovered in the web application in Cherwell Service Management (CSM) 10.2.3. XSS can occur via a payload in the SAMLResponse parameter of the HTTP request body.	6.1	More Details
CVE-2022-23907	CMS Made Simple v2.2.15 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the parameter m1_fmmessage.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25642	Obyte (formerly Byteball) Wallet before 3.4.1 allows XSS. A crafted chat message can lead to remote code execution.	6.1	More Details
CVE-2021-45229	It was discovered that the "Trigger DAG with config" screen was susceptible to XSS attacks via the `origin` query argument. This issue affects Apache Airflow versions 2.2.3 and below.	6.1	More Details
CVE-2021-3608	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device in versions prior to 6.1.0. The issue occurs while handling a "PVRDMA_REG_DSRHIGH" write from the guest and may result in a crash of QEMU or cause undefined behavior due to the access of an uninitialized pointer. The highest threat from this vulnerability is to system availability.	6.0	More Details
CVE-2021-3607	An integer overflow was found in the QEMU implementation of VMWare's paravirtual RDMA device in versions prior to 6.1.0. The issue occurs while handling a "PVRDMA_REG_DSRHIGH" write from the guest due to improper input validation. This flaw allows a privileged guest user to make QEMU allocate a large amount of memory, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	6.0	More Details
CVE-2020-36516	An issue was discovered in the Linux kernel through 5.16.11. The mixed IPID assignment method with the hash-based IPID assignment policy allows an off-path attacker to inject data into a victim's TCP session or terminate that session.	5.9	More Details
CVE-2022-24409	Dell BSAFE SSL-J contains remediation for a covert timing channel vulnerability that may be exploited by malicious users to compromise the affected system. Only customers with active BSAFE maintenance contracts can receive details about this vulnerability. Public disclosure of the vulnerability details will be shared at a later date.	5.9	More Details
CVE-2022-0615	Use-after-free in eset_rtp kernel module used in ESET products for Linux allows potential attacker to trigger denial-of-service condition on the system.	5.9	More Details
CVE-2021-25011	The Maps Plugin using Google Maps for WordPress plugin before 1.8.1 does not have proper authorisation and CSRF in most of its AJAX actions, which could allow any authenticated users, such as subscriber to delete arbitrary posts and update the plugin's settings.	5.7	More Details
CVE-2022-23104	WIN-911 2021 R1 and R2 are vulnerable to a permissions misconfiguration that may allow an attacker to locally write files to the program Operator Workspace directory, which holds DLL files and executables. A low-privilege attacker could write a malicious DLL file to the Operator Workspace directory to achieve privilege escalation and the permissions of the user running the program.	5.6	More Details
CVE-2022-23922	WIN-911 2021 R1 and R2 are vulnerable to a permissions misconfiguration that may allow an attacker to locally write files to the Program Announcer directory and elevate permissions whenever the program is executed.	5.6	More Details
CVE-2021-44961	A memory leakage flaw exists in the class PerimeterGenerator of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. Specially crafted stl files can exhaust available memory. An attacker can provide malicious files to trigger this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0695	Denial of Service in GitHub repository radareorg/radare2 prior to 5.6.4.	5.5	More Details
CVE-2021-44962	An out-of-bounds read vulnerability exists in the GCode::extrude() functionality of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. A specially crafted stl file could lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2022-0544	An integer underflow in the DDS loader of Blender leads to an out-of-bounds read, possibly allowing an attacker to read sensitive data using a crafted DDS image file. This flaw affects Blender versions prior to 2.83.19, 2.93.8 and 3.1.	5.5	More Details
CVE-2020-14480	Due to usernames/passwords being stored in plaintext in Random Access Memory (RAM), a local, authenticated attacker could gain access to certain credentials, including Windows Logon credentials.	5.5	More Details
CVE-2020-4925	A security vulnerability in the Spectrum Scale 5.0 and 5.1 allows a non-root user to overflow the mmfsd daemon with requests and preventing the daemon to service other requests. IBM X-Force ID: 191599.	5.5	More Details
