SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 June 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-2022-1517	LRM utilizes elevated privileges. An unauthenticated malicious actor can upload and execute code remotely at the operating system level, which can allow an attacker to change settings, configurations, software, or access sensitive data on the affected produc. An attacker could also exploit this vulnerability to access APIs not intended for general use and interact through the network.	10.0	More Details
CVE-2022-1518	LRM contains a directory traversal vulnerability that can allow a malicious actor to upload outside the intended directory structure.	10.0	More Details
CVE-2022-1519	LRM does not restrict the types of files that can be uploaded to the affected product. A malicious actor can upload any file type, including executable code that allows for a remote code exploit.	10.0	More Details
CVE-2022-2104	The www-data (Apache web server) account is configured to run sudo with no password for many commands (including /bin/sh and /bin/bash).	9.9	More Details
CVE-2021-40954	Laiketui 3.5.0 is affected by an arbitrary file upload vulnerability that can allow an attacker to execute arbitrary code.	9.8	More Details
CVE-2022-34064	The Zibal package in PyPI v1.0.0 was discovered to contain a code execution backdoor. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-33003	The watools package in PyPI v0.0.1 to v0.0.8 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33004	The Beginner package in PyPI v0.0.2 to v0.0.4 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34053	The DR-Web-Engine package in PyPI v0.2.0b0 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34054	The Perdido package in PyPI v0.0.1 to v0.0.2 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34055	The drxhello package in PyPI v0.0.1 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34056	The Watertools package in PyPI v0.0.0 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34057	The Scoptrial package in PyPI version v0.0.5 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34059	The Sixfab-Tool in PyPI v0.0.2 to v0.0.3 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34060	The Togglee package in PyPI version v0.0.8 was discovered to contain a code execution backdoor. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34061	The Catly-Translate package in PyPI v0.0.3 to v0.0.5 was discovered to contain a code execution backdoor. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34066	The Texercise package in PyPI v0.0.1 to v0.0.12 was discovered to contain a code execution backdoor. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-34065	The Rondolu-YT-Concate package in PyPI v0.1.0 was discovered to contain a code execution backdoor. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-22980	A Spring Data MongoDB application is vulnerable to SpEL Injection when using @Query or @Aggregation-annotated query methods with SpEL expressions that contain query parameter placeholders for value binding if the input is not sanitized.	9.8	More Details
CVE-2022-1574	The HTML2WP WordPress plugin through 1.0.0 does not have authorisation and CSRF checks when importing files, and does not validate them, as a result, unauthenticated attackers can upload arbitrary files (such as PHP) on the remote server	9.8	More Details
CVE-2022-2216	Server-Side Request Forgery (SSRF) in GitHub repository ionicabizau/parse-url prior to 7.0.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32092	D-Link DIR-645 v1.03 was discovered to contain a command injection vulnerability via the QUERY_STRING parameter at __ajax_explorer.sgi.	9.8	More Details
CVE-2022-32994	Halo CMS v1.5.3 was discovered to contain an arbitrary file upload vulnerability via the component /api/admin/attachments/upload.	9.8	More Details
CVE-2022-32995	Halo CMS v1.5.3 was discovered to contain a Server-Side Request Forgery (SSRF) via the template remote download function.	9.8	More Details
CVE-2022-34132	Benjamin BALET Jorani v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at application/controllers/Leaves.php.	9.8	More Details
CVE-2022-31056	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. In affected versions all assistance forms (Ticket/Change/Problem) permit sql injection on the actor fields. This issue has been resolved in version 10.0.2 and all affected users are advised to upgrade.	9.8	More Details
CVE-2022-31061	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. In affected versions there is a SQL injection vulnerability which is possible on login page. No user credentials are required to exploit this vulnerability. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue.	9.8	More Details
CVE-2022-31885	Marval MSM v14.19.0.12476 is vulnerable to OS Command Injection due to the insecure handling of VBScripts.	9.8	More Details
CVE-2020-19896	File inclusion vulnerability in Minicms v1.9 allows remote attackers to execute arbitary PHP code via post-edit.php.	9.8	More Details
CVE-2022-33002	The KGExplore package in PyPI v0.1.1 to v0.1.2 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-33001	The AAmiles package in PyPI v0.1.0 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-33000	The ML-Scanner package in PyPI v0.1.0 to v0.1.5 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-2103	An attacker with weak credentials could access the TCP port via an open FTP port, allowing an attacker to read sensitive files and write to remotely executable directories.	9.8	More Details
CVE-2022-31361	Docebo Community Edition v4.0.5 and below was discovered to contain a SQL injection vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31787	IdeaTMS 2022 is vulnerable to SQL Injection via the PATH_INFO	9.8	More Details
CVE-2022-32554	Pure Storage FlashArray products running Purity//FA 6.2.0 - 6.2.3, 6.1.0 - 6.1.12, 6.0.0 - 6.0.8, 5.3.0 - 5.3.17, 5.2.x and prior Purity//FA releases, and Pure Storage FlashBlade products running Purity//FB 3.3.0, 3.2.0 - 3.2.4, 3.1.0 - 3.1.12, 3.0.x and prior Purity//FB releases are vulnerable to possibly exposed credentials for accessing the product's management interface. The password may be known outside Pure Storage and could be used on an affected system, if reachable, to execute arbitrary instructions with root privileges. No other Pure Storage products or services are affected. Remediation is available from Pure Storage via a self-serve "opt-in" patch, manual patch application or a software upgrade to an unaffected version of Purity software.	9.8	More Details
CVE-2022-33127	The function that calls the diff tool in Diffy 3.4.1 does not properly handle double quotes in a filename when run in a windows environment. This allows attackers to execute arbitrary commands via a crafted string.	9.8	More Details
CVE-2022-31802	In CODESYS Gateway Server V2 for versions prior to V2.3.9.38 only a part of the the specified password is been compared to the real CODESYS Gateway password. An attacker may perform authentication by specifying a small password that matches the corresponding part of the longer real CODESYS Gateway password.	9.8	More Details
CVE-2022-31806	In CODESYS V2 PLCWinNT and Runtime Toolkit 32 in versions prior to V2.4.7.57 password protection is not enabled by default and there is no information or prompt to enable password protection at login in case no password is set at the controller.	9.8	More Details
CVE-2022-1668	Weak default root user credentials allow remote attackers to easily obtain OS superuser privileges over the open TCP port for SSH.	9.8	More Details
CVE-2022-21829	Concrete CMS Versions 9.0.0 through 9.0.2 and 8.5.7 and below can download zip files over HTTP and execute code from those zip files which could lead to an RCE. Fixed by enforcing 'concrete_secure' instead of 'concrete'. Concrete now only makes requests over https even a request comes in via http. Concrete CMS security team ranked this 8 with CVSS v3.1 vector: AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Credit goes to Anna for reporting HackerOne 1482520.	9.8	More Details
CVE-2022-32999	The cloudlabeling package in PyPI v0.0.1 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-28620	A remote authentication bypass vulnerability was discovered in HPE Cray Legacy Shasta System Solutions; HPE Slingshot; and HPE Cray EX supercomputers versions: Prior to node controller firmware associated with HPE Cray EX liquid cooled blades, and all versions of chassis controller firmware associated with HPE Cray EX liquid cooled cabinets prior to 1.6.27/1.5.33/1.4.27; All Slingshot versions prior to 1.7.2; All versions of node controller firmware associated with HPE Cray EX liquid cooled blades, and all versions of chassis controller firmware associated with HPE Cray EX liquid cooled cabinets prior to 1.6.27/1.5.33/1.4.27. HPE has provided a software update to resolve this vulnerability in HPE Cray Legacy Shasta System Solutions, HPE Slingshot, and HPE Cray EX Supercomputers.	9.8	More Details
CVE-2022-31887	Marval MSM v14.19.0.12476 has a 0-Click Account Takeover vulnerability which allows an attacker to change any user's password in the organization, this means that the user can also escalate achieve Privilege Escalation by changing the administrator password.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31767	IBM CICS TX Standard and Advanced 11.1 could allow a remote attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 227980.	9.8	More Details
CVE-2022-32998	The cryptoasset-data-downloader package in PyPI v1.0.0 to v1.0.1 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-32997	The RootInteractive package in PyPI v0.0.5 to v0.0.19b0 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2021-38945	IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 could allow a remote attacker to upload arbitrary files, caused by improper content validation. IBM X-Force ID: 211238.	9.8	More Details
CVE-2022-32996	The django-navbar-client package of v0.9.50 to v1.0.1 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-30885	The pyesasky for python, as distributed on PyPI, included a code-execution backdoor inserted by a third party. The current version, without this backdoor, is 1.2.0-1.4.2.	9.8	More Details
CVE-2021-39409	A vulnerability exists in Online Student Rate System v1.0 that allows any user to register as an administrator without needing to be authenticated.	9.8	More Details
CVE-2022-29168	Wire is a secure messaging application. Wire is vulnerable to arbitrary HTML and Javascript execution via insufficient escaping when rendering `@mentions` in the wire-webapp. If a user receives and views a malicious message, arbitrary code is injected and executed in the context of the victim allowing the attacker to fully control the user account. Wire-desktop clients that are connected to a vulnerable wire-webapp version are also vulnerable to this attack. The issue has been fixed in wire-webapp 2022-05-04-production.0 and is already deployed on all Wire managed services. On-premise instances of wire-webapp need to be updated to docker tag 2022-05-04-production.0-v0.29.7-0-a6f2ded or wire-server 2022-05-04 (chart/4.11.0) or later. No known workarounds exist.	9.6	More Details
CVE-2022-31229	Dell PowerScale OneFS, 8.2.x through 9.3.0.x, contain an error message with sensitive information. An administrator could potentially exploit this vulnerability, leading to disclosure of sensitive information. This sensitive information can be used to access sensitive resources.	9.6	More Details
CVE-2022-2102	Controls limiting uploads to certain file extensions may be bypassed. This could allow an attacker to intercept the initial file upload page response and modify the associated code. This modified code can be forwarded and used by a script loaded later in the sequence, allowing for arbitrary file upload into a location where PHP scripts may be executed.	9.4	More Details
CVE-2022-2105	Client-side JavaScript controls may be bypassed to change user credentials and permissions without authentication, including a “root” user level meant only for the vendor. Web server root level access allows for changing of safety critical parameters.	9.4	More Details
CVE-2022-34181	Jenkins xUnit Plugin 3.0.8 and earlier implements an agent-to-controller message that creates a user-specified directory if it doesn't exist, and parsing files inside it as test results, allowing attackers able to control agent processes to create an arbitrary directory on the Jenkins controller or to obtain test results from existing files in an attacker-specified directory.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20829	A vulnerability in the packaging of Cisco Adaptive Security Device Manager (ASDM) images and the validation of those images by Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker with administrative privileges to upload an ASDM image that contains malicious code to a device that is running Cisco ASA Software. This vulnerability is due to insufficient validation of the authenticity of an ASDM image during its installation on a device that is running Cisco ASA Software. An attacker could exploit this vulnerability by installing a crafted ASDM image on the device that is running Cisco ASA Software and then waiting for a targeted user to access that device using ASDM. A successful exploit could allow the attacker to execute arbitrary code on the machine of the targeted user with the privileges of that user on that machine. Notes: To successfully exploit this vulnerability, the attacker must have administrative privileges on the device that is running Cisco ASA Software. Potential targets are limited to users who manage the same device that is running Cisco ASA Software using ASDM. Cisco has released and will release software updates that address this vulnerability.	9.1	More Details
CVE-2022-1953	The Product Configurator for WooCommerce WordPress plugin before 1.2.32 suffers from an arbitrary file deletion vulnerability via an AJAX action, accessible to unauthenticated users, which accepts user input that is being used in a path and passed to unlink() without validation first	9.1	More Details
CVE-2022-30117	Concrete 8.5.7 and below as well as Concrete 9.0 through 9.0.2 allow traversal in /index.php/ccm/system/file/upload which could result in an Arbitrary File Delete exploit. This was remediated by sanitizing /index.php/ccm/system/file/upload to ensure Concrete doesn’t allow traversal and by changing isFullChunkFilePresent to have an early false return when input doesn't match expectations.Concrete CMS Security team ranked this 5.8 with CVSS v3.1 vector AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H. Credit to Siebene for reporting.	9.1	More Details
CVE-2022-33128	RG-EG series gateway EG350 EG_RGOS 11.1(6) was discovered to contain a SQL injection vulnerability via the function get_alarmAction at /alarm_pi/alarmService.php.	9.1	More Details
CVE-2022-1521	LRM does not implement authentication or authorization by default. A malicious actor can inject, replay, modify, and/or intercept sensitive data.	9.1	More Details
