SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 November 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-2022-29822	Due to improper parameter filtering in the Feathers js library, which may ultimately lead to SQL injection	10.0	More Details
CVE-2021-36206	All versions of CEVAS prior to 1.01.46 do not sufficiently validate user-controllable input and could allow a user to bypass authentication and retrieve data with specially crafted SQL queries.	10.0	More Details
CVE-2022-2421	Due to improper type validation in attachment parsing the Socket.io js library, it is possible to overwrite the _placeholder object which allows an attacker to place references to functions at arbitrary places in the resulting query object.	10.0	More Details
CVE-2022-2422	Due to improper input validation in the Feathers js library, it is possible to perform a SQL injection attack on the back-end database, in case the feathers-sequelize package is used.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29823	Feather-Sequalize cleanQuery method uses insecure recursive logic to filter unsupported keys from the query object. This results in a Remote Code Execution (RCE) with privileges of application.	10.0	More Details
CVE-2021-38397	Honeywell Experion PKS C200, C200E, C300, and ACE controllers are vulnerable to unrestricted file uploads, which may allow an attacker to remotely execute arbitrary code and cause a denial-of-service condition.	10.0	More Details
CVE-2022-42925	There is a vulnerability on Forma LMS version 3.1.0 and earlier that could allow an authenticated attacker (with the role of student) to privilege escalate in order to upload a Zip file through the plugin upload component. The exploitation of this vulnerability could lead to a remote code injection.	9.9	More Details
CVE-2022-41681	There is a vulnerability on Forma LMS version 3.1.0 and earlier that could allow an authenticated attacker (with the role of student) to privilege escalate in order to upload a Zip file through the SCORM importer feature. The exploitation of this vulnerability could lead to a remote code injection.	9.9	More Details
CVE-2022-37425	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in OpenNebula OpenNebula core on Linux allows Remote Code Inclusion.	9.9	More Details
CVE-2022-39366	DataHub is an open-source metadata platform. Prior to version 0.8.45, the `StatelessTokenService` of the DataHub metadata service (GMS) does not verify the signature of JWT tokens. This allows an attacker to connect to DataHub instances as any user if Metadata Service authentication is enabled. This vulnerability occurs because the `StatelessTokenService` of the Metadata service uses the `parse` method of `io.jsonwebtoken.JwtParser`, which does not perform a verification of the cryptographic token signature. This means that JWTs are accepted regardless of the used algorithm. This issue may lead to an authentication bypass. Version 0.8.45 contains a patch for the issue. There are no known workarounds.	9.9	More Details
CVE-2022-43002	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep54_pskpwd parameter at /goform/form2WizardStep54.	9.8	More Details
CVE-2022-41657	Delta Electronics InfraSuite Device Master Versions 00.00.01a and prior allow attacker provided data already serialized into memory to be used in file operation application programmable interfaces (APIs). This could create arbitrary files, which could be used in API operations and could ultimately result in remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43003	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setRepeaterSecurity function.	9.8	More Details
CVE-2022-37621	Prototype pollution vulnerability in function resolveShims in resolve-shims.js in thlorenz browserify-shim 3.8.15 via the fullPath variable in resolve-shims.js.	9.8	More Details
CVE-2022-43286	Nginx NJS v0.7.2 was discovered to contain a heap-use-after-free bug caused by illegal memory copy in the function njs_json_parse_iterator_call at njs_json.c.	9.8	More Details
CVE-2022-3754	Weak Password Requirements in GitHub repository thorsten/phpmyfaq prior to 3.1.8.	9.8	More Details
CVE-2021-42777	Stimulsoft (aka Stimulsoft Reports) 2013.1.1600.0, when Compilation Mode is used, allows an attacker to execute arbitrary C# code on any machine that renders a report, including the application server or a user's local machine, as demonstrated by System.Diagnostics.Process.Start.	9.8	More Details
CVE-2022-40741	Mail SQR Expert’s specific function has insufficient filtering for special characters. An unauthenticated remote attacker can exploit this vulnerability to perform arbitrary system command and disrupt service.	9.8	More Details
CVE-2022-37623	Prototype pollution vulnerability in function resolveShims in resolve-shims.js in thlorenz browserify-shim 3.8.15 via the shimPath variable in resolve-shims.js.	9.8	More Details
CVE-2020-21016	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary code as root via HNAP1/control/SetGuestWLanSettings.php.	9.8	More Details
CVE-2021-40241	xfig 3.2.7 is vulnerable to Buffer Overflow.	9.8	More Details
CVE-2022-3254	The WordPress Classifieds Plugin WordPress plugin before 4.3 does not properly sanitise and escape some parameters before using them in a SQL statement via an AJAX action available to unauthenticated users and when a specific premium module is active, leading to a SQL injection	9.8	More Details
CVE-2022-40471	Remote Code Execution in Clinic's Patient Management System v 1.0 allows Attacker to Upload arbitrary php webshell via profile picture upload functionality in users.php	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31692	Spring Security, versions 5.7 prior to 5.7.5 and 5.6 prior to 5.6.9 could be susceptible to authorization rules bypass via forward or include dispatcher types. Specifically, an application is vulnerable when all of the following are true: The application expects that Spring Security applies security to forward and include dispatcher types. The application uses the AuthorizationFilter either manually or via the authorizeHttpRequests() method. The application configures the FilterChainProxy to apply to forward and/or include requests (e.g. spring.security.filter.dispatcher-types = request, error, async, forward, include). The application may forward or include the request to a higher privilege-secured endpoint.The application configures Spring Security to apply to every dispatcher type via authorizeHttpRequests().shouldFilterAllDispatcherTypes(true)	9.8	More Details