CVE-2022-0476	Denial of Service in GitHub repository radareorg/radare2 prior to 5.6.4.	5.5	More Details
CVE-2022-22321	IBM MQ Appliance 9.2 CD and 9.2 LTS local messaging users stored with a password hash that provides insufficient protection. IBM X-Force ID: 218368.	5.5	More Details
CVE-2022-22908	SangforCSClient.exe in Sangfor VDI Client 5.4.2.1006 allows attackers, when they are able to read process memory, to discover the contents of the Username and Password fields.	5.5	More Details
CVE-2022-25012	Argus Surveillance DVR v4.0 employs weak password encryption.	5.5	More Details
CVE-2022-24613	metadata-extractor up to 2.16.0 can throw various uncaught exceptions while parsing a specially crafted JPEG file, which could result in an application crash. This could be used to mount a denial of service attack against services that use metadata-extractor library.	5.5	More Details
CVE-2021-43745	A Denial of Service vulnerabilty exists in Trilium Notes 0.48.6 in the setupPage function	5.5	More Details
CVE-2021-22479	The interface of a certain HarmonyOS module has an invalid address access vulnerability. Successful exploitation of this vulnerability may lead to kernel crash.	5.5	More Details
CVE-2021-38994	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 kernel to cause a denial of service. IBM X-Force ID: 213072.	5.5	More Details
CVE-2021-22478	The interface of a certain HarmonyOS module has a UAF vulnerability. Successful exploitation of this vulnerability may lead to information leakage.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22441	Some Huawei products have an integer overflow vulnerability. Successful exploitation of this vulnerability may lead to kernel crash.	5.5	More Details
CVE-2022-24614	When reading a specially crafted JPEG file, metadata-extractor up to 2.16.0 can be made to allocate large amounts of memory that finally leads to an out-of-memory error even for very small inputs. This could be used to mount a denial of service attack against services that use metadata-extractor library.	5.5	More Details
CVE-2021-38995	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 kernel to cause a denial of service. IBM X-Force ID: 213073.	5.5	More Details
CVE-2021-38993	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 smbcd daemon to cause a denial of service. IBM X-Force ID: 212962.	5.5	More Details
CVE-2022-24615	zip4j up to v2.10.0 can throw various uncaught exceptions while parsing a specially crafted ZIP file, which could result in an application crash. This could be used to mount a denial of service attack against services that use zip4j library.	5.5	More Details
CVE-2021-46702	Tor Browser 9.0.7 on Windows 10 build 10586 is vulnerable to information disclosure. This could allow local attackers to bypass the intended anonymity feature and obtain information regarding the onion services visited by a local user. This can be accomplished by analyzing RAM memory even several hours after the local user used the product. This occurs because the product doesn't properly free memory.	5.5	More Details
CVE-2021-37103	There is an improper permission management vulnerability in the Wallet apps. Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2022-25326	fscrypt through v0.3.2 creates a world-writable directory by default when setting up a filesystem, allowing unprivileged users to exhaust filesystem space. We recommend upgrading to fscrypt 0.3.3 or above and adjusting the permissions on existing fscrypt metadata directories where applicable.	5.5	More Details
CVE-2022-25327	The PAM module for fscrypt doesn't adequately validate fscrypt metadata files, allowing users to create malicious metadata files that prevent other users from logging in. A local user can cause a denial of service by creating a fscrypt metadata file that prevents other users from logging into the system. We recommend upgrading to version 0.3.3 or above	5.5	More Details
CVE-2022-0762	Incorrect Authorization in GitHub repository microweber/microweber prior to 1.3.	5.5	More Details
CVE-2022-25020	A cross-site scripting (XSS) vulnerability in Pluxml v5.8.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the thumbnail path of a blog post.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25413	Maxsite CMS v108 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the parameter f_tags at /admin/page_edit/3.	5.4	More Details
CVE-2022-24582	Accounting Journal Management 1.0 is vulnerable to XSS-PHPSESSID-Hijacking. The parameter manage_user from User lists is vulnerable to XSS-Stored and PHPSESSID attacks. The malicious user can attack the system by using the already session which he has from inside and outside of the network.	5.4	More Details