CVE-2022-31098	Weave GitOps is a simple open source developer platform for people who want cloud native applications, without needing Kubernetes expertise. A vulnerability in the logging of Weave GitOps could allow an authenticated remote attacker to view sensitive cluster configurations, aka KubeConfg, of registered Kubernetes clusters, including the service account tokens in plain text from Weave GitOps's pod logs on the management cluster. An unauthorized remote attacker can also view these sensitive configurations from external log storage if enabled by the management cluster. This vulnerability is due to the client factory dumping cluster configurations and their service account tokens when the cluster manager tries to connect to an API server of a registered cluster, and a connection error occurs. An attacker could exploit this vulnerability by either accessing logs of a pod of Weave GitOps, or from external log storage and obtaining all cluster configurations of registered clusters. A successful exploit could allow the attacker to use those cluster configurations to manage the registered Kubernetes clusters. This vulnerability has been fixed by commit 567356f471353fb5c676c77f5abc2a04631d50ca. Users should upgrade to Weave GitOps core version v0.8.1-rc.6 or newer. There is no known workaround for this vulnerability.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31035	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v1.0.0 are vulnerable to a cross-site scripting (XSS) bug allowing a malicious user to inject a `javascript:` link in the UI. When clicked by a victim user, the script will execute with the victim's permissions (up to and including admin). The script would be capable of doing anything which is possible in the UI or via the API, such as creating, modifying, and deleting Kubernetes resources. A patch for this vulnerability has been released in the following Argo CD versions: v2.4.1, v2.3.5, v2.2.10 and v2.1.16. There are no completely-safe workarounds besides upgrading.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-34134	Benjamin BALET Jorani v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /application/controllers/Users.php.	8.8	More Details
CVE-2022-32392	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/actions/manage_action.php:4	8.8	More Details
CVE-2022-31362	Docebo Community Edition v4.0.5 and below was discovered to contain an arbitrary file upload vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2022-31395	Algo Communication Products Ltd. 8373 IP Zone Paging Adapter Firmware 1.7.6 allows attackers to perform a directory traversal via a web request sent to /fm-data.lua.	8.8	More Details
CVE-2022-32534	The Bosch Ethernet switch PRA-ES8P2S with software version 1.01.05 and earlier was found to be vulnerable to command injection through its diagnostics web interface. This allows execution of shell commands.	8.8	More Details
CVE-2022-32536	The user access rights validation in the web server of the Bosch Ethernet switch PRA-ES8P2S with software version 1.01.05 was insufficient. This would allow a non-administrator user to obtain administrator user access rights.	8.8	More Details
CVE-2022-32552	Pure Storage FlashArray products running Purity//FA 6.2.0 - 6.2.3, 6.1.0 - 6.1.12, 6.0.0 - 6.0.8, 5.3.0 - 5.3.17, 5.2.x and prior Purity//FA releases, and Pure Storage FlashBlade products running Purity//FB 3.3.0, 3.2.0 - 3.2.4, 3.1.0 - 3.1.12, 3.0.x and prior Purity//FB releases are vulnerable to a privilege escalation via the manipulation of Python environment variables which can be exploited by a logged-in user to escape a restricted shell to an unrestricted shell with root privileges. No other Pure Storage products or services are affected. Remediation is available from Pure Storage via a self-serve “opt-in” patch, manual patch application or a software upgrade to an unaffected version of Purity software.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32553	Pure Storage FlashArray products running Purity//FA 6.2.0 - 6.2.3, 6.1.0 - 6.1.12, 6.0.0 - 6.0.8, 5.3.0 - 5.3.17, 5.2.x and prior Purity//FA releases, and Pure Storage FlashBlade products running Purity//FB 3.3.0, 3.2.0 - 3.2.4, 3.1.0 - 3.1.12, 3.0.x and prior Purity//FB releases are vulnerable to a privilege escalation via the manipulation of environment variables which can be exploited by a logged-in user to escape a restricted shell to an unrestricted shell with root privileges. No other Pure Storage products or services are affected. Remediation is available from Pure Storage via a self-serve “opt-in” patch, manual patch application or a software upgrade to an unaffected version of Purity software.	8.8	More Details
CVE-2022-2140	Elcomplus SmartICS v2.3.4.0 does not neutralize user-controllable input, which allows an authenticated user to inject arbitrary code into specific parameters.	8.8	More Details
CVE-2022-33007	TRENDnet Wi-Fi routers TEW751DR v1.03 and TEW-752DRU v1.03 were discovered to contain a stack overflow via the function genacgi_main.	8.8	More Details
CVE-2022-34200	A cross-site request forgery (CSRF) vulnerability in Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier allows attackers to connect to an attacker-specified URL.	8.8	More Details
CVE-2022-34203	A cross-site request forgery (CSRF) vulnerability in Jenkins EasyQA Plugin 1.0 and earlier allows attackers to connect to an attacker-specified HTTP server.	8.8	More Details
CVE-2022-31086	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. In versions prior to 8.0 incorrect regular expressions allow to upload PHP scripts to config/templates/pdf. This vulnerability could lead to a Remote Code Execution if the /config/templates/pdf/ directory is accessible for remote users. This is not a default configuration of LAM. This issue has been fixed in version 8.0. There are no known workarounds for this issue.	8.8	More Details
CVE-2022-34300	In tinyexr 1.0.1, there is a heap-based buffer over-read in tinyexr::DecodePixelData.	8.8	More Details
CVE-2013-1916	In WordPress Plugin User Photo 0.9.4, when a photo is uploaded, it is only partially validated and it is possible to upload a backdoor on the server hosting WordPress. This backdoor can be called (executed) even if the photo has not been yet approved.	8.8	More Details
CVE-2022-32391	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/actions/view_action.php:4	8.8	More Details
CVE-2022-32393	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/cells/view_cell.php:4	8.8	More Details
CVE-2022-22967	An issue was discovered in SaltStack Salt in versions before 3002.9, 3003.5, 3004.2. PAM auth fails to reject locked accounts, which allows a previously authorized user whose account is locked still run Salt commands when their account is locked. This affects both local shell accounts with an active session and salt-api users that authenticate via PAM eauth.	8.8	More Details
CVE-2022-32394	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/view_inmate.php:3	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32395	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/crimes/manage_crime.php:4	8.8	More Details
CVE-2022-32396	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/visits/manage_visit.php:4	8.8	More Details
CVE-2022-32397	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/visits/view_visit.php:4	8.8	More Details
CVE-2022-32398	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/cells/manage_cell.php:4	8.8	More Details
CVE-2022-32399	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/crimes/view_crime.php:4	8.8	More Details
CVE-2022-32401	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/manage_privilege.php:4	8.8	More Details
CVE-2022-32402	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/prisons/manage_prison.php:4	8.8	More Details
CVE-2022-32403	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/manage_record.php:4	8.8	More Details
CVE-2022-32404	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/manage_inmate.php:3	8.8	More Details
CVE-2022-32405	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/prisons/view_prison.php:4	8.8	More Details
CVE-2021-41635	When installed as Windows service MELAG FTP Server 2.2.0.4 is run as SYSTEM user, which grants remote attackers to abuse misconfigurations or vulnerabilities with administrative access over the entire host system.	8.8	More Details
CVE-2022-32137	In multiple CODESYS products, a low privileged remote attacker may craft a request, which may cause a heap-based buffer overflow, resulting in a denial-of-service condition or memory overwrite. User interaction is not required.	8.8	More Details
CVE-2022-32138	In multiple CODESYS products, a remote attacker may craft a request which may cause an unexpected sign extension, resulting in a denial-of-service condition or memory overwrite.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30707	Violation of secure design principles exists in the communication of CAMS for HIS. Affected products and versions are CENTUM series where LHS4800 is installed (CENTUM CS 3000 and CENTUM CS 3000 Small R3.08.10 to R3.09.00), CENTUM series where CAMS function is used (CENTUM VP, CENTUM VP Small, and CENTUM VP Basic R4.01.00 to R4.03.00), CENTUM series regardless of the use of CAMS function (CENTUM VP, CENTUM VP Small, and CENTUM VP Basic R5.01.00 to R5.04.20 and R6.01.00 to R6.09.00), Exaopc R3.72.00 to R3.80.00 (only if NTPF100-S6 'For CENTUM VP Support CAMS for HIS' is installed), B/M9000 CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01). If an adjacent attacker successfully compromises a computer using CAMS for HIS software, they can use credentials from the compromised machine to access data from another machine using CAMS for HIS software. This can lead to a disabling of CAMS for HIS software functions on any affected machines, or information disclosure/alteration.	8.8	More Details
CVE-2022-32143	In multiple CODESYS products, file download and upload function allows access to internal files in the working directory e.g. firmware files of the PLC. All requests are processed on the controller only if no level 1 password is configured on the controller or if remote attacker has previously successfully authenticated himself to the controller. A successful Attack may lead to a denial of service, change of local files, or drain of confidential Information. User interaction is not required	8.8	More Details
CVE-2021-40553	piwigo 11.5.0 is affected by a remote code execution (RCE) vulnerability in the LocalFiles Editor.	8.8	More Details
CVE-2022-31883	Marval MSM v14.19.0.12476 is has an Insecure Direct Object Reference (IDOR) vulnerability. A low privilege user is able to see other users API Keys including the Admins API Keys.	8.8	More Details
CVE-2021-26636	Stored XSS and SQL injection vulnerability in MaxBoard could lead to occur Remote Code Execution, which could lead to information exposure and privilege escalation.	8.8	More Details
CVE-2021-26637	There is no account authentication and permission check logic in the firmware and existing apps of SiHAS's SGW-300, ACM-300, GCM-300, so unauthorized users can remotely control the device.	8.8	More Details
CVE-2022-31034	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v0.11.0 are vulnerable to a variety of attacks when an SSO login is initiated from the Argo CD CLI or UI. The vulnerabilities are due to the use of insufficiently random values in parameters in Oauth2/OIDC login flows. In each case, using a relatively-predictable (time-based) seed in a non-cryptographically-secure pseudo-random number generator made the parameter less random than required by the relevant spec or by general best practices. In some cases, using too short a value made the entropy even less sufficient. The attacks on login flows which are meant to be mitigated by these parameters are difficult to accomplish but can have a high impact potentially granting an attacker admin access to Argo CD. Patches for this vulnerability has been released in the following Argo CD versions: v2.4.1, v2.3.5, v2.2.10 and v2.1.16. There are no known workarounds for this vulnerability.	8.3	More Details
CVE-2022-31106	Underscore.deep is a collection of Underscore mixins that operate on nested objects. Versions of `underscore.deep` prior to version 0.5.3 are vulnerable to a prototype pollution vulnerability. An attacker can craft a malicious payload and pass it to `deepFromFlat`, which would pollute any future Objects created. Any users that have `deepFromFlat` or `deepPick` (due to its dependency on `deepFromFlat`) in their code should upgrade to version 0.5.3 as soon as possible. Users unable to upgrade may mitigate this issue by modifying `deepFromFlat` to prevent specific keywords which will prevent this from happening.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1572	The HTML2WP WordPress plugin through 1.0.0 does not have authorisation and CSRF checks in an AJAX action, available to any authenticated users such as subscriber, which could allow them to delete arbitrary file	8.1	More Details
CVE-2022-31084	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. In versions prior to 8.0 There are cases where LAM instantiates objects from arbitrary classes. An attacker can inject the first constructor argument. This can lead to code execution if non-LAM classes are instantiated that execute code during object creation. This issue has been fixed in version 8.0.	8.1	More Details
CVE-2022-34299	There is a heap-based buffer over-read in libdwarf 0.4.0. This issue is related to dwarf_global_formref_b.	8.1	More Details
CVE-2022-32142	Multiple CODESYS Products are prone to a out-of bounds read or write access. A low privileged remote attacker may craft a request with invalid offset, which can cause an out-of-bounds read or write access, resulting in denial-of-service condition or local memory overwrite, which can lead to a change of local files. User interaction is not required.	8.1	More Details
CVE-2022-31101	prestashop/blockwishlist is a prestashop extension which adds a block containing the customer's wishlists. In affected versions an authenticated customer can perform SQL injection. This issue is fixed in version 2.1.1. Users are advised to upgrade. There are no known workarounds for this issue.	8.1	More Details
CVE-2022-33121	A Cross-Site Request Forgery (CSRF) in MiniCMS v1.11 allows attackers to arbitrarily delete local .dat files via clicking on a malicious link.	8.1	More Details
CVE-2022-31230	Dell PowerScale OneFS, versions 8.2.x-9.2.x, contain broken or risky cryptographic algorithm. A remote unprivileged malicious attacker could potentially exploit this vulnerability, leading to full system access.	8.1	More Details
CVE-2022-33202	Authentication bypass vulnerability in the setup screen of L2Blocker(on-premise) Ver4.8.5 and earlier and L2Blocker(Cloud) Ver4.8.5 and earlier allows an adjacent attacker to perform an unauthorized login and obtain the stored information or cause a malfunction of the device by using alternative paths or channels for Sensor.	8.1	More Details
CVE-2022-1965	Multiple products of CODESYS implement a improper error handling. A low privilege remote attacker may craft a request, which is not properly processed by the error handling. In consequence, the file referenced by the request could be deleted. User interaction is not required.	8.1	More Details
CVE-2022-1903	The ARMember WordPress plugin before 3.4.8 is vulnerable to account takeover (even the administrator) due to missing nonce and authorization checks in an AJAX action available to unauthenticated users, allowing them to change the password of arbitrary users by knowing their username	8.1	More Details
CVE-2022-33108	XPDF v4.04 was discovered to contain a stack overflow vulnerability via the Object::Copy class of object.cc files.	7.8	More Details
CVE-2022-33028	LibreDWG v0.12.4.4608 was discovered to contain a heap buffer overflow via the function dwg_add_object at decode.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23763	Origin validation error vulnerability in NeoRS's ActiveX moudle allows attackers to download and execute arbitrary files. Remote attackers can use this vulerability to encourage users to access crafted web pages, causing damage such as malicious code infections.	7.8	More Details
CVE-2020-21046	A local privilege escalation vulnerability was identified within the "luminati_net_updater_win_eagleget_com" service in EagleGet Downloader version 2.1.5.20 Stable. This issue allows authenticated non-administrative user to escalate their privilege and conduct code execution as a SYSTEM privilege.	7.8	More Details