CVE-2022-38142	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior deserialize user-supplied data provided through the Device-Gateway service port without proper verification. An attacker could provide malicious serialized objects to execute arbitrary code upon deserialization.	9.8	More Details
CVE-2022-40202	The database backup function in Delta Electronics InfraSuite Device Master Versions 00.00.01a and prior lacks proper authentication. An attacker could provide malicious serialized objects which, when deserialized, could activate an opcode for a backup scheduling function without authentication. This function allows the user to designate all function arguments and the file to be executed. This could allow the attacker to start any new process and achieve remote code execution.	9.8	More Details
CVE-2022-43774	The HandlerPageP_KID class in Delta Electronics DIAEnergy v1.9 contains a SQL Injection flaw that could allow an attacker to gain code execution on a remote system.	9.8	More Details
CVE-2022-2474	Authentication is currently unsupported in Haas Controller version 100.20.000.1110 when using the “Ethernet Q Commands” service, which allows any user on the same network segment as the controller (even while connected remotely) to access the service and write unauthorized macros to the device.	9.8	More Details
CVE-2022-41688	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior lack proper authentication for functions that create and modify user groups. An attacker could provide malicious serialized objects that could run these functions without authentication to create a new user and add them to the administrator group.	9.8	More Details
CVE-2022-41772	Delta Electronics InfraSuite Device Master Versions 00.00.01a and prior mishandle .ZIP archives containing characters used in path traversal. This path traversal could result in remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42468	Apache Flume versions 1.4.0 through 1.10.1 are vulnerable to a remote code execution (RCE) attack when a configuration uses a JMS Source with an unsafe providerURL. This issue is fixed by limiting JNDI to allow only the use of the java protocol or no protocol.	9.8	More Details
CVE-2022-40293	The application was vulnerable to a session fixation that could be used hijack accounts.	9.8	More Details
CVE-2022-40296	The application was vulnerable to a Server-Side Request Forgery attacks, allowing the backend server to interact with unexpected endpoints, potentially including internal and local services, leading to attacks in other downstream systems.	9.8	More Details
CVE-2022-44542	lesspipe before 2.06 allows attackers to execute code via Perl Storable (pst) files, because of deserialized object destructor execution via a key/value pair in a hash.	9.8	More Details
CVE-2022-2572	In affected versions of Octopus Server where access is managed by an external authentication provider, it was possible that the API key/keys of a disabled/deleted user were still valid after the access was revoked.	9.8	More Details
CVE-2022-41552	Server-Side Request Forgery (SSRF) vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Data Center Analytics, Analytics probe components), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe components) allows Server Side Request Forgery. This issue affects Hitachi Infrastructure Analytics Advisor: from 2.0.0-00 through 4.4.0-00; Hitachi Ops Center Analyzer: from 10.0.0-00 before 10.9.0-00.	9.8	More Details
CVE-2022-32941	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A buffer overflow may result in arbitrary code execution.	9.8	More Details
CVE-2022-42808	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. A remote user may be able to cause kernel code execution.	9.8	More Details
CVE-2022-42813	A certificate validation issue existed in the handling of WKWebView. This issue was addressed with improved validation. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. Processing a maliciously crafted certificate may lead to arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27582	Password recovery vulnerability in SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The firmware versions <=1.10.1 allow to optionally disable device configuration over the network interfaces. Please make sure that you apply general security practices when operating the SIM4000. A fix is planned but not yet scheduled.	9.8	More Details
CVE-2022-27584	Password recovery vulnerability in SICK SIM2000ST Partnumber 1080579 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The firmware versions <=1.7.0 allow to optionally disable device configuration over the network interfaces. Please make sure that you apply general security practices when operating the SIM2000ST. A fix is planned but not yet scheduled.	9.8	More Details
CVE-2022-27585	Password recovery vulnerability in SICK SIM1000 FX Partnumber 1097816 and 1097817 with firmware version <1.6.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.6.0 as soon as possible (available in SICK Support Portal).	9.8	More Details
CVE-2022-2475	Haas Controller version 100.20.000.1110 has insufficient granularity of access control when using the "Ethernet Q Commands" service. Any user is able to write macros into registers outside of the authorized accessible range. This could allow a user to access privileged resources or resources out of context.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27586	Password recovery vulnerability in SICK SIM1004 Partnumber 1098148 with firmware version <2.0.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 2.0.0 as soon as possible (available in SICK Support Portal).	9.8	More Details
CVE-2022-37913	Vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an unauthenticated remote attacker to bypass authentication. Successful exploitation of these vulnerabilities could allow an attacker to gain administrative privileges leading to a complete compromise of the Aruba EdgeConnect Enterprise Orchestrator with versions 9.1.2.40051 and below, 9.0.7.40108 and below, 8.10.23.40009 and below, and any older branches of Orchestrator not specifically mentioned.	9.8	More Details
CVE-2022-39976	School Activity Updates with SMS Notification v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /modules/announcement/index.php?view=edit&id=.	9.8	More Details