CVE-2021-39038	IBM WebSphere Application Server 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 22.0.0.2 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 213968.	5.4	More Details
CVE-2022-25407	Hospital Management System v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Doctor parameter at /admin-panel1.php.	5.4	More Details
CVE-2022-25408	Hospital Management System v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the dpassword parameter at /admin-panel1.php.	5.4	More Details
CVE-2022-0727	Improper Access Control in GitHub repository chocobozzz/peertube prior to 4.1.0.	5.4	More Details
CVE-2022-25409	Hospital Management System v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the demail parameter at /admin-panel1.php.	5.4	More Details
CVE-2022-25410	Maxsite CMS v180 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the parameter f_file_description at /admin/files.	5.4	More Details
CVE-2021-38986	IBM MQ Appliance 9.2 CD and 9.2 LTS does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 212942.	5.4	More Details
CVE-2022-25022	A cross-site scripting (XSS) vulnerability in Htmly v2.8.1 allows attackers to excute arbitrary web scripts HTML via a crafted payload in the content field of a blog post.	5.4	More Details
CVE-2022-24347	JetBrains YouTrack before 2021.4.36872 was vulnerable to stored XSS via a project icon.	5.4	More Details
CVE-2022-26332	Cipi 3.1.15 allows Add Server stored XSS via the /api/servers name field.	5.4	More Details
CVE-2022-24620	Piwigo version 12.2.0 is vulnerable to stored cross-site scripting (XSS), which can lead to privilege escalation. In this way, admin can steal webmaster's cookies to get the webmaster's access.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24344	JetBrains YouTrack before 2021.4.31698 was vulnerable to stored XSS on the Notification templates page.	5.4	More Details
CVE-2022-24566	In Checkmk <=2.0.0p19 fixed in 2.0.0p20 and Checkmk <=1.6.0p27 fixed in 1.6.0p28, the title of a Predefined condition is not properly escaped when shown as condition, which can result in Cross Site Scripting (XSS).	5.4	More Details
CVE-2022-24339	JetBrains TeamCity before 2021.2.1 was vulnerable to stored XSS.	5.4	More Details
CVE-2022-24612	An authenticated user can upload an XML file containing an XSS via the ITSM module of EyesOfNetwork 5.3.11, resulting in a stored XSS.	5.4	More Details
CVE-2022-25015	A stored cross-site scripting (XSS) vulnerability in Ice Hrm 30.0.0.OS allows attackers to steal cookies via a crafted payload inserted into the First Name field.	5.4	More Details
CVE-2022-0719	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3.	5.4	More Details
CVE-2022-26146	Tricentis qTest before 10.4 allows stored XSS by an authenticated attacker.	5.4	More Details
CVE-2021-44607	A Cross Site Scripting (XSS) vulnerability exists in FUEL-CMS 1.5.1 in the Assets page via an SVG file.	5.4	More Details
CVE-2022-0726	Missing Authorization in GitHub repository chocobozzz/peertube prior to 4.1.0.	5.4	More Details
CVE-2021-44566	A Cross Site Scripting (XSS) vulnerability exists in RosarioSIS before 4.3 via the SanitizeMarkDown function in ProgramFunctions/MarkDownHTML.fnc.php.	5.4	More Details
CVE-2021-24933	The Dynamic Widgets WordPress plugin through 1.5.16 does not escape the prefix parameter before outputting it back in an attribute when using the term_tree AJAX action (available to any authenticated users), leading to a Reflected Cross-Site Scripting issue	5.4	More Details
CVE-2021-24971	The WP Responsive Menu WordPress plugin before 3.1.7.1 does not have capability and CSRF checks in the wpr_live_update AJAX action, as well as do not sanitise and escape some of the data submitted. As a result, any authenticated, such as subscriber could update the plugin's settings and perform Cross-Site Scripting attacks against all visitor and users on the frontend	5.4	More Details
CVE-2021-44608	Multiple Cross Site Scripting (XSS) vulnerabilities exists in bloofoxCMS 0.5.2.1 - 0.5.1 via the (1) file parameter and (2) type parameter in an edit action in index.php.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24710	Weblate is a copyleft software web-based continuous localization system. Versions prior to 4.11 do not properly neutralize user input used in user name and language fields. Due to this improper neutralization it is possible to perform cross-site scripting via these fields. The issues were fixed in the 4.11 release. Users unable to upgrade are advised to add their own neutralize logic.	5.4	More Details