CVE-2022-31087	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. In versions prior to 8.0 the tmp directory, which is accessible by /lam/tmp/, allows interpretation of .php (and .php5/.php4/.phpt/etc) files. An attacker capable of writing files under www-data privileges can write a web-shell into this directory, and gain a Code Execution on the host. This issue has been fixed in version 8.0. Users unable to upgrade should disallow executing PHP scripts in (/var/lib/ldap-account-manager/)tmp directory.	7.8	More Details
CVE-2022-28619	A potential security vulnerability has been identified in the installer of HPE Version Control Repository Manager. The vulnerability could allow local escalation of privilege. HPE has made the following software update to resolve the vulnerability in HPE Version Control Repository Manager installer 7.6.14.0.	7.8	More Details
CVE-2022-33034	LibreDWG v0.12.4.4608 was discovered to contain a stack overflow via the function copy_bytes at decode_r2007.c.	7.8	More Details
CVE-2022-33033	LibreDWG v0.12.4.4608 was discovered to contain a double-free via the function dwg_read_file at dwg.c.	7.8	More Details
CVE-2022-33032	LibreDWG v0.12.4.4608 was discovered to contain a heap-buffer-overflow via the function decode_preR13_section_hdr at decode_r11.c.	7.8	More Details
CVE-2022-33026	LibreDWG v0.12.4.4608 was discovered to contain a heap buffer overflow via the function bit_calc_CRC at bits.c.	7.8	More Details
CVE-2022-33027	LibreDWG v0.12.4.4608 was discovered to contain a heap-use-after-free via the function dwg_add_handleref at dwg.c.	7.8	More Details
CVE-2022-2206	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-33025	LibreDWG v0.12.4.4608 was discovered to contain a heap-use-after-free via the function decode_preR13_section at decode_r11.c.	7.8	More Details
CVE-2022-2175	Buffer Over-read in GitHub repository vim/vim prior to 8.2.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2210	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-2182	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-2183	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-2207	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-31090	Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.	7.7	More Details
CVE-2022-31091	Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.	7.7	More Details
CVE-2022-1746	The authentication mechanism used by poll workers to administer voting using the tested version of Dominion Voting Systems ImageCast X can expose cryptographic secrets used to protect election information. An attacker could leverage this vulnerability to gain access to sensitive information and perform privileged actions, potentially affecting other election equipment.	7.6	More Details
CVE-2022-33095	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/jobfairol/resumelist.	7.5	More Details
CVE-2022-34296	In Zalando Skipper before 0.13.218, a query predicate could be bypassed via a prepared request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40899	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in repo-git-downloader v0.1.1 when downloading crafted invalid git repositories.	7.5	More Details
CVE-2022-28168	In Brocade SANnav before Brocade SANnav v2.2.0.2 and Brocade SANnav2.1.1.8, encoded scp-server passwords are stored using Base64 encoding, which could allow an attacker able to access log files to easily decode the passwords.	7.5	More Details
CVE-2021-40893	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in validate-data v0.1.1 when validating crafted invalid emails.	7.5	More Details
CVE-2022-0722	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository ionicabizau/parse-url prior to 7.0.0.	7.5	More Details
CVE-2021-41689	DCMTK through 3.6.6 does not handle string copy properly. Sending specific requests to the dcmqrdb program, it would query its database and copy the result even if the result is null, which can incur a head-based overflow. An attacker can use it to launch a DoS attack.	7.5	More Details
CVE-2022-24893	ESP-IDF is the official development framework for Espressif SoCs. In Espressif's Bluetooth Mesh SDK (`ESP-BLE-MESH`), a memory corruption vulnerability can be triggered during provisioning, because there is no check for the `SegN` field of the Transaction Start PDU. This can result in memory corruption related attacks and potentially attacker gaining control of the entire system. Patch commits are available on the 4.1, 4.2, 4.3 and 4.4 branches and users are recommended to upgrade. The upgrade is applicable for all applications and users of `ESP-BLE-MESH` component from `ESP-IDF`. As it is implemented in the Bluetooth Mesh stack, there is no workaround for the user to fix the application layer without upgrading the underlying firmware.	7.5	More Details
CVE-2022-1667	Client-side JavaScript controls may be bypassed by directly running a JS function to reboot the PLC (e.g., from the browser console) or by loading the corresponding, browser accessible PHP script	7.5	More Details
CVE-2022-28621	A remote disclosure of sensitive information vulnerability was discovered in HPE NonStop DSM/SCM version: T6031H03^ADP. HPE has provided a software update to resolve this vulnerability in HPE NonStop DSM/SCM.	7.5	More Details
CVE-2022-28166	In Brocade SANnav version before SANN2.2.0.2 and Brocade SANNav before 2.1.1.8, the implementation of TLS/SSL Server Supports the Use of Static Key Ciphers (ssl-static-key-ciphers) on ports 443 & 18082.	7.5	More Details
CVE-2022-33096	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/resume/index.	7.5	More Details
CVE-2022-33024	There is an Assertion `int decode_preR13_entities(BITCODE_RL, BITCODE_RL, unsigned int, BITCODE_RL, BITCODE_RL, Bit_Chain *, Dwg_Data *' failed at dwg2dxf: decode.c:5801 in libredwg v0.12.4.4608.	7.5	More Details
CVE-2021-40900	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in regexfn v1.0.5 when validating crafted invalid emails.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26477	The Security Team noticed that the termination condition of the for loop in the readExternal method is a controllable variable, which, if tampered with, may lead to CPU exhaustion. As a fix, we added an upper bound and termination condition in the read and write logic. We classify it as a "low-priority but useful improvement". SystemDS is a distributed system and needs to serialize/deserialize data but in many code paths (e.g., on Spark broadcast/shuffle or writing to sequence files) the byte stream is anyway protected by additional CRC fingerprints. In this particular case though, the number of decoders is upper-bounded by twice the number of columns, which means an attacker would need to modify two entries in the byte stream in a consistent manner. By adding these checks robustness was strictly improved with almost zero overhead. These code changes are available in versions higher than 2.2.1.	7.5	More Details
CVE-2021-41688	DCMTK through 3.6.6 does not handle memory free properly. The object in the program is free but its address is still used in other locations. Sending specific requests to the dcmqrdb program will incur a double free. An attacker can use it to launch a DoS attack.	7.5	More Details
CVE-2022-22390	IBM Db2 for Linux, UNIX and Windows 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an information disclosure caused by improper privilege management when table function is used. IBM X-Force ID: 221973.	7.5	More Details
CVE-2022-21231	All versions of package deep-get-set are vulnerable to Prototype Pollution via the 'deep' function. **Note:** This vulnerability derives from an incomplete fix of [CVE-2020-7715] (https://security.snyk.io/vuln/SNYK-JS-DEEPGETSET-598666)	7.5	More Details
CVE-2021-41687	DCMTK through 3.6.6 does not handle memory free properly. The program malloc a heap memory for parsing data, but does not free it when error in parsing. Sending specific requests to the dcmqrdb program incur the memory leak. An attacker can use it to launch a DoS attack.	7.5	More Details
CVE-2021-40901	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in scniro-validator v1.0.1 when validating crafted invalid emails.	7.5	More Details
CVE-2021-40956	LaiKetui v3.5.0 has SQL injection in the background through the menu management function, and sensitive data can be obtained.	7.5	More Details
CVE-2022-31805	In the CODESYS Development System multiple components in multiple versions transmit the passwords for the communication between clients and servers unprotected.	7.5	More Details
CVE-2022-31804	The CODESYS Gateway Server V2 does not verifiy that the size of a request is within expected limits. An unauthenticated attacker may allocate an arbitrary amount of memory, which may lead to a crash of the Gateway due to an out-of-memory condition.	7.5	More Details
CVE-2022-28622	A potential security vulnerability has been identified in HPE StoreOnce Software. The SSH server supports weak key exchange algorithms which could lead to remote unauthorized access. HPE has made the following software update to resolve the vulnerability in HPE StoreOnce Software 4.3.2.	7.5	More Details
CVE-2022-29519	Cleartext transmission of sensitive information vulnerability exists in STARDOM FCN Controller and FCJ Controller R1.01 to R4.31, which may allow an adjacent attacker to login the affected products and alter device configuration settings or tamper with device firmware.	7.5	More Details
CVE-2021-41638	The authentication checks of the MELAG FTP Server in version 2.2.0.4 are incomplete, which allows a remote attacker to access local files only by using a valid username.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28171	The web module in some Hikvision Hybrid SAN/Cluster Storage products have the following security vulnerability. Due to the insufficient input validation, attacker can exploit the vulnerability to execute restricted commands by sending messages with malicious commands to the affected device.	7.5	More Details
CVE-2021-40892	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in validate-color v2.1.0 when handling crafted invalid rgb(a) strings.	7.5	More Details
CVE-2021-40895	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in todo-regex v0.1.1 when matching crafted invalid TODO statements.	7.5	More Details
CVE-2021-41690	DCMTK through 3.6.6 does not handle memory free properly. The malloced memory for storing all file information are recorded in a global variable LST and are not freed properly. Sending specific requests to the dcmqrdb program can incur a memory leak. An attacker can use it to launch a DoS attack.	7.5	More Details
CVE-2022-21952	A Missing Authentication for Critical Function vulnerability in spacewalk-java of SUSE Manager Server 4.1, SUSE Manager Server 4.2 allows remote attackers to easily exhaust available disk resources leading to DoS. This issue affects: SUSE Manager Server 4.1 spacewalk-java versions prior to 4.1.46. SUSE Manager Server 4.2 spacewalk-java versions prior to 4.2.37.	7.5	More Details
CVE-2021-40896	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in that-value v0.1.3 when validating crafted invalid emails.	7.5	More Details
CVE-2021-40897	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in split-html-to-chars v1.0.5 when splitting crafted invalid htmls.	7.5	More Details
CVE-2021-40894	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in underscore-99xp v1.7.2 when the deepValueSearch function is called.	7.5	More Details
CVE-2021-40898	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in scaffold-helper v1.2.0 when copying crafted invalid files.	7.5	More Details
CVE-2022-2119	OFFIS DCMTK's (All versions prior to 3.6.7) service class provider (SCP) is vulnerable to path traversal, allowing an attacker to write DICOM files into arbitrary directories under controlled names. This could allow remote code execution.	7.5	More Details
CVE-2022-34750	An issue was discovered in MediaWiki through 1.38.1. The lemma length of a Wikibase lexeme is currently capped at a thousand characters. Unfortunately, this length is not validated, allowing much larger lexemes to be created, which introduces various denial-of-service attack vectors within the Wikibase and WikibaseLexeme extensions. This is related to Special:NewLexeme and Special:NewProperty.	7.5	More Details
CVE-2022-31089	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In affected versions certain types of invalid files requests are not handled properly and can crash the server. If you are running multiple Parse Server instances in a cluster, the availability impact may be low; if you are running Parse Server as single instance without redundancy, the availability impact may be high. This issue has been addressed in versions 4.10.12 and 5.2.3. Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31103	lettersanitizer is a DOM-based HTML email sanitizer for in-browser email rendering. All versions of lettersanitizer below 1.0.2 are affected by a denial of service issue when processing a CSS at-rule `@keyframes`. This package is depended on by [react-letter](https://github.com/mat-sz/react-letter), therefore everyone using react-letter is also at risk. The problem has been patched in version 1.0.2.	7.5	More Details
CVE-2021-33651	When performing the analytical operation of the DepthwiseConv2D operator, if the attribute depth_multiplier is 0, it will cause a division by 0 exception.	7.5	More Details
CVE-2022-33093	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the key parameter at /freelance/resume_list.	7.5	More Details
CVE-2021-33650	When performing the inference shape operation of the SparseToDense operator, if the number of inputs is less than three, it will access data outside of bounds of inputs which allocated from heap buffers.	7.5	More Details
CVE-2021-40941	In Bento4 1.6.0-638, there is an allocator is out of memory in the function AP4_Array<AP4_TrunAtom::Entry>::EnsureCapacity in Ap4Array.h:172, as demonstrated by GPAC. This can cause a denial of service (DOS).	7.5	More Details
CVE-2022-34180	Jenkins Embeddable Build Status Plugin 2.0.3 and earlier does not correctly perform the ViewStatus permission check in the HTTP endpoint it provides for "unprotected" status badge access, allowing attackers without any permissions to obtain the build status badge icon for any attacker-specified job and/or build.	7.5	More Details
CVE-2022-33092	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/job/index.	7.5	More Details
CVE-2021-33649	When performing the inference shape operation of the Transpose operator, if the value in the perm element is greater than or equal to the size of the input_shape, it will access data outside of bounds of input_shape which allocated from heap buffers.	7.5	More Details
CVE-2022-34179	Jenkins Embeddable Build Status Plugin 2.0.3 and earlier allows specifying a `style` query parameter that is used to choose a different SVG image style without restricting possible values, resulting in a relative path traversal vulnerability that allows attackers without Overall/Read permission to specify paths to other SVG images on the Jenkins controller file system.	7.5	More Details
CVE-2021-33653	When performing the derivation shape operation of the SpaceToBatch operator, if there is a value of 0 in the parameter block_shape element, it will cause a division by 0 exception.	7.5	More Details