CVE-2022-3386	Advantech R-SeeNet Versions 2.4.17 and prior are vulnerable to a stack-based buffer overflow. An unauthorized attacker can use an outsized filename to overflow the stack buffer and enable remote code execution.	9.8	More Details
CVE-2022-40876	In Tenda ax1803 v1.0.0.1, the http requests handled by the fromAdvSetMacMtuWan functions, wanSpeed, cloneType, mac, can cause a stack overflow and enable remote code execution (RCE).	9.8	More Details
CVE-2022-43001	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setSecurity function.	9.8	More Details
CVE-2022-43367	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a command injection vulnerability in the formSetDebugCfg function.	9.8	More Details
CVE-2022-3095	The implementation of backslash parsing in the Dart URI class for versions prior to 2.18 and Flutter versions prior to 3.30 differs from the WhatWG URL standards. Dart uses the RFC 3986 syntax, which creates incompatibilities with the '\' characters in URIs, which can lead to auth bypass in webapps interpreting URIs. We recommend updating Dart or Flutter to mitigate the issue.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39365	Pimcore is an open source data and experience management platform. Prior to version 10.5.9, the user controlled twig templates rendering in `Pimcore/Mail` & `ClassDefinition\Layout\Text` is vulnerable to server-side template injection, which could lead to remote code execution. Version 10.5.9 contains a patch for this issue. As a workaround, one may apply the patch manually.	9.8	More Details
CVE-2022-43000	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep4_pskpwd parameter at /goform/form2WizardStep4.	9.8	More Details
CVE-2022-3363	Business Logic Errors in GitHub repository ikus060/rdiffweb prior to 2.5.0a7.	9.8	More Details
CVE-2022-43168	Rukovoditel v3.2.1 was discovered to contain a SQL injection vulnerability via the reports_id parameter.	9.8	More Details
CVE-2022-37914	Vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an unauthenticated remote attacker to bypass authentication. Successful exploitation of these vulnerabilities could allow an attacker to gain administrative privileges leading to a complete compromise of the Aruba EdgeConnect Enterprise Orchestrator with versions 9.1.2.40051 and below, 9.0.7.40108 and below, 8.10.23.40009 and below, and any older branches of Orchestrator not specifically mentioned.	9.8	More Details
CVE-2022-37915	A vulnerability in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to a complete system compromise of Aruba EdgeConnect Enterprise Orchestration with versions 9.1.x branch only, Any 9.1.x Orchestrator instantiated as a new machine with a release prior to 9.1.3.40197, Orchestrators upgraded to 9.1.x were not affected.	9.8	More Details
CVE-2022-3741	Impact varies for each individual vulnerability in the application. For generation of accounts, it may be possible, depending on the amount of system resources available, to create a DoS event in the server. These accounts still need to be activated; however, it is possible to identify the output Status Code to separate accounts that are generated and waiting for email verification. \n\nFor the sign in directories, it is possible to brute force login attempts to either login portal, which could lead to account compromise.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37782	Employee Record Management System v 1.2 is vulnerable to SQL Injection via editempprofile.php.	9.8	More Details
CVE-2021-38734	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Menu.php.	9.8	More Details
CVE-2021-38736	SEMCMS Shop V 1.1 is vulnerable to SQL Injection via Ant_Global.php.	9.8	More Details
CVE-2021-38737	SEMCMS v 1.1 is vulnerable to SQL Injection via Ant_Pro.php.	9.8	More Details
CVE-2021-38217	SEMCMS v 1.2 is vulnerable to SQL Injection via SEMCMS_User.php.	9.8	More Details
CVE-2021-38729	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Plist.php.	9.8	More Details
CVE-2021-38730	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Info.php.	9.8	More Details
CVE-2021-38731	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Zekou.php.	9.8	More Details
CVE-2021-38732	SEMCMS SHOP v 1.1 is vulnerable to SQL via Ant_Message.php.	9.8	More Details
CVE-2021-38733	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_BlogCat.php.	9.8	More Details
CVE-2022-42998	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the srcip parameter at /goform/form2IPQoSTcAdd.	9.8	More Details
CVE-2022-43775	The HICT_Loop class in Delta Electronics DIAEnergy v1.9 contains a SQL Injection flaw that could allow an attacker to gain code execution on a remote system.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3385	Advantech R-SeeNet Versions 2.4.17 and prior are vulnerable to a stack-based buffer overflow. An unauthorized attacker can remotely overflow the stack buffer and enable remote code execution.	9.8	More Details
CVE-2022-3708	The Web Stories plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including 1.24.0 due to insufficient validation of URLs supplied via the 'url' parameter found via the /v1/hotlink/proxy REST API Endpoint. This makes it possible for authenticated users to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	9.6	More Details
CVE-2022-39355	Discourse Patreon enables syncronization between Discourse Groups and Patreon rewards. On sites with Patreon login enabled, an improper authentication vulnerability could be used to take control of a victim's forum account. This vulnerability is patched in commit number 846d012151514b35ce42a1636c7d70f6dcee879e of the discourse-patreon plugin. Out of an abundance of caution, any Discourse accounts which have logged in with an unverified-email Patreon account will be logged out and asked to verify their email address on their next login. As a workaround, disable the patreon integration and log out all users with associated Patreon accounts.	9.1	More Details
CVE-2022-2782	In affected versions of Octopus Server it is possible for a session token to be valid indefinitely due to improper validation of the session token parameters.	9.1	More Details
CVE-2021-36898	Auth. SQL Injection (SQLi) vulnerability in Quiz And Survey Master plugin <= 7.3.4 on WordPress.	9.1	More Details