CVE-2021-44565	A Cross Site Scripting (XSS) vulnerability exists in RosarioSIS before 7.6.1 via the xss_clean function in classes/Security.php, which allows remote malicious users to inject arbitrary JavaScript or HTML. An example of affected components are all Markdown input fields.	5.4	More Details
CVE-2022-0723	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.11.	5.4	More Details
CVE-2021-23495	The package karma before 6.3.16 are vulnerable to Open Redirect due to missing validation of the return_url query parameter.	5.4	More Details
CVE-2022-24565	Checkmk <=2.0.0p19 Fixed in 2.0.0p20 and Checkmk <=1.6.0p27 Fixed in 1.6.0p28 are affected by a Cross Site Scripting (XSS) vulnerability. The Alias of a site was not properly escaped when shown as condition for notifications.	5.4	More Details
CVE-2021-25042	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 5.5 does not have authorisation and CSRF checks in the updateIpAddress AJAX action, allowing any authenticated user to call it, or make a logged in user do it via a CSRF attack and add an arbitrary IP address to exclude. Furthermore, due to the lack of validation, sanitisation and escaping, users could set a malicious value and perform Cross-Site Scripting attacks against logged in admin	5.4	More Details
CVE-2021-44533	Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 did not handle multi-value Relative Distinguished Names correctly. Attackers could craft certificate subjects containing a single-value Relative Distinguished Name that would be interpreted as a multi-value Relative Distinguished Name, for example, in order to inject a Common Name that would allow bypassing the certificate subject verification.Affected versions of Node.js that do not accept multi-value Relative Distinguished Names and are thus not vulnerable to such attacks themselves. However, third-party code that uses node's ambiguous presentation of certificate subjects may be vulnerable.	5.3	More Details
CVE-2022-24594	In waline 1.6.1, an attacker can submit messages using X-Forwarded-For to forge any IP address.	5.3	More Details
CVE-2022-26315	qrcp through 0.8.4, in receive mode, allows ../ Directory Traversal via the file name specified by the uploader.	5.3	More Details
CVE-2022-24332	In JetBrains TeamCity before 2021.2, a logout action didn't remove a Remember Me cookie.	5.3	More Details
CVE-2022-24334	In JetBrains TeamCity before 2021.2.1, the Agent Push feature allowed selection of any private key on the server.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24329	In JetBrains Kotlin before 1.6.0, it was not possible to lock dependencies for Multiplatform Gradle Projects.	5.3	More Details
CVE-2022-23701	A potential remote host header injection security vulnerability has been identified in HPE Integrated Lights-Out 4 (iLO 4) firmware version(s): Prior to 2.60. This vulnerability could be remotely exploited to allow an attacker to supply invalid input to the iLO 4 webserver, causing it to respond with a redirect to an attacker-controlled domain. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 4 (iLO 4).	5.3	More Details
CVE-2022-24336	In JetBrains TeamCity before 2021.2.1, an unauthenticated attacker can cancel running builds via an XML-RPC request to the TeamCity server.	5.3	More Details
CVE-2022-25355	EC-CUBE 3.0.0 to 3.0.18-p3 and EC-CUBE 4.0.0 to 4.1.1 improperly handle HTTP Host header values, which may lead a remote unauthenticated attacker to direct the vulnerable version of EC-CUBE to send an Email with some forged reissue-password URL to EC-CUBE users.	5.3	More Details
CVE-2022-24633	All versions of FileCloud prior to 21.3 are vulnerable to user enumeration. The vulnerability exists in the parameter "path" passing "/SHARED/<username>". A malicious actor could identify the existence of users by requesting share information on specified share paths.	5.3	More Details
CVE-2022-26157	An issue was discovered in the web application in Cherwell Service Management (CSM) 10.2.3. The ASP.NET_Sessionid cookie is not protected by the Secure flag. This makes it prone to interception by an attacker if traffic is sent over unencrypted channels.	5.3	More Details
CVE-2021-44532	Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 converts SANs (Subject Alternative Names) to a string format. It uses this string to check peer certificates against hostnames when validating connections. The string format was subject to an injection vulnerability when name constraints were used within a certificate chain, allowing the bypass of these name constraints.Versions of Node.js with the fix for this escape SANs containing the problematic characters in order to prevent the injection. This behavior can be reverted through the --security-revert command-line option.	5.3	More Details