CVE-2022-31093	NextAuth.js is a complete open source authentication solution for Next.js applications. In affected versions an attacker can send a request to an app using NextAuth.js with an invalid `callbackUrl` query parameter, which internally is converted to a `URL` object. The URL instantiation would fail due to a malformed URL being passed into the constructor, causing it to throw an unhandled error which led to the **API route handler timing out and logging in to fail**. This has been remedied in versions 3.29.5 and 4.5.0. If for some reason you cannot upgrade, the workaround requires you to rely on Advanced Initialization. Please see the documentation for more.	7.5	More Details
CVE-2021-33648	When performing the inference shape operation of Affine, Concat, MatMul, ArgMinMax, EmbeddingLookup, and Gather operators, if the input shape size is 0, it will access data outside of bounds of shape which allocated from heap buffers.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31092	Pimcore is an Open Source Data & Experience Management Platform. Pimcore offers developers listing classes to make querying data easier. This listing classes also allow to order or group the results based on one or more columns which should be quoted by default. The actual issue is that quoting is not done properly in both cases, so there's the theoretical possibility to inject custom SQL if the developer is using this methods with input data and not doing proper input validation in advance and so relies on the auto-quoting being done by the listing classes. This issue has been resolved in version 10.4.4. Users are advised to upgrade or to apple the patch manually. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-33105	Redis v7.0 was discovered to contain a memory leak via the component streamGetEdgeID.	7.5	More Details
CVE-2022-34177	Jenkins Pipeline: Input Step Plugin 448.v37cea_9a_10a_70 and earlier archives files uploaded for `file` parameters for Pipeline `input` steps on the controller as part of build metadata, using the parameter name without sanitization as a relative path inside a build-related directory, allowing attackers able to configure Pipelines to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content.	7.5	More Details
CVE-2021-33654	When performing the initialization operation of the Split operator, if a dimension in the input shape is 0, it will cause a division by 0 exception.	7.5	More Details
CVE-2021-33647	When performing the inference shape operation of the Tile operator, if the input data type is not int or int32, it will access data outside of bounds of heap allocated buffers.	7.5	More Details
CVE-2022-33097	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/campus/campus_job.	7.5	More Details
CVE-2022-34175	Jenkins 2.335 through 2.355 (both inclusive) allows attackers in some cases to bypass a protection mechanism, thereby directly accessing some view fragments containing sensitive information, bypassing any permission checks in the corresponding view.	7.5	More Details
CVE-2021-41460	ECShop 4.1.0 has SQL injection vulnerability, which can be exploited by attackers to obtain sensitive information.	7.5	More Details
CVE-2022-34174	In Jenkins 2.355 and earlier, LTS 2.332.3 and earlier, an observable timing discrepancy on the login form allows distinguishing between login attempts with an invalid username, and login attempts with a valid username and wrong password, when using the Jenkins user database security realm.	7.5	More Details
CVE-2022-2121	OFFIS DCMTK's (All versions prior to 3.6.7) has a NULL pointer dereference vulnerability while processing DICOM files, which may result in a denial-of-service condition.	7.5	More Details
CVE-2022-2120	OFFIS DCMTK's (All versions prior to 3.6.7) service class user (SCU) is vulnerable to relative path traversal, allowing an attacker to write DICOM files into arbitrary directories under controlled names. This could allow remote code execution.	7.5	More Details
CVE-2022-33094	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/job/map.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33652	When the Reduce operator run operation is executed, if there is a value of 0 in the parameter axis_sizes element, it will cause a division by 0 exception.	7.5	More Details
CVE-2022-30560	When an attacker obtaining the administrative account and password, or through a man-in-the-middle attack, the attacker could send a specified crafted packet to the vulnerable interface then lead the device to crash.	7.4	More Details
CVE-2022-1524	LRM version 2.4 and lower does not implement TLS encryption. A malicious actor can MITM attack sensitive data in-transit, including credentials.	7.4	More Details
CVE-2022-30563	When an attacker uses a man-in-the-middle attack to sniff the request packets with success logging in through ONVIF, he can log in to the device by replaying the user's login packet.	7.4	More Details
CVE-2022-31081	HTTP::Daemon is a simple http server class written in perl. Versions prior to 6.15 are subject to a vulnerability which could potentially be exploited to gain privileged access to APIs or poison intermediate caches. It is uncertain how large the risks are, most Perl based applications are served on top of Nginx or Apache, not on the `HTTP::Daemon`. This library is commonly used for local development and tests. Users are advised to update to resolve this issue. Users unable to upgrade may add additional request handling logic as a mitigation. After calling `my $rqst = $conn->get_request()` one could inspect the returned `HTTP::Request` object. Querying the 'Content-Length' (`my $cl = $rqst->header('Content-Length')`) will show any abnormalities that should be dealt with by a `400` response. Expected strings of 'Content-Length' SHOULD consist of either a single non-negative integer, or, a comma separated repetition of that number. (that is `42` or `42, 42, 42`). Anything else MUST be rejected.	7.3	More Details
CVE-2022-0624	Authorization Bypass Through User-Controlled Key in GitHub repository ionicabizau/parse-path prior to 5.0.0.	7.3	More Details
CVE-2021-26638	Improper Authentication vulnerability in S&D smarthome(smartcare) application can cause authentication bypass and information exposure. Remote attackers can use this vulerability to take control of the home environment including indoor control.	7.3	More Details
CVE-2017-20099	A vulnerability was found in Analytics Stats Counter Statistics Plugin 1.2.2.5 and classified as critical. This issue affects some unknown processing. The manipulation leads to code injection. The attack may be initiated remotely.	7.3	More Details
CVE-2017-20104	A vulnerability was found in Simplessus 3.7.7. It has been declared as critical. This vulnerability affects unknown code of the component Cookie Handler. The manipulation of the argument UWA_SID leads to sql injection (Time). The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.8.3 is able to address this issue. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2021-40955	SQL injection exists in LaiKetui v3.5.0 the background administrator list.	7.2	More Details
CVE-2022-33114	Jfinal CMS v5.1.0 was discovered to contain a SQL injection vulnerability via the attrVal parameter at /jfinal_cms/system/dict/list.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1977	The Import Export All WordPress Images, Users & Post Types WordPress plugin before 6.5.3 does not fully validate the file to be imported via an URL before making an HTTP request to it, which could allow high privilege users such as admin to perform Blind SSRF attacks	7.2	More Details
CVE-2022-30997	Use of hard-coded credentials vulnerability exists in STARDOM FCN Controller and FCJ Controller R4.10 to R4.31, which may allow an attacker with an administrative privilege to read/change configuration settings or update the controller with tampered firmware.	7.2	More Details
CVE-2022-32400	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/user/manage_user.php:4.	7.2	More Details
CVE-2021-41637	Weak access control permissions in MELAG FTP Server 2.2.0.4 allow the "Everyone" group to read the local FTP configuration file, which includes among other information the unencrypted passwords of all FTP users.	7.1	More Details
CVE-2022-31094	ScratchTools is a web extension designed to make interacting with the Scratch programming language community (Scratching) easier. In affected versions anybody who uses the Recently Viewed Projects feature is vulnerable to having their account taken over if they view a project that tries to. The issue is that if a user visits a project that includes Javascript in the title, then when the Recently Viewed Projects feature displays it, it could run the Javascript. This issue has been addressed in the 2.5.2 release. Users having issues scratching should open an issue in the project issue tracker https://github.com/STForScratch/ScratchTools/	7.1	More Details
CVE-2022-1743	The tested version of Dominion Voting System ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.	6.8	More Details
CVE-2022-2088	An authenticated user with admin privileges may be able to terminate any process on the system running Elcomplus SmartICS v2.3.4.0.	6.8	More Details
CVE-2022-1745	The authentication mechanism used by technicians on the tested version of Dominion Voting Systems ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions.	6.8	More Details
CVE-2022-1744	Applications on the tested version of Dominion Voting Systems ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.	6.8	More Details
CVE-2022-1742	The tested version of Dominion Voting Systems ImageCast X allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.	6.8	More Details
CVE-2022-1741	The tested version of Dominion Voting Systems ImageCast X has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code.	6.8	More Details
CVE-2022-1739	The tested version of Dominion Voting Systems ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42056	Thales Safenet Authentication Client (SAC) for Linux and Windows through 10.7.7 creates insecure temporary hid and lock files allowing a local attacker, through a symlink attack, to overwrite arbitrary files, and potentially achieve arbitrary command execution with high privileges.	6.7	More Details
CVE-2021-29768	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could allow a low level user to obtain sensitive information from the details of the 'Cloud Storage' page for which they should not have access. IBM X-Force ID: 202682.	6.5	More Details
CVE-2022-1843	The MailPress WordPress plugin through 7.2.1 does not have CSRF checks in various places, which could allow attackers to make a logged in admin change the settings, purge log files and more via CSRF attacks	6.5	More Details
CVE-2022-1666	The default password for the web application’s root user (the vendor’s private account) was weak and the MD5 hash was used to crack the password using a widely available open-source tool.	6.5	More Details
CVE-2022-22389	IBM Db2 for Linux, UNIX and Windows 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may terminate abnormally when executing specially crafted SQL statements by an authenticated user. IBM X-Force ID: 2219740.	6.5	More Details
CVE-2021-41636	MELAG FTP Server 2.2.0.4 allows an attacker to use the CWD command to break out of the FTP servers root directory and operate on the entire operating system, while the access restrictions of the user running the FTP server apply.	6.5	More Details
CVE-2022-20828	A vulnerability in the CLI parser of Cisco FirePOWER Software for Adaptive Security Appliance (ASA) FirePOWER module could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected ASA FirePOWER module as the root user. This vulnerability is due to improper handling of undefined command parameters. An attacker could exploit this vulnerability by using a crafted command on the CLI or by submitting a crafted HTTPS request to the web-based management interface of the Cisco ASA that is hosting the ASA FirePOWER module. Note: To exploit this vulnerability, the attacker must have administrative access to the Cisco ASA. A user who has administrative access to a particular Cisco ASA is also expected to have administrative access to the ASA FirePOWER module that is hosted by that Cisco ASA.	6.5	More Details
CVE-2022-28167	Brocade SANnav before Brocade SANvav v. 2.2.0.2 and Brocade SANanv v.2.1.1.8 logs the Brocade Fabric OS switch password in plain text in asyncjobscheduler-manager.log	6.5	More Details
CVE-2013-1891	In OpenCart 1.4.7 to 1.5.5.1, implemented anti-traversal code in filemanager.php is ineffective and can be bypassed.	6.5	More Details
CVE-2022-28172	The web module in some Hikvision Hybrid SAN/Cluster Storage products have the following security vulnerability. Due to the insufficient input validation, attacker can exploit the vulnerability to XSS attack by sending messages with malicious commands to the affected device.	6.5	More Details
CVE-2022-31016	Argo CD is a declarative continuous deployment for Kubernetes. Argo CD versions v0.7.0 and later are vulnerable to an uncontrolled memory consumption bug, allowing an authorized malicious user to crash the repo-server service, resulting in a Denial of Service. The attacker must be an authenticated Argo CD user authorized to deploy Applications from a repository which contains (or can be made to contain) a large file. The fix for this vulnerability is available in versions 2.3.5, 2.2.10, 2.1.16, and later. There are no known workarounds. Users are recommended to upgrade.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31884	Marval MSM v14.19.0.12476 has an Improper Access Control vulnerability which allows a low privilege user to delete other users API Keys including high privilege and the Administrator users API Keys.	6.5	More Details
CVE-2022-32141	Multiple CODESYS Products are prone to a buffer over read. A low privileged remote attacker may craft a request with an invalid offset, which can cause an internal buffer over-read, resulting in a denial-of-service condition. User interaction is not required.	6.5	More Details
CVE-2022-31100	rulex is a new, portable, regular expression language. When parsing untrusted rulex expressions, rulex may crash, possibly enabling a Denial of Service attack. This happens when the expression contains a multi-byte UTF-8 code point in a string literal or after a backslash, because rulex tries to slice into the code point and panics as a result. This is a security concern for you, if your service parses untrusted rulex expressions (expressions provided by an untrusted user), and your service becomes unavailable when the thread running rulex panics. The crashes are fixed in version **0.4.3**. Affected users are advised to update to this version. The only known workaround for this issue is to assume that regular expression parsing will panic and to add logic to catch panics.	6.5	More Details
CVE-2022-34209	A cross-site request forgery (CSRF) vulnerability in Jenkins ThreadFix Plugin 1.5.4 and earlier allows attackers to connect to an attacker-specified URL.	6.5	More Details
CVE-2022-34207	A cross-site request forgery (CSRF) vulnerability in Jenkins Beaker builder Plugin 1.10 and earlier allows attackers to connect to an attacker-specified URL.	6.5	More Details
CVE-2022-34205	A cross-site request forgery (CSRF) vulnerability in Jenkins Jianliao Notification Plugin 1.1 and earlier allows attackers to send HTTP POST requests to an attacker-specified URL.	6.5	More Details
CVE-2022-34202	Jenkins EasyQA Plugin 1.0 and earlier stores user passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-34201	A missing permission check in Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	6.5	More Details
CVE-2022-34199	Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details
CVE-2022-33116	An issue in the jmpath variable in /modules/mindmap/index.php of GUnet Open eClass Platform (aka openeclass) v3.12.4 and below allows attackers to read arbitrary files via a directory traversal.	6.5	More Details