CVE-2021-38395	Honeywell Experion PKS C200, C200E, C300, and ACE controllers are vulnerable to improper neutralization of special elements in output, which may allow an attacker to remotely execute arbitrary code and cause a denial-of-service condition.	9.1	More Details
CVE-2022-31678	VMware Cloud Foundation (NSX-V) contains an XML External Entity (XXE) vulnerability. On VCF 3.x instances with NSX-V deployed, this may allow a user to exploit this issue leading to a denial-of-service condition or unintended information disclosure.	9.1	More Details
CVE-2022-27583	A remote unprivileged attacker can interact with the configuration interface of a Flexi-Compact FLX3-CPUC1 or FLX3-CPUC2 running an affected firmware version to potentially impact the availability of the FlexiCompact.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41636	Communication traffic involving "Ethernet Q Commands" service of Haas Controller version 100.20.000.1110 is transmitted in cleartext. This allows an attacker to obtain sensitive information being passed to and from the controller.	9.1	More Details
CVE-2022-40289	The application was vulnerable to an authenticated Stored Cross-Site Scripting (XSS) in the upload and download functionality, which could be leveraged to escalate privileges or compromise any accounts they can coerce into observing the targeted files.	9.0	More Details
CVE-2022-40288	The application was vulnerable to an authenticated Stored Cross-Site Scripting (XSS) in the user profile data fields, which could be leveraged to escalate privileges within and compromise any account that views their user profile.	9.0	More Details
CVE-2022-40287	The application was found to be vulnerable to an authenticated Stored Cross-Site Scripting (XSS) vulnerability in messaging functionality, leading to privilege escalation or a compromise of a targeted account.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-3723	Type confusion in V8 in Google Chrome prior to 107.0.5304.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-40291	The application was vulnerable to Cross-Site Request Forgery (CSRF) attacks, allowing an attacker to coerce users into sending malicious requests to the site to delete their account, or in rare circumstances, hijack their account and create other admin accounts.	8.8	More Details
CVE-2022-41133	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a SQL injection that exists in GetDIAE_line_message_settingsListParameters. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries.	8.8	More Details
CVE-2022-40967	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a SQL injection that exists in CheckIoTHubNameExisted. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32934	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. A remote user may be able to cause kernel code execution.	8.8	More Details
CVE-2022-41644	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior lacks authentication for a function that changes group privileges. An attacker could use this to create a denial-of-service state or escalate their own privileges.	8.8	More Details
CVE-2022-43340	A Cross-Site Request Forgery (CSRF) in dzzoffice 2.02.1_SC_UTF8 allows attackers to arbitrarily create user accounts and grant Administrator rights to regular users.	8.8	More Details
CVE-2022-32922	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-41779	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior deserialize network packets without proper verification. If the device connects to an attacker-controlled server, the attacker could send maliciously crafted packets that would be deserialized and executed, leading to remote code execution.	8.8	More Details
CVE-2022-0074	Untrusted Search Path vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server and LiteSpeed Web Server Container allows Privilege Escalation. This affects versions from 1.6.15 before 1.7.16.1.	8.8	More Details
CVE-2022-39286	Jupyter Core is a package for the core common functionality of Jupyter projects. Jupyter Core prior to version 4.11.2 contains an arbitrary code execution vulnerability in `jupyter_core` that stems from `jupyter_core` executing untrusted files in CWD. This vulnerability allows one user to run code as another. Version 4.11.2 contains a patch for this issue. There are no known workarounds.	8.8	More Details
CVE-2022-0073	Improper Input Validation vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server and LiteSpeed Web Server dashboards allows Command Injection. This affects 1.7.0 versions before 1.7.16.1.	8.8	More Details
CVE-2022-40190	SAUTER Controls moduWeb firmware version 2.7.1 is vulnerable to reflective cross-site scripting (XSS). The web application does not adequately sanitize request strings of malicious JavaScript. An attacker utilizing XSS could then execute malicious code in users' browsers and steal sensitive information, including user credentials.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40294	The application was identified to have an CSV injection in data export functionality, allowing for malicious code to be embedded within export data and then triggered in exported data viewers.	8.8	More Details
CVE-2022-39362	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want.	8.8	More Details
CVE-2022-41996	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.	8.8	More Details
CVE-2022-3370	Use after free in Custom Elements in Google Chrome prior to 106.0.5249.91 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3373	Out of bounds write in V8 in Google Chrome prior to 106.0.5249.91 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-32888	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-42309	Xenstore: Guests can crash xenstored Due to a bug in the fix of XSA-115 a malicious guest can cause xenstored to use a wrong pointer during node creation in an error path, resulting in a crash of xenstored or a memory corruption in xenstored causing further damage. Entering the error path can be controlled by the guest e.g. by exceeding the quota value of maximum nodes per domain.	8.8	More Details
CVE-2022-3304	Use after free in CSS in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-26709	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26710	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, tvOS 15.5, watchOS 8.6. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-35387	Hospital Management System v 4.0 is vulnerable to SQL Injection via file:hospital/hms/admin/view-patient.php.	8.8	More Details