CVE-2020-14504	The web interface of the 1734-AENTR communication module mishandles authentication for HTTP POST requests. A remote, unauthenticated attacker can send a crafted request that may allow for modification of the configuration settings.	5.3	More Details
CVE-2021-34361	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Proxy Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Proxy Server: QTS 4.5.x: Proxy Server 1.4.2 (2021/12/30) and later	5.3	More Details
CVE-2021-25118	The Yoast SEO WordPress plugin (from versions 16.7 until 17.2) discloses the full internal path of featured images in posts via the wp/v2/posts REST endpoints which could help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.	5.3	More Details
CVE-2022-26159	The auto-completion plugin in Ametys CMS before 4.5.0 allows a remote unauthenticated attacker to read documents such as plugins/web/service/search/auto-completion/<domain>/en.xml (and similar pathnames for other languages), which contain all characters typed by all users, including the content of private pages. For example, a private page may contain usernames, e-mail addresses, and possibly passwords.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25328	The bash_completion script for fscrypt allows injection of commands via crafted mountpoint paths, allowing privilege escalation under a specific set of circumstances. A local user who has control over mountpoint paths could potentially escalate their privileges if they create a malicious mountpoint path and if the system administrator happens to be using the fscrypt bash completion script to complete mountpoint paths. We recommend upgrading to version 0.3.3 or above	5.0	More Details
CVE-2021-24689	The Contact Forms - Drag & Drop Contact Form Builder WordPress plugin through 1.0.5 allows high privilege users to download arbitrary files from the web server via a path traversal attack	4.9	More Details
CVE-2022-0360	The Easy Drag And drop All Import : WP Ultimate CSV Importer WordPress plugin before 6.4.3 does not sanitise and escaped imported comments, which could allow high privilege users to import malicious ones (either intentionnaly or not) and lead to Stored Cross-Site Scripting issues	4.8	More Details
CVE-2021-43945	Affected versions of Atlassian Jira Server and Data Center allow remote attackers with Roadmaps Administrator permissions to inject arbitrary HTML or JavaScript via a Stored Cross-Site Scripting (SXSS) vulnerability in the /rest/jpo/1.0/hierarchyConfiguration endpoint. The affected versions are before version 8.20.3.	4.8	More Details
CVE-2022-23655	Octobercms is a self-hosted CMS platform based on the Laravel PHP Framework. Affected versions of OctoberCMS did not validate gateway server signatures. As a result non-authoritative gateway servers may be used to exfiltrate user private keys. Users are advised to upgrade their installations to build 474 or v1.1.10. The only known workaround is to manually apply the patch (e3b455ad587282f0fbcb7763c6d9c3d000ca1e6a) which adds server signature validation.	4.8	More Details
CVE-2022-0772	Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.2.2.	4.8	More Details
CVE-2021-24898	The EditableTable WordPress plugin through 0.1.4 does not sanitise and escape any of the Table and Column fields, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24901	The Security Audit WordPress plugin through 1.0.0 does not sanitise and escape the Data Id setting, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24903	The GRAND FlaGallery WordPress plugin through 6.1.2 does not sanitise and escape some of its gallery settings, which could allow high privilege users to perform Cross-Site scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24920	The StatCounter WordPress plugin before 2.0.7 does not sanitise and escape the Project ID and Secure Code settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-23987	The WS Form LITE and Pro WordPress plugins before 1.8.176 do not sanitise and escape their Form Name, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0763	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.	4.8	More Details
CVE-2021-43943	Affected versions of Atlassian Jira Service Management Server and Data Center allow attackers with administrator privileges to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the "Object Schema" field of /secure/admin/InsightDefaultCustomFieldConfig.jspa. The affected versions are before version 4.21.0.	4.8	More Details