CVE-2022-31099	rulex is a new, portable, regular expression language. When parsing untrusted rulex expressions, the stack may overflow, possibly enabling a Denial of Service attack. This happens when parsing an expression with several hundred levels of nesting, causing the process to abort immediately. This is a security concern for you, if your service parses untrusted rulex expressions (expressions provided by an untrusted user), and your service becomes unavailable when the process running rulex aborts due to a stack overflow. The crash is fixed in version **0.4.3**. Affected users are advised to update to this version. There are no known workarounds for this issue.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34211	A cross-site request forgery (CSRF) vulnerability in Jenkins vRealize Orchestrator Plugin 3.0 and earlier allows attackers to send an HTTP POST request to an attacker-specified URL.	6.5	More Details
CVE-2022-32140	Multiple CODESYS products are affected to a buffer overflow.A low privileged remote attacker may craft a request, which can cause a buffer copy without checking the size of the service, resulting in a denial-of-service condition. User Interaction is not required.	6.5	More Details
CVE-2021-3779	A malicious MySQL server can request local file content from a client using ruby-mysql prior to version 2.10.0 without explicit authorization from the user. This issue was resolved in version 2.10.0 and later.	6.5	More Details
CVE-2022-31052	Synapse is an open source home server implementation for the Matrix chat network. In versions prior to 1.61.1 URL previews of some web pages can exhaust the available stack space for the Synapse process due to unbounded recursion. This is sometimes recoverable and leads to an error for the request causing the problem, but in other cases the Synapse process may crash altogether. It is possible to exploit this maliciously, either by malicious users on the homeserver, or by remote users sending URLs that a local user's client may automatically request a URL preview for. Remote users are not able to exploit this directly, because the URL preview endpoint is authenticated. Deployments with `url_preview_enabled: false` set in configuration are not affected. Deployments with `url_preview_enabled: true` set in configuration **are** affected. Deployments with no configuration value set for `url_preview_enabled` are not affected, because the default is `false`. Administrators of homeservers with URL previews enabled are advised to upgrade to v1.61.1 or higher. Users unable to upgrade should set `url_preview_enabled` to false.	6.5	More Details
CVE-2021-3430	Assertion reachable with repeated LL_CONNECTION_PARAM_REQ. Zephyr versions >= v1.14 contain Reachable Assertion (CWE-617). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-46h3-hjcq-2jjr	6.5	More Details
CVE-2022-31886	Marval MSM v14.19.0.12476 is vulnerable to Cross Site Request Forgery (CSRF). An attacker can disable the 2FA by sending the user a malicious form.	6.5	More Details
CVE-2021-41559	Silverstripe silverstripe/framework 4.8.1 has a quadratic blowup in Convert::xml2array() that enables a remote attack via a crafted XML document.	6.5	More Details
CVE-2022-24444	Silverstripe silverstripe/framework through 4.10 allows Session Fixation.	6.5	More Details
CVE-2022-34210	A missing permission check in Jenkins ThreadFix Plugin 1.5.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	6.5	More Details
CVE-2022-34012	Insecure permissions in OneBlog v2.3.4 allows low-level administrators to reset the passwords of high-level administrators who hold greater privileges.	6.5	More Details
CVE-2022-34295	totd before 1.5.3 does not properly randomize mesg IDs.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31064	BigBlueButton is an open source web conferencing system. Users in meetings with private chat enabled are vulnerable to a cross site scripting attack in affected versions. The attack occurs when the attacker (with xss in the name) starts a chat. in the victim's client the JavaScript will be executed. This issue has been addressed in version 2.4.8 and 2.5.0. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-32139	In multiple CODESYS products, a low privileged remote attacker may craft a request, which cause an out-of-bounds read, resulting in a denial-of-service condition. User Interaction is not required.	6.5	More Details
CVE-2022-32136	In multiple CODESYS products, a low privileged remote attacker may craft a request that cause a read access to an uninitialized pointer, resulting in a denial-of-service. User interaction is not required.	6.5	More Details
CVE-2022-2147	Cloudflare Warp for Windows from version 2022.2.95.0 contained an unquoted service path which enables arbitrary code execution leading to privilege escalation. The fix was released in version 2022.3.186.0.	6.5	More Details
CVE-2022-34213	Jenkins Squash TM Publisher (Squash4Jenkins) Plugin 1.0.0 and earlier stores passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-2221	Information Exposure vulnerability in My Account Settings of Devolutions Remote Desktop Manager before 2022.1.8 allows authenticated users to access credentials of other users. This issue affects: Devolutions Remote Desktop Manager versions prior to 2022.1.8.	6.5	More Details
CVE-2022-31065	BigBlueButton is an open source web conferencing system. In affected versions an attacker can embed malicious JS in their username and have it executed on the victim's client. When a user receives a private chat from the attacker (whose username contains malicious JavaScript), the script gets executed. Additionally when the victim receives a notification that the attacker has left the session. This issue has been patched in version 2.4.8 and 2.5.0. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-31057	Shopware is an open source e-commerce software made in Germany. Versions of Shopware 5 prior to version 5.7.12 are subject to an authenticated Stored XSS in Administration. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-26862	Prior Dell BIOS versions contain an Input Validation vulnerability. A locally authenticated malicious user could potentially exploit this vulnerability by sending malicious input to an SMI in order to bypass security controls in SMM.	6.3	More Details
CVE-2017-20103	A vulnerability classified as critical has been found in Kama Click Counter Plugin up to 3.4.8. This affects an unknown part of the file wp-admin/admin.php. The manipulation of the argument order_by/order with the input ASC%2c(select*from(select(sleep(2)))a) leads to sql injection (Blind). It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.4.9 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2019-25071	A vulnerability was found in Apple iPhone up to 12.4.1. It has been declared as critical. Affected by this vulnerability is Siri. Playing an audio or video file might be able to initiate Siri on the same device which makes it possible to execute commands remotely. Exploit details have been disclosed to the public. The existence and implications of this vulnerability are doubted by Apple even though multiple public videos demonstrating the attack exist. Upgrading to version 13.0 migt be able to address this issue. It is recommended to upgrade affected devices. NOTE: Apple claims, that after examining the report they do not see any actual security implications.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20086	A vulnerability, which was classified as critical, was found in VaultPress Plugin 1.8.4. This affects an unknown part. The manipulation leads to code injection. It is possible to initiate the attack remotely.	6.3	More Details
CVE-2017-20095	A vulnerability classified as critical was found in Simple Ads Manager Plugin. This vulnerability affects unknown code. The manipulation leads to code injection. The attack can be initiated remotely.	6.3	More Details
CVE-2022-2214	A vulnerability was found in SourceCodester Library Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /librarian/bookdetails.php. The manipulation of the argument id with the input ' AND (SELECT 9198 FROM (SELECT(SLEEP(5)))iqZA)-- PbtB leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-2212	A vulnerability was found in SourceCodester Library Management System 1.0. It has been classified as critical. Affected is an unknown function of the component /card/index.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-26864	Prior Dell BIOS versions contain an Input Validation vulnerability. A locally authenticated malicious user could potentially exploit this vulnerability by sending malicious input to an SMI in order to bypass security controls in SMM.	6.3	More Details
CVE-2022-26863	Prior Dell BIOS versions contain an Input Validation vulnerability. A locally authenticated malicious user could potentially exploit this vulnerability by sending malicious input to an SMI in order to bypass security controls in SMM.	6.3	More Details
CVE-2022-32124	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the component /index/jobfairol/show/.	6.1	More Details
CVE-2022-32125	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /job.	6.1	More Details
CVE-2021-29055	Cross Site Scripting (XSS) vulnerability in sourcecodester School File Management System 1.0 via the Firtstname parameter to the Update Account form in student_profile.php.	6.1	More Details
CVE-2022-32126	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company.	6.1	More Details
CVE-2022-2218	Cross-site Scripting (XSS) - Stored in GitHub repository ionicabizau/parse-url prior to 7.0.0.	6.1	More Details
CVE-2020-21161	Cross Site Scripting (XSS) vulnerability in Ruckus Wireless ZoneDirector 9.8.3.0.	6.1	More Details
CVE-2022-34305	In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33146	Open redirect vulnerability in web2py versions prior to 2.22.5 allows a remote attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL.	6.1	More Details
CVE-2022-29931	The administration interface of the Raytion Custom Security Manager (Raytion CSM) in Version 7.2.0 allows reflected Cross-site Scripting (XSS).	6.1	More Details
CVE-2022-2217	Cross-site Scripting (XSS) - Generic in GitHub repository ionicabizau/parse-url prior to 7.0.0.	6.1	More Details
CVE-2022-2174	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.18.	6.1	More Details
CVE-2022-23077	In habitica versions v4.119.0 through v4.232.2 are vulnerable to DOM XSS via the login page.	6.1	More Details
CVE-2020-19897	A reflected Cross Site Scripting (XSS) in wuzhicms v4.1.0 allows remote attackers to execute arbitrary web script or HTML via the imgurl parameter.	6.1	More Details
CVE-2022-1916	The Active Products Tables for WooCommerce. Professional products tables for WooCommerce store WordPress plugin before 1.0.5 does not sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected cross-Site Scripting	6.1	More Details
CVE-2022-1904	The Pricing Tables WordPress Plugin WordPress plugin before 3.2.1 does not sanitise and escape parameter before outputting it back in a page available to any user (both authenticated and unauthenticated) when a specific setting is enabled, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1593	The Site Offline or Coming Soon WordPress plugin through 1.6.6 does not have CSRF check in place when updating its settings, and it also lacking sanitisation as well as escaping in some of them. As a result, attackers could make a logged in admin change them and put Cross-Site Scripting payloads in them via a CSRF attack	6.1	More Details
CVE-2022-29096	Dell Wyse Management Suite 3.6.1 and below contains a Reflected Cross-Site Scripting Vulnerability in saveGroupConfigurations page. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	6.1	More Details
CVE-2022-32127	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/view_be_browsed/total.	6.1	More Details
CVE-2022-32128	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/service/increment/add/im.	6.1	More Details
CVE-2022-34133	Benjamin BALET Jorani v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Comment parameter at application/controllers/Leaves.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31085	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. In versions prior to 8.0 the session files include the LDAP user name and password in clear text if the PHP OpenSSL extension is not installed or encryption is disabled by configuration. This issue has been fixed in version 8.0. Users unable to upgrade should install the PHP OpenSSL extension and make sure session encryption is enabled in LAM main configuration.	6.1	More Details
CVE-2022-34328	PMB 7.3.10 allows reflected XSS via the id parameter in an lvl=author_see request to index.php.	6.1	More Details
CVE-2022-1470	The Ultimate WooCommerce CSV Importer WordPress plugin through 2.0 does not sanitise and escape the imported data before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-33005	A cross-site scripting (XSS) vulnerability in the System Settings/IOT Settings module of Delta Electronics DIAEnergie v1.08.00 allows attackers to execute arbitrary web scripts via a crafted payload injected into the Name text field.	6.1	More Details
CVE-2022-30118	Title for CVE: XSS in /dashboard/system/express/entities/forms/save_control/[GUID]: old browsers only.Description: When using Internet Explorer with the XSS protection disabled, editing a form control in an express entities form for Concrete 8.5.7 and below as well as Concrete 9.0 through 9.0.2 can allow XSS. This cannot be exploited in modern-day web browsers due to an automatic input escape mechanism. Concrete CMS Security team ranked this vulnerability 2 with CVSS v3.1 Vector AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N. Thanks zeroinside for reporting.	6.1	More Details
CVE-2022-30119	XSS in /dashboard/reports/logs/view - old browsers only. When using Internet Explorer with the XSS protection disabled, insufficient sanitation where built urls are outputted can be exploited for Concrete 8.5.7 and below as well as Concrete 9.0 through 9.0.2. This cannot be exploited in modern-day web browsers due to an automatic input escape mechanism. Concrete CMS Security team ranked this vulnerability 2 with CVSS v3.1 Vector AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N. Thanks zeroinside for reporting.	6.1	More Details
CVE-2022-30120	XSS in /dashboard/blocks/stacks/view_details/ - old browsers only. When using an older browser with built-in XSS protection disabled, insufficient sanitation where built urls are outputted can be exploited for Concrete 8.5.7 and below as well as Concrete 9.0 through 9.0.2 to allow XSS. This cannot be exploited in modern-day web browsers due to an automatic input escape mechanism. Concrete CMS Security team ranked this vulnerability 3.1with CVSS v3.1 Vector AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N. Sanitation has been added where built urls are output. Credit to Credit to Bogdan Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/) for reporting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32209	# Possible XSS Vulnerability in Rails::Html::SanitizerThere is a possible XSS vulnerability with certain configurations of Rails::Html::Sanitizer.This vulnerability has been assigned the CVE identifier CVE-2022-32209.Versions Affected: ALLNot affected: NONEFixed Versions: v1.4.3## ImpactA possible XSS vulnerability with certain configurations of Rails::Html::Sanitizer may allow an attacker to inject content if the application developer has overridden the sanitizer's allowed tags to allow both `select` and `style` elements.Code is only impacted if allowed tags are being overridden. This may be done via application configuration:```ruby# In config/application.rbconfig.action_view.sanitized_allowed_tags = ["select", "style"]```see https://guides.rubyonrails.org/configuring.html#configuring-action-viewOr it may be done with a `:tags` option to the Action View helper `sanitize`:```<%= sanitize @comment.body, tags: ["select", "style"] %>```see https://api.rubyonrails.org/classes/ActionView/Helpers/SanitizeHelper.html#method-i-sanitizeOr it may be done with Rails::Html::SafeListSanitizer directly:```ruby# class-level optionRails::Html::SafeListSanitizer.allowed_tags = ["select", "style"]```or```ruby# instance-level optionRails::Html::SafeListSanitizer.new.sanitize(@article.body, tags: ["select", "style"])```All users overriding the allowed tags by any of the above mechanisms to include both "select" and "style" should either upgrade or use one of the workarounds immediately.## ReleasesThe FIXED releases are available at the normal locations.## WorkaroundsRemove either `select` or `style` from the overridden allowed tags.## CreditsThis vulnerability was responsibly reported by [windshock](https://hackerone.com/windshock?type=user).	6.1	More Details