CVE-2022-26730	A memory corruption issue existed in the processing of ICC profiles. This issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13. Processing a maliciously crafted image may lead to arbitrary code execution.	8.8	More Details
CVE-2022-26716	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-26717	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-3305	Use after free in survey in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-39361	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries.	8.8	More Details
CVE-2022-3306	Use after free in survey in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3659	Use after free in Accessibility in Google Chrome on Chrome OS prior to 107.0.5304.62 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific UI interactions. (Chromium security severity: Medium)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2864	The demon image annotation plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.7. This is due to missing nonce validation in the ~/includes/settings.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-3658	Use after free in Feedback service on Chrome OS in Google Chrome on Chrome OS prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-3657	Use after free in Extensions in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-3656	Insufficient data validation in File System in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-3655	Heap buffer overflow in Media Galleries in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-3654	Use after free in Layout in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3401	The Bricks theme for WordPress is vulnerable to remote code execution due to the theme allowing site editors to include executable code blocks in website content in versions 1.2 to 1.5.3. This, combined with the missing authorization vulnerability (CVE-2022-3400), makes it possible for authenticated attackers with minimal permissions, such as a subscriber, can edit any page, post, or template on the vulnerable WordPress website and inject a code execution block that can be used to achieve remote code execution.	8.8	More Details
CVE-2022-3653	Heap buffer overflow in Vulkan in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3652	Type confusion in V8 in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44019	In Total.js 4 before 0e5ace7, /api/common/ping can achieve remote command execution via shell metacharacters in the host parameter.	8.8	More Details
CVE-2022-42823	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-3357	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.	8.8	More Details
CVE-2022-39944	In Apache Linkis <=1.2.0 when used with the MySQL Connector/J, a deserialization vulnerability with possible remote code execution impact exists when an attacker has write access to a database and configures a JDBC EC with a MySQL data source and malicious parameters. Therefore, the parameters in the jdbc url should be blacklisted. Versions of Apache Linkis <= 1.2.0 will be affected, We recommend users to update to 1.3.0.	8.8	More Details
CVE-2022-40238	A Remote Code Injection vulnerability exists in CERT software prior to version 1.50.5. An authenticated attacker can inject arbitrary pickle object as part of a user's profile. This can lead to code execution on the server when the user's profile is accessed.	8.8	More Details
CVE-2022-28763	The Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.12.2 is susceptible to a URL parsing vulnerability. If a malicious Zoom meeting URL is opened, the malicious link may direct the user to connect to an arbitrary network address, leading to additional attacks including session takeovers.	8.8	More Details
CVE-2022-41773	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a SQL injection that exists in CheckDIACloud. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries.	8.8	More Details
CVE-2022-37202	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/advicefeedback/list	8.8	More Details
CVE-2022-42795	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 16, iOS 16, macOS Ventura 13, watchOS 9. Processing a maliciously crafted image may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3315	Type confusion in Blink in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2022-3307	Use after free in media in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-26719	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-41702	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the InsertReg API.	8.7	More Details
CVE-2022-41701	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the PutShift API.	8.7	More Details
CVE-2022-41651	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the SetPF API.	8.7	More Details
CVE-2022-40965	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the PostEnergyType API.	8.7	More Details
CVE-2022-41555	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the PutLineMessageSetting API.	8.7	More Details
CVE-2022-3059	The application was vulnerable to multiple instances of SQL injection (authenticated and unauthenticated) through a vulnerable parameter. Due to the stacked query support, complex SQL commands could be crafted and injected into the vulnerable parameter and using a sleep based inferential SQL injection it was possible to extract data from the database.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3369	An Improper Access Control vulnerability in the bdservicehost.exe component, as used in Bitdefender Engines for Windows, allows an attacker to delete privileged registry keys by pointing a Registry symlink to a privileged key. This issue affects: Bitdefender Engines versions prior to 7.92659. It also affects Bitdefender Antivirus Free, Bitdefender Antivirus Plus, Bitdefender Internet Security, Bitdefender Total Security, as well as Bitdefender Endpoint Security Tools for Windows with engine versions prior to 7.92659.	8.6	More Details
CVE-2022-39367	QTIWorks is a software suite for standards-based assessment delivery. Prior to version 1.0-beta15, the QTIWorks Engine allows users to upload QTI content packages as ZIP files. The ZIP handling code does not sufficiently check the paths of files contained within ZIP files, so can insert files into other locations in the filesystem if they are writable by the process running the QTIWorks Engine. In extreme cases, this could allow anonymous users to change files in arbitrary locations in the filesystem. In normal QTIWorks Engine deployments, the impact is somewhat reduced because the default QTIWorks configuration does not enable the public demo functionality, so ZIP files can only be uploaded by users with "instructor" privileges. This vulnerability is fixed in version 1.0-beta15. There are no database configuration changes required when upgrading to this version. No known workarounds for this issue exist.	8.6	More Details