CVE-2021-4222	The WP-Paginate WordPress plugin before 2.1.4 does not sanitise and escape its preset settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-43724	A Cross Site Scripting (XSS) vulnerability exits in Subrion CMS through 4.2.1 in the Create Page functionality of the admin Account via a SGV file.	4.8	More Details
CVE-2022-0328	The Simple Membership WordPress plugin before 4.0.9 does not have CSRF check when deleting members in bulk, which could allow attackers to make a logged in admin delete them via a CSRF attack	4.7	More Details
CVE-2021-26092	Failure to sanitize input in the SSL VPN web portal of FortiOS 5.2.10 through 5.2.15, 5.4.0 through 5.4.13, 5.6.0 through 5.6.14, 6.0.0 through 6.0.12, 6.2.0 through 6.2.7, 6.4.0 through 6.4.4; and FortiProxy 1.2.0 through 1.2.9, 2.0.0 through 2.0.1 may allow a remote unauthenticated attacker to perform a reflected Cross-site Scripting (XSS) attack by sending a request to the error page with malicious GET parameters.	4.7	More Details
CVE-2022-23653	B2 Command Line Tool is the official command line tool for the backblaze cloud storage service. Linux and Mac releases of the B2 command-line tool version 3.2.0 and below contain a key disclosure vulnerability that, in certain conditions, can be exploited by local attackers through a time-of-check-time-of-use (TOCTOU) race condition. The command line tool saves API keys (and bucket name-to-id mapping) in a local database file (`$XDG_CONFIG_HOME/b2/account_info`, `~/.b2_account_info` or a user-defined path) when `b2 authorize-account` is first run. This happens regardless of whether a valid key is provided or not. When first created, the file is world readable and is (typically a few milliseconds) later altered to be private to the user. If the directory is readable by a local attacker and the user did not yet run `b2 authorize-account` then during the brief period between file creation and permission modification, a local attacker can race to open the file and maintain a handle to it. This allows the local attacker to read the contents after the file after the sensitive information has been saved to it. Users that have not yet run `b2 authorize-account` should upgrade to B2 Command-Line Tool v3.2.1 before running it. Users that have run `b2 authorize-account` are safe if at the time of the file creation no other local users had read access to the local configuration file. Users that have run `b2 authorize-account` where the designated path could be opened by another local user should upgrade to B2 Command-Line Tool v3.2.1 and remove the database and regenerate all application keys. Note that `b2 clear-account` does not remove the database file and it should not be used to ensure that all open handles to the file are invalidated. If B2 Command-Line Tool cannot be upgraded to v3.2.1 due to a dependency conflict, a binary release can be used instead. Alternatively a new version could be installed within a virtualenv, or the permissions can be changed to prevent local users from opening the database file.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23651	b2-sdk-python is a python library to access cloud storage provided by backblaze. Linux and Mac releases of the SDK version 1.14.0 and below contain a key disclosure vulnerability that, in certain conditions, can be exploited by local attackers through a time-of-check-time-of-use (TOCTOU) race condition. SDK users of the SqliteAccountInfo format are vulnerable while users of the InMemoryAccountInfo format are safe. The SqliteAccountInfo saves API keys (and bucket name-to-id mapping) in a local database file ($XDG_CONFIG_HOME/b2/account_info, ~/.b2_account_info or a user-defined path). When first created, the file is world readable and is (typically a few milliseconds) later altered to be private to the user. If the directory containing the file is readable by a local attacker then during the brief period between file creation and permission modification, a local attacker can race to open the file and maintain a handle to it. This allows the local attacker to read the contents after the file after the sensitive information has been saved to it. Consumers of this SDK who rely on it to save data using SqliteAccountInfo class should upgrade to the latest version of the SDK. Those who believe a local user might have opened a handle using this race condition, should remove the affected database files and regenerate all application keys. Users should upgrade to b2-sdk-python 1.14.1 or later.	4.7	More Details
CVE-2022-0743	Cross-site Scripting (XSS) - Stored in GitHub repository getgrav/grav prior to 1.7.31.	4.6	More Details