CVE-2021-39047	IBM Planning Analytics 2.0 and IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 214349.	6.1	More Details
CVE-2022-32129	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/account/safety/trade.	6.1	More Details
CVE-2022-34178	Jenkins Embeddable Build Status Plugin 2.0.3 allows specifying a 'link' query parameter that build status badges will link to, without restricting possible values, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-34182	Jenkins Nested View Plugin 1.20 through 1.25 (both inclusive) does not escape search parameters, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-32131	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /index/notice/show.	6.1	More Details
CVE-2022-32130	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/down_resume/total/nature.	6.1	More Details
CVE-2021-39408	Cross Site Scripting (XSS) vulnerability exists in Online Student Rate System 1.0 via the page parameter on the index.php file	6.1	More Details
CVE-2022-30561	When an attacker uses a man-in-the-middle attack to sniff the request packets with success logging in, the attacker could log in to the device by replaying the user's login packet.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30028	Dradis Professional Edition before 4.3.0 allows attackers to change an account password via reusing a password reset token.	5.9	More Details
CVE-2022-23170	SysAid - Okta SSO integration - was found vulnerable to XML External Entity Injection vulnerability. Any SysAid environment that uses the Okta SSO integration might be vulnerable. An unauthenticated attacker could exploit the XXE vulnerability by sending a malformed POST request to the identity provider endpoint. An attacker can extract the identity provider endpoint by decoding the SAMLRequest parameter's value and searching for the AssertionConsumerServiceURL parameter's value. It often allows an attacker to view files on the application server filesystem and interact with any back-end or external systems that the application can access. In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.	5.9	More Details
CVE-2022-2145	Cloudflare WARP client for Windows (up to v. 2022.5.309.0) allowed creation of mount points from its ProgramData folder. During installation of the WARP client, it was possible to escalate privileges and overwrite SYSTEM protected files.	5.8	More Details
CVE-2022-31082	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. glpi-inventory-plugin is a plugin for GLPI to handle inventory management. In affected versions a SQL injection can be made using package deployment tasks. This issue has been resolved in version 1.0.2. Users are advised to upgrade. Users unable to upgrade should delete the `front/deploypackage.public.php` file if they are not using the `deploy tasks` feature.	5.8	More Details
CVE-2022-34212	A missing permission check in Jenkins vRealize Orchestrator Plugin 3.0 and earlier allows attackers with Overall/Read permission to send an HTTP POST request to an attacker-specified URL.	5.7	More Details
CVE-2022-31009	wire-ios is an iOS client for the Wire secure messaging application. Invalid accent colors of Wire communication partners may render the iOS Wire Client partially unusable by causing it to crash multiple times on launch. These invalid accent colors can be used by and sent between Wire users. The root cause was an unnecessary assert statement when converting an integer value into the corresponding enum value, causing an exception instead of a fallback to a default value. This issue is fixed in [wire-ios](https://github.com/wireapp/wire-ios/commit/caa0e27dbe51f9edfda8c7a9f017d93b8cfddefb) and in Wire for iOS 3.100. There is no workaround available, but users may use other Wire clients (such as the [web app](https://app.wire.com)) to continue using Wire, or upgrade their client.	5.7	More Details
CVE-2022-31096	Discourse is an open source discussion platform. Under certain conditions, a logged in user can redeem an invite with an email that either doesn't match the invite's email or does not adhere to the email domain restriction of an invite link. The impact of this flaw is aggravated when the invite has been configured to add the user that accepts the invite into restricted groups. Once a user has been incorrectly added to a restricted group, the user may then be able to view content which that are restricted to the respective group. Users are advised to upgrade to the current stable releases. There are no known workarounds to this issue.	5.7	More Details
CVE-2022-2208	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.5163.	5.5	More Details
CVE-2021-40606	The gf_bs_write_data function in GPAC 1.0.1 allows attackers to cause a denial of service via a crafted file in the MP4Box command.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40944	In GPAC MP4Box 1.1.0, there is a Null pointer reference in the function gf_filter_pid_get_packet function in src/filter_core/filter_pid.c:5394, as demonstrated by GPAC. This can cause a denial of service (DOS).	5.5	More Details
CVE-2021-40607	The schm_box_size function in GPAC 1.0.1 allows attackers to cause a denial of service via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-40943	In Bento4 1.6.0-638, there is a null pointer reference in the function AP4_DescriptorListInspector::Action function in Ap4Descriptor.h:124 , as demonstrated by GPAC. This can cause a denial of service (DOS).	5.5	More Details
CVE-2021-40609	The GetHintFormat function in GPAC 1.0.1 allows attackers to cause a denial of service via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-40608	The gf_hinter_track_finalize function in GPAC 1.0.1 allows attackers to cause a denial of service via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-40942	In GPAC MP4Box v1.1.0, there is a heap-buffer-overflow in the function filter_parse_dyn_args function in filter_core/filter.c:1454, as demonstrated by GPAC. This can cause a denial of service (DOS).	5.5	More Details
CVE-2022-2231	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.	5.5	More Details
CVE-2017-20082	A vulnerability, which was classified as problematic, has been found in JUNG Smart Visu Server 1.0.804/1.0.830/1.0.832. This issue affects some unknown processing. The manipulation leads to backdoor. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.900 is able to address this issue. It is recommended to upgrade the affected component.	5.5	More Details
CVE-2022-32990	An issue in gimp_layer_invalidate_boundary of GNOME GIMP 2.10.30 allows attackers to trigger an unhandled exception via a crafted XCF file, causing a Denial of Service (DoS).	5.5	More Details
CVE-2022-34495	rpmsg_probe in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.	5.5	More Details
CVE-2022-33124	AIOHTTP 3.8.1 can report a "ValueError: Invalid IPv6 URL" outcome, which can lead to a Denial of Service (DoS). NOTE: multiple third parties dispute this issue because there is no example of a context in which denial of service would occur, and many common contexts have exception handing in the calling application	5.5	More Details
CVE-2022-34494	rpmsg_virtio_add_ctrl_dev in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20651	A vulnerability in the logging component of Cisco Adaptive Security Device Manager (ASDM) could allow an authenticated, local attacker to view sensitive information in clear text on an affected system. Cisco ADSM must be deployed in a shared workstation environment for this issue to be exploited. This vulnerability is due to the storage of unencrypted credentials in certain logs. An attacker could exploit this vulnerability by accessing the logs on an affected system. A successful exploit could allow the attacker to view the credentials of other users of the shared device.	5.5	More Details
CVE-2022-33070	Protobuf-c v1.4.0 was discovered to contain an invalid arithmetic shift via the function parse_tag_and_wiretype in protobuf-c/protobuf-c.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via unspecified vectors.	5.5	More Details
CVE-2022-33069	Ethereum Solidity v0.8.14 contains an assertion failure via SMTEncoder::indexOrMemberAssignment() at SMTEncoder.cpp.	5.5	More Details
CVE-2022-33068	An integer overflow in the component hb-ot-shape-fallback.cc of Harfbuzz v4.3.0 allows attackers to cause a Denial of Service (DoS) via unspecified vectors.	5.5	More Details
CVE-2022-33067	Lrzip v0.651 was discovered to contain multiple invalid arithmetic shifts via the functions get_magic in lrzip.c and Predictor::init in libzpaq/libzpaq.cpp. These vulnerabilities allow attackers to cause a Denial of Service via unspecified vectors.	5.5	More Details
CVE-2021-41639	MELAG FTP Server 2.2.0.4 stores unencrpyted passwords of FTP users in a local configuration file.	5.5	More Details
CVE-2022-22502	IBM Robotic Process Automation 21.0.1 and 21.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 227124.	5.4	More Details
CVE-2022-34192	Jenkins ontrack Jenkins Plugin 4.0.0 and earlier does not escape the name of Ontrack: Multi Parameter choice, Ontrack: Parameter choice, and Ontrack: SingleParameter parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34172	In Jenkins 2.340 through 2.355 (both inclusive) symbol-based icons unescape previously escaped values of 'tooltip' parameters, resulting in a cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-27509	Persistent XSS in Galaxkey Secure Mail Client in Galaxkey up to 5.6.11.5 allows an attacker to perform an account takeover by intercepting the HTTP Post request when sending an email and injecting a specially crafted XSS payload in the 'subject' field. The payload executes when the recipient logs into their mailbox.	5.4	More Details
CVE-2022-34173	In Jenkins 2.340 through 2.355 (both inclusive) the tooltip of the build button in list views supports HTML without escaping the job display name, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2022-27238	BigBlueButton version 2.4.7 (or earlier) is vulnerable to stored Cross-Site Scripting (XSS) in the private chat functionality. A threat actor could inject JavaScript payload in his/her username. The payload gets executed in the browser of the victim each time the attacker sends a private message to the victim or when notification about the attacker leaving room is displayed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34193	Jenkins Package Version Plugin 1.0.1 and earlier does not escape the name of Package version parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-33910	An XSS vulnerability in MantisBT before 2.25.5 allows remote attackers to attach crafted SVG documents to issue reports or bugnotes. When a user or an admin clicks on the attachment, file_download.php opens the SVG document in a browser tab instead of downloading it as a file, causing the JavaScript code to execute.	5.4	More Details
CVE-2022-34191	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.77 and earlier does not escape the name of NetStorm Test parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34183	Jenkins Agent Server Parameter Plugin 1.1 and earlier does not escape the name and description of Agent Server parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34184	Jenkins CRX Content Package Deployer Plugin 1.9 and earlier does not escape the name and description of CRX Content Package Choice parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34185	Jenkins Date Parameter Plugin 0.0.4 and earlier does not escape the name and description of Date parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34186	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier does not escape the name and description of Moded Extended Choice parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34190	Jenkins Maven Metadata Plugin for Jenkins CI server Plugin 2.1 and earlier does not escape the name and description of List maven artifact versions parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34187	Jenkins Filesystem List Parameter Plugin 0.0.7 and earlier does not escape the name and description of File system objects list parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2021-38871	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 208345.	5.4	More Details
CVE-2021-29865	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 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: 206091.	5.4	More Details
CVE-2022-34188	Jenkins Hidden Parameter Plugin 0.0.4 and earlier does not escape the name and description of Hidden Parameter parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20105	A vulnerability was found in Simplessus 3.7.7. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument path with the input ..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.8.3 is able to address this issue. It is recommended to upgrade the affected component.	5.4	More Details
CVE-2022-34176	Jenkins JUnit Plugin 1119.va_a_5e9068da_d7 and earlier does not escape descriptions of test results, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission.	5.4	More Details
CVE-2022-2041	The Brizy WordPress plugin before 2.4.2 does not sanitise and escape some element content, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2021-41432	A stored cross-site scripting (XSS) vulnerability exists in FlatPress 1.2.1 that allows for arbitrary execution of JavaScript commands through blog content.	5.4	More Details
CVE-2022-25238	Silverstripe silverstripe/framework through 4.10.0 allows XSS, inside of script tags that can can be added to website content via XHR by an authenticated CMS user if the cwp-core module is not installed on the sanitise_server_side contig is not set to true in project code.	5.4	More Details
CVE-2022-34198	Jenkins Stash Branch Parameter Plugin 0.3.0 and earlier does not escape the name and description of Stash Branch parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-23057	In ERPNext, versions v12.0.9--v13.0.3 are vulnerable to Stored Cross-Site-Scripting (XSS), due to user input not being validated properly. A low privileged attacker could inject arbitrary code into input fields when editing his profile.	5.4	More Details