CVE-2022-32892	An access issue was addressed with improvements to the sandbox. This issue is fixed in Safari 16, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13. A sandboxed process may be able to circumvent sandbox restrictions.	8.6	More Details
CVE-2022-20933	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32890	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. A sandboxed process may be able to circumvent sandbox restrictions.	8.6	More Details
CVE-2022-42923	Forma LMS on its 3.1.0 version and earlier is vulnerable to a SQL injection vulnerability. The exploitation of this vulnerability could allow an authenticated attacker (with the role of student) to perform a SQL injection on the 'id' parameter in the 'appCore/index.php?r=adm/mediagallery/delete' function in order to dump the entire database or delete all contents from the 'core_user_file' table.	8.3	More Details
CVE-2022-3409	A vulnerability in bmcweb of OpenBMC Project allows user to cause denial of service. This vulnerability was identified during mitigation for CVE-2022-2809. When fuzzing the multipart_parser code using AFL++ with address sanitizer enabled to find smallest memory corruptions possible. It detected problem in how multipart_parser handles unclosed http headers. If long enough http header is passed in the multipart form without colon there is one byte overwrite on heap. It can be conducted multiple times in a loop to cause DoS.	8.2	More Details
CVE-2022-2741	The denial-of-service can be triggered by transmitting a carefully crafted CAN frame on the same CAN network as the vulnerable node. The frame must have a CAN ID matching an installed filter in the vulnerable node (this can easily be guessed based on CAN traffic analyses). The frame must contain the opposite RTR bit as what the filter installed in the vulnerable node contains (if the filter matches RTR frames, the frame must be a data frame or vice versa).	8.2	More Details
CVE-2022-39016	Javascript injection in PDFtron in M-Files Hubshare before 3.3.10.9 allows authenticated attackers to perform an account takeover via a crafted PDF upload.	8.2	More Details
CVE-2022-39017	Improper input validation and output encoding in all comments fields, in M-Files Hubshare before 3.3.10.9 allows authenticated attackers to introduce cross-site scripting attacks via specially crafted comments.	8.2	More Details
CVE-2022-39018	Broken access controls on PDFtron data in M-Files Hubshare before 3.3.11.3 allows unauthenticated attackers to access restricted PDF files via a known URL.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2809	A vulnerability in bmcweb of OpenBMC Project allows user to cause denial of service. When fuzzing the multipart_parser code using AFL++ with address sanitizer enabled to find smallest memory corruptions possible. It detected problem in how multipart_parser handles unclosed http headers. If long enough http header is passed in the multipart form without colon there is one byte overwrite on heap. It can be conducted multiple times in a loop to cause DoS.	8.2	More Details
CVE-2022-31690	Spring Security, versions 5.7 prior to 5.7.5, and 5.6 prior to 5.6.9, and older unsupported versions could be susceptible to a privilege escalation under certain conditions. A malicious user or attacker can modify a request initiated by the Client (via the browser) to the Authorization Server which can lead to a privilege escalation on the subsequent approval. This scenario can happen if the Authorization Server responds with an OAuth2 Access Token Response containing an empty scope list (per RFC 6749, Section 5.1) on the subsequent request to the token endpoint to obtain the access token.	8.1	More Details
CVE-2022-42915	curl before 7.86.0 has a double free. If curl is told to use an HTTP proxy for a transfer with a non-HTTP(S) URL, it sets up the connection to the remote server by issuing a CONNECT request to the proxy, and then tunnels the rest of the protocol through. An HTTP proxy might refuse this request (HTTP proxies often only allow outgoing connections to specific port numbers, like 443 for HTTPS) and instead return a non-200 status code to the client. Due to flaws in the error/cleanup handling, this could trigger a double free in curl if one of the following schemes were used in the URL for the transfer: dict, gopher, gophers, ldap, ldaps, rtmp, rtmps, or telnet. The earliest affected version is 7.77.0.	8.1	More Details
CVE-2022-33859	A security vulnerability was discovered in the Eaton Foreseer EPMS software. Foreseer EPMS connects an operation’s vast array of devices to assist in the reduction of energy consumption and avoid unplanned downtime caused by the failures of critical systems. A threat actor may upload arbitrary files using the file upload feature. This vulnerability is present in versions 4.x, 5.x, 6.x & 7.0 to 7.5. A new version (v7.6) containing the remediation has been made available by Eaton and a mitigation has been provided for the affected versions that are currently supported. Customers are advised to update the software to the latest version (v7.6). Foreseer EPMS versions 4.x, 5.x, 6.x are no longer supported by Eaton. Please refer to the End-of-Support notification https://www.eaton.com/in/en-us/catalog/services/foreseer/foreseer-legacy.html .	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3360	The LearnPress WordPress plugin before 4.1.7.2 unserialises user input in a REST API endpoint available to unauthenticated users, which could lead to PHP Object Injection when a suitable gadget is present, leadint to remote code execution (RCE). To successfully exploit this vulnerability attackers must have knowledge of the site secrets, allowing them to generate a valid hash via the wp_hash() function.	8.1	More Details