CVE-2021-44747	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the Fmlib component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine.	4.6	More Details
CVE-2021-38955	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a local user with elevated privileges to cause a denial of service due to a file creation vulnerability in the audit commands. IBM X-Force ID: 211825.	4.4	More Details
CVE-2022-24446	An issue was discovered in Zoho ManageEngine Key Manager Plus 6.1.6. A user, with the level Operator, can see all SSH servers (and user information) even if no SSH server or user is associated to the operator.	4.3	More Details
CVE-2022-22300	A improper handling of insufficient permissions or privileges in Fortinet FortiAnalyzer version 5.6.0 through 5.6.11, FortiAnalyzer version 6.0.0 through 6.0.11, FortiAnalyzer version 6.2.0 through 6.2.9, FortiAnalyzer version 6.4.0 through 6.4.7, FortiAnalyzer version 7.0.0 through 7 .0.2, FortiManager version 5.6.0 through 5.6.11, FortiManager version 6.0.0 through 6.0.11, FortiManager version 6.2.0 through 6.2.9, FortiManager version 6.4.0 through 6.4.7, FortiManager version 7.0.0 through 7.0.2 allows attacker to bypass the device policy and force the password-change action for its user.	4.3	More Details
CVE-2020-10635	Simulation models for KUKA.Sim Pro version 3.1 are hosted by a server maintained by KUKA. When these devices request a model, the server transmits the model in plaintext.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20625	A vulnerability in the Cisco Discovery Protocol service of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the service to restart, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of Cisco Discovery Protocol messages that are processed by the Cisco Discovery Protocol service. An attacker could exploit this vulnerability by sending a series of malicious Cisco Discovery Protocol messages to an affected device. A successful exploit could allow the attacker to cause the Cisco Discovery Protocol service to fail and restart. In rare conditions, repeated failures of the process could occur, which could cause the entire device to restart.	4.3	More Details
CVE-2022-0746	Business Logic Errors in GitHub repository dolibarr/dolibarr prior to 16.0.	4.3	More Details
CVE-2022-0345	The Customize WordPress Emails and Alerts WordPress plugin before 1.8.7 does not have authorisation and CSRF check in its bnfw_search_users AJAX action, allowing any authenticated users to call it and query for user e-mail prefixes (finding the first letter, then the second one, then the third one etc.).	4.3	More Details
CVE-2021-24730	The Logo Showcase with Slick Slider WordPress plugin before 1.2.5 does not have CSRF and authorisation checks in the lswss_save_attachment_data AJAX action, allowing any authenticated users, such as Subscriber, to change title, description, alt text, and URL of arbitrary uploaded media.	4.3	More Details
CVE-2022-24343	In JetBrains YouTrack before 2021.4.31698, a custom logo could be set by a user who has read-only permissions.	4.3	More Details
CVE-2022-0377	Users of the LearnPress WordPress plugin before 4.1.5 can upload an image as a profile avatar after the registration. After this process the user crops and saves the image. Then a "POST" request that contains user supplied name of the image is sent to the server for renaming and cropping of the image. As a result of this request, the name of the user-supplied image is changed with a MD5 value. This process can be conducted only when type of the image is JPG or PNG. An attacker can use this vulnerability in order to rename an arbitrary image file. By doing this, they could destroy the design of the web site.	4.3	More Details
CVE-2021-24913	The Logo Showcase with Slick Slider WordPress plugin before 2.0.1 does not have CSRF check in the lswss_save_attachment_data AJAX action, allowing attackers to make a logged in high privilege user, change title, description, alt text, and URL of arbitrary uploaded media.	4.3	More Details
CVE-2022-21179	Cross-site request forgery (CSRF) vulnerability in EC-CUBE plugin 'Mail Magazine Management Plugin' ver4.0.0 to 4.1.1 (for EC-CUBE 4 series) and ver1.0.0 to 1.0.4 (for EC-CUBE 3 series) allows a remote unauthenticated attacker to hijack the authentication of an administrator via a specially crafted page, and Mail Magazine Templates and/or transmitted history information may be deleted unintendedly.	4.3	More Details