CVE-2022-34197	Jenkins Sauce OnDemand Plugin 1.204 and earlier does not escape the name and description of Sauce Labs Browsers parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-1776	The Popups, Welcome Bar, Optins and Lead Generation Plugin WordPress plugin before 2.1.8 does not sanitize and escape some campaign parameters, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-34196	Jenkins REST List Parameter Plugin 1.5.2 and earlier does not escape the name and description of REST list parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-2040	The Brizy WordPress plugin before 2.4.2 does not sanitise and escape some element URL, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-34195	Jenkins Repository Connector Plugin 2.2.0 and earlier does not escape the name and description of Maven Repository Artifact parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34189	Jenkins Image Tag Parameter Plugin 1.10 and earlier does not escape the name and description of Image Tag parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46824	Cross Site Scripting (XSS) vulnerability in sourcecodester School File Management System 1.0 via the Lastname parameter to the Update Account form in student_profile.php.	5.4	More Details
CVE-2022-23896	Admidio 4.1.2 version is affected by stored cross-site scripting (XSS).	5.4	More Details
CVE-2022-34194	Jenkins Readonly Parameter Plugin 1.0.0 and earlier does not escape the name and description of Readonly String and Readonly Text parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-1964	The Easy SVG Support WordPress plugin before 3.3.0 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads	5.4	More Details
CVE-2022-33113	Jfinal CMS v5.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the keyword text field under the publish blog module.	5.4	More Details
CVE-2022-34170	In Jenkins 2.320 through 2.355 (both inclusive) and LTS 2.332.1 through LTS 2.332.3 (both inclusive) the help icon does not escape the feature name that is part of its tooltip, effectively undoing the fix for SECURITY-1955, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2022-34171	In Jenkins 2.321 through 2.355 (both inclusive) and LTS 2.332.1 through LTS 2.332.3 (both inclusive) the HTML output generated for new symbol-based SVG icons includes the 'title' attribute of 'l:ionicon' (until Jenkins 2.334) and 'alt' attribute of 'l:icon' (since Jenkins 2.335) without further escaping, resulting in a cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2021-20543	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 198929.	5.4	More Details
CVE-2021-41634	A user enumeration vulnerability in MELAG FTP Server 2.2.0.4 allows an attacker to identify valid FTP usernames.	5.3	More Details
CVE-2022-31803	In CODESYS Gateway Server V2 an insufficient check for the activity of TCP client connections allows an unauthenticated attacker to consume all available TCP connections and prevent legitimate users or clients from establishing a new connection to the CODESYS Gateway Server V2. Existing connections are not affected and therefore remain intact.	5.3	More Details
CVE-2021-20355	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 194891.	5.3	More Details
CVE-2022-31088	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. In versions prior to 8.0 the user name field at login could be used to enumerate LDAP data. This is only the case for LDAP search configuration. This issue has been fixed in version 8.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20083	A vulnerability, which was classified as critical, was found in JUNG Smart Visu Server 1.0.804/1.0.830/1.0.832. Affected is an unknown function of the component SSH Server. The manipulation leads to backdoor. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.900 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2022-34298	The NT auth module in OpenAM before 14.6.6 allows a "replace Samba username attack."	5.3	More Details
CVE-2021-38879	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 209057.	5.3	More Details
CVE-2017-20106	A vulnerability, which was classified as critical, has been found in Lithium Forum 2017 Q1. This issue affects some unknown processing of the component Compose Message Handler. The manipulation of the argument upload_url leads to server-side request forgery. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2017-20084	A vulnerability has been found in JUNG Smart Visu Server 1.0.804/1.0.830/1.0.832 and classified as critical. Affected by this vulnerability is an unknown functionality of the component KNX Group Address. The manipulation leads to backdoor. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.900 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2022-31248	A Observable Response Discrepancy vulnerability in spacewalk-java of SUSE Manager Server 4.1, SUSE Manager Server 4.2 allows remote attackers to discover valid usernames. This issue affects: SUSE Manager Server 4.1 spacewalk-java versions prior to 4.1.46-1. SUSE Manager Server 4.2 spacewalk-java versions prior to 4.2.37-1.	5.3	More Details
CVE-2022-31068	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. In affected versions all GLPI instances with the native inventory used may leak sensitive information. The feature to get refused file is not authenticated. This issue has been addressed in version 10.0.2 and all affected users are advised to upgrade.	5.3	More Details
CVE-2022-32549	Apache Sling Commons Log <= 5.4.0 and Apache Sling API <= 2.25.0 are vulnerable to log injection. The ability to forge logs may allow an attacker to cover tracks by injecting fake logs and potentially corrupt log files.	5.3	More Details
CVE-2022-0085	Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.	5.3	More Details
CVE-2022-29526	Go before 1.17.10 and 1.18.x before 1.18.2 has Incorrect Privilege Assignment. When called with a non-zero flags parameter, the Faccessat function could incorrectly report that a file is accessible.	5.3	More Details
CVE-2017-20107	A vulnerability, which was classified as problematic, was found in ShadeYouVPN.com Client 2.0.1.11. Affected is an unknown function. The manipulation leads to improper privilege management. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Upgrading to version 2.0.1.12 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9754	NAVER Whale browser mobile app before 1.10.6.2 allows the attacker to bypass its browser unlock function via incognito mode.	5.3	More Details
CVE-2022-29578	Meridian Cooperative Utility Software versions 22.02 and 22.03 allows remote attackers to obtain sensitive information such as name, address, and daily energy usage.	5.3	More Details
CVE-2022-23080	In directus versions v9.0.0-beta.2 through 9.6.0 are vulnerable to server-side request forgery (SSRF) in the media upload functionality which allows a low privileged user to perform internal network port scans.	5.0	More Details
CVE-2021-30651	A malicious authenticated SMG administrator user can obtain passwords for external LDAP/Active Directory servers that they might not otherwise be authorized to access.	4.9	More Details
CVE-2022-29097	Dell WMS 3.6.1 and below contains a Path Traversal vulnerability in Device API. A remote attacker could potentially exploit this vulnerability, to gain unauthorized read access to the files stored on the server filesystem, with the privileges of the running web application.	4.9	More Details
CVE-2021-3434	Stack based buffer overflow in le_ecred_conn_req(). Zephyr versions >= v2.5.0 Stack-based Buffer Overflow (CWE-121). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-8w87-6rfp-cfrm	4.9	More Details
CVE-2022-29330	Missing access control in the backup system of Telesoft VitalPBX before 3.2.1 allows attackers to access the PJSIP and SIP extension credentials, cryptographic keys and voicemails files via unspecified vectors.	4.9	More Details
CVE-2022-32535	The Bosch Ethernet switch PRA-ES8P2S with software version 1.01.05 runs its web server with root privilege. In combination with CVE-2022-23534 this could give an attacker root access to the switch.	4.8	More Details
CVE-2022-1326	The Form - Contact Form WordPress plugin through 1.2.0 does not sanitize and escape Custom text fields, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31104	Wasmtime is a standalone runtime for WebAssembly. In affected versions wasmtime's implementation of the SIMD proposal for WebAssembly on x86_64 contained two distinct bugs in the instruction lowerings implemented in Cranelift. The aarch64 implementation of the simd proposal is not affected. The bugs were presented in the `i8x16.swizzle` and `select` WebAssembly instructions. The `select` instruction is only affected when the inputs are of `v128` type. The correspondingly affected Cranelift instructions were `swizzle` and `select`. The `swizzle` instruction lowering in Cranelift erroneously overwrote the mask input register which could corrupt a constant value, for example. This means that future uses of the same constant may see a different value than the constant itself. The `select` instruction lowering in Cranelift wasn't correctly implemented for vector types that are 128-bits wide. When the condition was 0 the wrong instruction was used to move the correct input to the output of the instruction meaning that only the low 32 bits were moved and the upper 96 bits of the result were left as whatever the register previously contained (instead of the input being moved from). The `select` instruction worked correctly if the condition was nonzero, however. This bug in Wasmtime's implementation of these instructions on x86_64 represents an incorrect implementation of the specified semantics of these instructions according to the WebAssembly specification. The impact of this is benign for hosts running WebAssembly but represents possible vulnerabilities within the execution of a guest program. For example a WebAssembly program could take unintended branches or materialize incorrect values internally which runs the risk of exposing the program itself to other related vulnerabilities which can occur from miscompilations. We have released Wasmtime 0.38.1 and cranelift-codegen (and other associated cranelift crates) 0.85.1 which contain the corrected implementations of these two instructions in Cranelift. If upgrading is not an option for you at this time, you can avoid the vulnerability by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other aarch64 hosts are not affected. Note that s390x hosts don't yet implement the simd proposal and are not affected.	4.8	More Details
CVE-2022-33009	A stored cross-site scripting (XSS) vulnerability in LightCMS v1.3.11 allows attackers to execute arbitrary web scripts or HTML via uploading a crafted PDF file.	4.8	More Details
CVE-2022-1327	The Image Gallery WordPress plugin before 1.1.6 does not sanitize and escape some of its Image fields, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-32987	Multiple cross-site scripting (XSS) vulnerabilities in /bsms/?page=manage_account of Simple Bakery Shop Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Username or Full Name fields.	4.8	More Details
CVE-2022-1010	The Login using WordPress Users (WP as SAML IDP) WordPress plugin before 1.13.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-1321	The miniOrange's Google Authenticator WordPress plugin before 5.5.6 does not sanitise and escape some of its settings, leading to malicious users with administrator privileges to store malicious Javascript code leading to Cross-Site Scripting attacks when unfiltered_html is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-1113	The Flower Delivery by Florist One WordPress plugin through 3.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setups)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1095	The Mihdan: No External Links WordPress plugin before 5.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-1029	The Limit Login Attempts WordPress plugin before 4.0.72 does not sanitise and escape some of its settings, leading to malicious users with administrator privileges to store malicious Javascript code leading to Cross-Site Scripting attacks when unfiltered_html is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-1028	The WordPress Security Firewall, Malware Scanner, Secure Login and Backup plugin before 4.2.1 does not sanitise and escape some of its settings, leading to malicious users with administrator privileges to store malicious Javascript code leading to Cross-Site Scripting attacks when unfiltered_html is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-1971	The NextCellent Gallery WordPress plugin through 1.9.35 does not sanitise and escape some of its image settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-1990	The Nested Pages WordPress plugin before 3.1.21 does not escape and sanitize the some of its settings, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when the unfiltered_html is disallowed	4.8	More Details
CVE-2022-1994	The Login With OTP Over SMS, Email, WhatsApp and Google Authenticator WordPress plugin before 1.0.8 does not escape its 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-2022-1995	The Malware Scanner WordPress plugin before 4.5.2 does not sanitise and escape some of its settings, leading to malicious users with administrator privileges to store malicious Javascript code leading to Cross-Site Scripting attacks when unfiltered_html is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-33122	A stored cross-site scripting (XSS) vulnerability in eyoucms v1.5.6 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the URL field under the login page.	4.8	More Details
CVE-2022-32530	A CWE-668 Exposure of Resource to Wrong Sphere vulnerability exists that could cause users to be misled, hiding alarms, showing the wrong server connection option or the wrong control request when a mobile device has been compromised by a malicious application. Affected Product: Geo SCADA Mobile (Build 222 and prior)	4.8	More Details
CVE-2022-30562	If the user enables the https function on the device, an attacker can modify the user's request data packet through a man-in-the-middle attack ,Injection of a malicious URL in the Host: header of the HTTP Request results in a 302 redirect to an attacker-controlled page.	4.7	More Details
CVE-2022-1740	The tested version of Dominion Voting Systems ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device.	4.6	More Details
CVE-2022-1747	The authentication mechanism used by voters to activate a voting session on the tested version of Dominion Voting Systems ImageCast X is susceptible to forgery. An attacker could leverage this vulnerability to print an arbitrary number of ballots without authorization.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33953	IBM Robotic Process Automation 21.0.1 and 21.0.2 could allow a user with psychical access to the system to obtain sensitive information due to insufficiently protected access tokens. IBM X-Force ID: 229198.	4.6	More Details
CVE-2017-20102	A vulnerability was found in Album Lock 4.0 and classified as critical. Affected by this issue is some unknown functionality of the file /getImage. The manipulation of the argument filePaht leads to path traversal. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	4.4	More Details
CVE-2022-1847	The Rotating Posts WordPress plugin through 1.11 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2022-1845	The WP Post Styling WordPress plugin before 1.3.1 does not have CSRF checks in various actions, which could allow attackers to make a logged in admin delete plugin's data, update the settings, add new entries and more via CSRF attacks	4.3	More Details
CVE-2022-1914	The Clean-Contact WordPress plugin through 1.6 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored XSS due to the lack of sanitisation and escaping as well	4.3	More Details
CVE-2022-1913	The Add Post URL WordPress plugin through 2.1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping	4.3	More Details
CVE-2022-34206	A missing permission check in Jenkins Jianliao Notification Plugin 1.1 and earlier allows attackers with Overall/Read permission to send HTTP POST requests to an attacker-specified URL.	4.3	More Details