CVE-2022-39357	Winter is a free, open-source content management system based on the Laravel PHP framework. The Snowboard framework in versions 1.1.8, 1.1.9, and 1.2.0 is vulnerable to prototype pollution in the main Snowboard class as well as its plugin loader. The 1.0 branch of Winter is not affected, as it does not contain the Snowboard framework. This issue has been patched in v1.1.10 and v1.2.1. As a workaround, one may avoid this issue by following some common security practices for JavaScript, including implementing a content security policy and auditing scripts.	8.1	More Details
CVE-2022-41648	The HEIDENHAIN Controller TNC 640, version 340590 07 SP5, running HEROS 5.08.3 controlling the HARTFORD 5A-65E CNC machine is vulnerable to improper authentication, which may allow an attacker to deny service to the production line, steal sensitive data from the production line, and alter any products created by the production line.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39369	phpCAS is an authentication library that allows PHP applications to easily authenticate users via a Central Authentication Service (CAS) server. The phpCAS library uses HTTP headers to determine the service URL used to validate tickets. This allows an attacker to control the host header and use a valid ticket granted for any authorized service in the same SSO realm (CAS server) to authenticate to the service protected by phpCAS. Depending on the settings of the CAS server service registry in worst case this may be any other service URL (if the allowed URLs are configured to "^(https)://.*") or may be strictly limited to known and authorized services in the same SSO federation if proper URL service validation is applied. This vulnerability may allow an attacker to gain access to a victim's account on a vulnerable CASified service without victim's knowledge, when the victim visits attacker's website while being logged in to the same CAS server. phpCAS 1.6.0 is a major version upgrade that starts enforcing service URL discovery validation, because there is unfortunately no 100% safe default config to use in PHP. Starting this version, it is required to pass in an additional service base URL argument when constructing the client class. For more information, please refer to the upgrading doc. This vulnerability only impacts the CAS client that the phpCAS library protects against. The problematic service URL discovery behavior in phpCAS < 1.6.0 will only be disabled, and thus you are not impacted from it, if the phpCAS configuration has the following setup: 1. `phpCAS::setUrl()` is called (a reminder that you have to pass in the full URL of the current page, rather than your service base URL), and 2. `phpCAS::setCallbackURL()` is called, only when the proxy mode is enabled. 3. If your PHP's HTTP header input `X-Forwarded-Host`, `X-Forwarded-Server`, `Host`, `X-Forwarded-Proto`, `X-Forwarded-Protocol` is sanitized before reaching PHP (by a reverse proxy, for example), you will not be impacted by this vulnerability either. If your CAS server service registry is configured to only allow known and trusted service URLs the severity of the vulnerability is reduced substantially in its severity since an attacker must be in control of another authorized service. Otherwise, you should upgrade the library to get the safe service discovery behavior.	8.0	More Details
CVE-2022-41973	multipath-tools 0.7.7 through 0.9.x before 0.9.2 allows local users to obtain root access, as exploited in conjunction with CVE-2022-41974. Local users able to access /dev/shm can change symlinks in multipathd due to incorrect symlink handling, which could lead to controlled file writes outside of the /dev/shm directory. This could be used indirectly for local privilege escalation to root.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41974	multipath-tools 0.7.0 through 0.9.x before 0.9.2 allows local users to obtain root access, as exploited alone or in conjunction with CVE-2022-41973. Local users able to write to UNIX domain sockets can bypass access controls and manipulate the multipath setup. This can lead to local privilege escalation to root. This occurs because an attacker can repeat a keyword, which is mishandled because arithmetic ADD is used instead of bitwise OR.	7.8	More Details
CVE-2022-43281	wasm-interp v1.0.29 was discovered to contain a heap overflow via the component std::vector<wabt::Type, std::allocator<wabt::Type>>::size() at /bits/stl_vector.h.	7.8	More Details
CVE-2022-42827	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited..	7.8	More Details
CVE-2022-42796	This issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.7 and iPadOS 15.7, macOS Ventura 13. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2022-32794	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2022-32865	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42820	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may cause unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2022-3379	Horner Automation's Cscape version 9.90 SP7 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the current process by writing outside the memory buffer.	7.8	More Details
CVE-2022-3378	Horner Automation's Cscape version 9.90 SP 7 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the current process by accessing an uninitialized pointer, leading to an out-of-bounds memory write.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42809	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. Processing a maliciously crafted gcx file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2022-42801	A logic issue was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42800	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A user may be able to cause unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2022-43752	Oracle Solaris version 10 1/13, when using the Common Desktop Environment (CDE), is vulnerable to a privilege escalation vulnerability. A low privileged user can escalate to root by crafting a malicious printer and double clicking on the the crafted printer's icon.	7.8	More Details
CVE-2022-32898	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32914	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32899	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32903	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32905	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13. Processing a maliciously crafted DMG file may lead to arbitrary code execution with system privileges.	7.8	More Details