CVE-2020-27958	The Job Composer app in Ohio Supercomputer Center Open OnDemand before 1.7.19 and 1.8.x before 1.8.18 allows remote authenticated users to provide crafted input in a job template.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24688	The Orange Form WordPress plugin through 1.0.1 does not have any authorisation and CSRF checks in all of its AJAX calls, for example the or_delete_filed one which is available to both unauthenticated and authenticated users could allow attackers to delete arbitrary posts.The AJAX calls performing actions on posts also do not ensure that the post belong to them (or that they are allowed to perform such action on it)	4.3	More Details
CVE-2022-22349	IBM Sterling External Authentication Server 3.4.3.2, 6.0.2.0, and 6.0.3.0 is vulnerable to path traversals, due to not properly validating RESTAPI configuration data. An authorized user could import invalid data which could be used for an attack. IBM X-Force ID: 220144.	4.3	More Details
CVE-2020-15936	A improper input validation in Fortinet FortiGate version 6.4.3 and below, version 6.2.5 and below, version 6.0.11 and below, version 5.6.13 and below allows attacker to disclose sensitive information via SNI Client Hello TLS packets.	2.6	More Details
CVE-2022-24719	Fluture-Node is a FP-style HTTP and streaming utils for Node based on Fluture. Using `followRedirects` or `followRedirectsWith` with any of the redirection strategies built into fluture-node 4.0.0 or 4.0.1, paired with a request that includes confidential headers such as Authorization or Cookie, exposes you to a vulnerability where, if the destination server were to redirect the request to a server on a third-party domain, or the same domain over unencrypted HTTP, the headers would be included in the follow-up request and be exposed to the third party, or potential http traffic sniffing. The redirection strategies made available in version 4.0.2 automatically redact confidential headers when a redirect is followed across to another origin. A workaround has been identified by using a custom redirection strategy via the `followRedirectsWith` function. The custom strategy can be based on the new strategies available in fluture-node@4.0.2.	2.6	More Details
CVE-2021-3883	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3884	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3886	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3877	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3876	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3880	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3893	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3887	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-36819	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-3937	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3940	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2022-25019	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-38602. Reason: This candidate is a reservation duplicate of CVE-2021-38602. Notes: All CVE users should reference CVE-2021-38602 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-0655	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-3873	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-36820	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-3870	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3868	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-36818	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2022-25029	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-25096. Reason: This candidate is a duplicate of CVE-2022-25096. Notes: All CVE users should reference CVE-2022-25096 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-36817	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36816	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-36815	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-36814	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-36813	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-36812	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-36811	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-36810	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27000	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27016	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27013	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27012	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27011	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27010	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-27008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-3867	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-3871	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details