CVE-2022-34208	A missing permission check in Jenkins Beaker builder Plugin 1.10 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2022-1885	The Cimy Header Image Rotator WordPress plugin through 6.1.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2022-1846	The Tiny Contact Form WordPress plugin through 0.7 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2017-20091	A vulnerability was found in File Manager Plugin 3.0.1. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely.	4.3	More Details
CVE-2017-20090	A vulnerability was found in Global Content Blocks Plugin 2.1.5. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely.	4.3	More Details
CVE-2017-20088	A vulnerability classified as problematic has been found in Atahualpa Theme. Affected is an unknown function. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely.	4.3	More Details
CVE-2022-1844	The WP Sentry WordPress plugin through 1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping as well	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34204	A missing permission check in Jenkins EasyQA Plugin 1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server.	4.3	More Details
CVE-2022-1842	The OpenBook Book Data WordPress plugin through 3.5.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping as well	4.3	More Details
CVE-2022-1653	The Social Share Buttons by Supsystic WordPress plugin before 2.2.4 does not perform CSRF checks in it's ajax endpoints and admin pages, allowing an attacker to trick any logged in user to manipulate or change the plugin settings, as well as create, delete and rename projects and networks.	4.3	More Details
CVE-2021-3431	Assertion reachable with repeated LL_FEATURE_REQ. Zephyr versions >= v2.5.0 contain Reachable Assertion (CWE-617). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7548-5m6f-mqv9	4.3	More Details
CVE-2021-3432	Invalid interval in CONNECT_IND leads to Division by Zero. Zephyr versions >= v1.14.0 Divide By Zero (CWE-369). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7364-p4wc-8mj4	4.3	More Details
CVE-2022-1627	The My Private Site WordPress plugin before 3.0.8 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2022-1625	The New User Approve WordPress plugin before 2.4 does not have CSRF check in place when updating its settings and adding invitation codes, which could allow attackers to add invitation codes (for bypassing the provided restrictions) and to change plugin settings by tricking admin users into visiting specially crafted websites.	4.3	More Details
CVE-2022-1573	The HTML2WP WordPress plugin through 1.0.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them	4.3	More Details
CVE-2022-29858	Silverstripe silverstripe/assets through 1.10 is vulnerable to improper access control that allows protected images to be published by changing an existing image short code on website content.	4.3	More Details
CVE-2022-1960	The MyCSS WordPress plugin through 1.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2017-20093	A vulnerability, which was classified as problematic, was found in Download Manager Plugin 2.8.99. Affected is an unknown function. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely.	4.3	More Details
CVE-2022-0875	The Google Authenticator WordPress plugin before 1.0.5 does not have CSRF check when saving its settings, and does not sanitise as well as escape them, allowing attackers to make a logged in admin change them and perform Cross-Site Scripting attacks	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31036	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v1.3.0 are vulnerable to a symlink following bug allowing a malicious user with repository write access to leak sensitive YAML files from Argo CD's repo-server. A malicious Argo CD user with write access for a repository which is (or may be) used in a Helm-type Application may commit a symlink which points to an out-of-bounds file. If the target file is a valid YAML file, the attacker can read the contents of that file. Sensitive files which could be leaked include manifest files from other Applications' source repositories (potentially decrypted files, if you are using a decryption plugin) or any YAML-formatted secrets which have been mounted as files on the repo-server. Patches for this vulnerability has been released in the following Argo CD versions: v2.4.1, v2.3.5, v2.2.10 and v2.1.16. If you are using a version >=v2.3.0 and do not have any Helm-type Applications you may disable the Helm config management tool as a workaround.	4.3	More Details
CVE-2022-0444	The Backup, Restore and Migrate WordPress Sites With the XCloner Plugin WordPress plugin before 4.3.6 does not have authorisation and CSRF checks when resetting its settings, allowing unauthenticated attackers to reset them, including generating a new backup encryption key.	4.3	More Details
CVE-2021-20421	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	4.3	More Details
CVE-2021-20544	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 198931.	4.3	More Details
CVE-2022-31039	Greenlight is a simple front-end interface for your BigBlueButton server. In affected versions an attacker can view any room's settings even though they are not authorized to do so. Only the room owner and administrator should be able to view a room's settings. This issue has been patched in release version 2.12.6.	4.3	More Details
CVE-2022-34013	OneBlog v2.3.4 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via the Logo parameter under the Link module.	4.3	More Details
CVE-2022-34011	OneBlog v2.3.4 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via the parameter entryUrls.	4.3	More Details
CVE-2022-31076	KubeEdge is built upon Kubernetes and extends native containerized application orchestration and device management to hosts at the Edge. In affected versions a malicious message can crash CloudCore by triggering a nil-pointer dereference in the UDS Server. Since the UDS Server only communicates with the CSI Driver on the cloud side, the attack is limited to the local host network. As such, an attacker would already need to be an authenticated user of the Cloud. Additionally it will be affected only when users turn on the unixsocket switch in the config file cloudcore.yaml. This bug has been fixed in Kubeedge 1.11.0, 1.10.1, and 1.9.3. Users should update to these versions to resolve the issue. Users unable to upgrade should sisable the unixsocket switch of CloudHub in the config file cloudcore.yaml.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31108	Mermaid is a JavaScript based diagramming and charting tool that uses Markdown-inspired text definitions and a renderer to create and modify complex diagrams. An attacker is able to inject arbitrary `CSS` into the generated graph allowing them to change the styling of elements outside of the generated graph, and potentially exfiltrate sensitive information by using specially crafted `CSS` selectors. The following example shows how an attacker can exfiltrate the contents of an input field by bruteforcing the `value` attribute one character at a time. Whenever there is an actual match, an `http` request will be made by the browser in order to "load" a background image that will let an attacker know what's the value of the character. This issue may lead to `Information Disclosure` via CSS selectors and functions able to generate HTTP requests. This also allows an attacker to change the document in ways which may lead a user to perform unintended actions, such as clicking on a link, etc. This issue has been resolved in version 9.1.3. Users are advised to upgrade. Users unable to upgrade should ensure that user input is adequately escaped before embedding it in CSS blocks.	4.1	More Details
CVE-2022-31077	KubeEdge is built upon Kubernetes and extends native containerized application orchestration and device management to hosts at the Edge. In affected versions a malicious message response from KubeEdge can crash the CSI Driver controller server by triggering a nil-pointer dereference panic. As a consequence, the CSI Driver controller will be in denial of service. This bug has been fixed in Kubeedge 1.11.0, 1.10.1, and 1.9.3. Users should update to these versions to resolve the issue. At the time of writing, no workaround exists.	4.0	More Details
CVE-2021-3435	Information leakage in le_ecred_conn_req(). Zephyr versions >= v2.4.0 Use of Uninitialized Resource (CWE-908). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-xhg3-gvj6-4rqh	4.0	More Details
CVE-2021-3433	Invalid channel map in CONNECT_IND results to Deadlock. Zephyr versions >= v2.5.0 Improper Check or Handling of Exceptional Conditions (CWE-703). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-3c2f-w4v6-qxrp	4.0	More Details
CVE-2022-2106	Elcomplus SmartICS v2.3.4.0 does not validate the filenames sufficiently, which enables authenticated administrator-level users to perform path traversal attacks and specify arbitrary files.	3.8	More Details
CVE-2017-20092	A vulnerability classified as problematic was found in Google Analytics Dashboard Plugin 2.1.1. Affected by this vulnerability is an unknown functionality. The manipulation leads to basic cross site scripting. The attack can be launched remotely.	3.5	More Details
CVE-2017-20085	A vulnerability has been found in Atahualpa Theme and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to basic cross site scripting. The attack can be launched remotely.	3.5	More Details
CVE-2017-20101	A vulnerability, which was classified as problematic, was found in ProjectSend r754. This affects an unknown part of the file process.php?do=zip_download. The manipulation of the argument client/file leads to information disclosure. It is possible to initiate the attack remotely.	3.5	More Details
CVE-2017-20094	A vulnerability, which was classified as problematic, has been found in NewStatPress Plugin 1.2.4. This issue affects some unknown processing. The manipulation leads to basic cross site scripting (Persistent). The attack may be initiated remotely. Upgrading to version 1.2.5 is able to address this issue. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2017-20100	A vulnerability was found in Air Transfer 1.0.14/1.2.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20098	A vulnerability was found in Admin Custom Login Plugin 2.4.5.2. It has been classified as problematic. Affected is an unknown function. The manipulation leads to basic cross site scripting (Persistent). It is possible to launch the attack remotely.	3.5	More Details
CVE-2017-20087	A vulnerability, which was classified as problematic, has been found in Alpine PhotoTile for Instagram Plugin 1.2.7.7. Affected by this issue is some unknown functionality. The manipulation leads to basic cross site scripting. The attack may be launched remotely.	3.5	More Details
CVE-2017-20097	A vulnerability was found in WP-Filebase Download Manager Plugin 3.4.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross site scripting. The attack may be launched remotely.	3.5	More Details
CVE-2017-20096	A vulnerability classified as problematic has been found in WP-SpamFree Anti-Spam Plugin 2.1.1.4. This affects an unknown part. The manipulation leads to basic cross site scripting. It is possible to initiate the attack remotely.	3.5	More Details
CVE-2017-20089	A vulnerability was found in Gwolle Guestbook Plugin 1.7.4. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to basic cross site scripting. The attack may be initiated remotely.	3.5	More Details
CVE-2022-2213	A vulnerability was found in SourceCodester Library Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/edit_admin_details.php?id=admin. The manipulation of the argument Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-0987	A flaw was found in PackageKit in the way some of the methods exposed by the Transaction interface examines files. This issue allows a local user to measure the time the methods take to execute and know whether a file owned by root or other users exists.	3.3	More Details
CVE-2021-20551	IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 199149.	3.3	More Details
CVE-2022-33879	The initial fixes in CVE-2022-30126 and CVE-2022-30973 for regexes in the StandardsExtractingContentHandler were insufficient, and we found a separate, new regex DoS in a different regex in the StandardsExtractingContentHandler. These are now fixed in 1.28.4 and 2.4.1.	3.3	More Details
CVE-2022-31017	Zulip is an open-source team collaboration tool. Versions 2.1.0 through and including 5.2 are vulnerable to a logic error. A stream configured as private with protected history, where new subscribers should not be allowed to see messages sent before they were subscribed, when edited causes the server to incorrectly send an API event that includes the edited message to all of the stream's current subscribers. This API event is ignored by official clients, but can be observed by using a modified client or the browser's developer tools. This bug will be fixed in Zulip Server 5.3. There are no known workarounds.	2.0	More Details
CVE-2022-29301	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-20660. Reason: This candidate is a reservation duplicate of CVE-2021-20660. Notes: All CVE users should reference CVE-2021-20660 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-29299	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-20660. Reason: This candidate is a reservation duplicate of CVE-2021-20660. Notes: All CVE users should reference CVE-2021-20660 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23056	In ERPNext, versions v13.0.0-beta.13 through v13.30.0 are vulnerable to Stored XSS at the Patient History page which allows a low privilege user to conduct an account takeover attack.	N/A	More Details
CVE-2022-23058	ERPNext in versions v12.0.9-v13.0.3 are affected by a stored XSS vulnerability that allows low privileged users to store malicious scripts in the ‘username’ field in ‘my settings’ which can lead to full account takeover.	N/A	More Details
CVE-2022-23055	In ERPNext, versions v11.0.0-beta through v13.0.2 are vulnerable to Missing Authorization, in the chat rooms functionality. A low privileged attacker can send a direct message or a group message to any member or group, impersonating themselves as the administrator. The attacker can also read chat messages of groups that they do not belong to, and of other users.	N/A	More Details
CVE-2022-2246	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-34491	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-29969. Reason: This candidate is a duplicate of CVE-2022-29969. A typo caused the wrong ID to be used. Notes: All CVE users should reference CVE-2022-29969 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-30932	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-2013-2216	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-2022-32159	In openlibrary versions deploy-2016-07-0 through deploy-2021-12-22 are vulnerable to Stored XSS.	N/A	More Details
CVE-2013-2180	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-23078	In habitica versions v4.119.0 through v4.232.2 are vulnerable to open redirect via the login page.	N/A	More Details
CVE-2022-23079	In motor-admin versions 0.0.1 through 0.2.56 are vulnerable to host header injection in the password reset functionality where malicious actor can send fake password reset email to arbitrary victim.	N/A	More Details
CVE-2013-2084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2013-2069. Reason: This candidate is a reservation duplicate of CVE-2013-2069. Notes: All CVE users should reference CVE-2013-2069 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-34604	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. It is a duplicate of CVE-2022-22514. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23081	In openlibrary versions deploy-2016-07-0 through deploy-2021-12-22 are vulnerable to Reflected XSS.	N/A	More Details