CVE-2022-32889	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32887	The issue was addressed with improved memory handling. This issue is fixed in iOS 16. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32866	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32947	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32907	This issue was addressed with improved checks. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32915	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32924	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26762	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2022-32939	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32940	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32944	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32932	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31256	A Improper Link Resolution Before File Access ('Link Following') vulnerability in a script called by the sendmail systemd service of openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: SUSE openSUSE Factory sendmail versions prior to 8.17.1-1.1.	7.7	More Details
CVE-2022-41680	Forma LMS on its 3.1.0 version and earlier is vulnerable to a SQL injection vulnerability. The exploitation of this vulnerability could allow an authenticated attacker (with the role of student) to perform a SQL injection on the 'search[value] parameter in the appLms/ajax.server.php?r=mycertificate/getMyCertificates' function in order to dump the entire database.	7.6	More Details
CVE-2022-39020	Multiple instances of XSS (stored and reflected) was found in the application. For example, features such as student assessment submission, file upload, news, ePortfolio and calendar event creation were found to be vulnerable to cross-site scripting.	7.6	More Details
CVE-2022-42924	Forma LMS on its 3.1.0 version and earlier is vulnerable to a SQL injection vulnerability. The exploitation of this vulnerability could allow an authenticated attacker (with the role of student) to perform a SQL injection on the 'dyn_filter' parameter in the 'appLms/ajax.adm_server.php?r=widget/userselector/getusertabledata' function in order to dump the entire database.	7.6	More Details
CVE-2022-43747	baramundi Management Agent (bMA) in baramundi Management Suite (bMS) 2021 R1 and R2 and 2022 R1 allows remote code execution. This is fixed in security update S-2022-01, which contains fixed bMA setup files for these versions. This also is fixed in baramundi Management Suite 2022 R2.	7.5	More Details
CVE-2022-32910	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5, Security Update 2022-005 Catalina. An archive may be able to bypass Gatekeeper.	7.5	More Details
CVE-2022-43284	Nginx NJS v0.7.2 to v0.7.4 was discovered to contain a segmentation violation via njs_scope_valid_value at njs_scope.h. NOTE: the vendor disputes the significance of this report because NJS does not operate on untrusted input.	7.5	More Details
CVE-2022-43285	Nginx NJS v0.7.4 was discovered to contain a segmentation violation in njs_promise_reaction_job. NOTE: the vendor disputes the significance of this report because NJS does not operate on untrusted input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42916	In curl before 7.86.0, the HSTS check could be bypassed to trick it into staying with HTTP. Using its HSTS support, curl can be instructed to use HTTPS directly (instead of using an insecure cleartext HTTP step) even when HTTP is provided in the URL. This mechanism could be bypassed if the host name in the given URL uses IDN characters that get replaced with ASCII counterparts as part of the IDN conversion, e.g., using the character UTF-8 U+3002 (IDEOGRAPHIC FULL STOP) instead of the common ASCII full stop of U+002E (.). The earliest affected version is 7.77.0 2021-05-26.	7.5	More Details
CVE-2022-39294	conduit-hyper integrates a conduit application with the hyper server. Prior to version 0.4.2, `conduit-hyper` did not check any limit on a request's length before calling [`hyper::body::to_bytes`](https://docs.rs/hyper/latest/hyper/body/fn.to_bytes.html). An attacker could send a malicious request with an abnormally large `Content-Length`, which could lead to a panic if memory allocation failed for that request. In version 0.4.2, `conduit-hyper` sets an internal limit of 128 MiB per request, otherwise returning status 400 ("Bad Request"). This crate is part of the implementation of Rust's crates.io, but that service is not affected due to its existing cloud infrastructure, which already drops such malicious requests. Even with the new limit in place, `conduit-hyper` is not recommended for production use, nor to directly serve the public Internet.	7.5	More Details
CVE-2022-3780	Database connections on deleted users could stay active on MySQL data sources in Remote Desktop Manager 2022.3.7 and below which allow deleted users to access unauthorized data. This issue affects : Remote Desktop Manager 2022.3.7 and prior versions.	7.5	More Details
CVE-2022-3786	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3602	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).	7.5	More Details
CVE-2022-40839	A SQL injection vulnerability in the height and width parameter in NdkAdvancedCustomizationFields v3.5.0 allows unauthenticated attackers to exfiltrate database data.	7.5	More Details
CVE-2022-43223	open5gs v2.4.11 was discovered to contain a memory leak in the component ngap-handler.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted UE attachment.	7.5	More Details
CVE-2022-43222	open5gs v2.4.11 was discovered to contain a memory leak in the component src/smf/pfcp-path.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PFCP packet.	7.5	More Details
CVE-2022-43221	open5gs v2.4.11 was discovered to contain a memory leak in the component src/upf/pfcp-path.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PFCP packet.	7.5	More Details
CVE-2022-40617	strongSwan before 5.9.8 allows remote attackers to cause a denial of service in the revocation plugin by sending a crafted end-entity (and intermediate CA) certificate that contains a CRL/OCSP URL that points to a server (under the attacker's control) that doesn't properly respond but (for example) just does nothing after the initial TCP handshake, or sends an excessive amount of application data.	7.5	More Details
CVE-2022-43081	Fast Food Ordering System v1.0 was discovered to contain a SQL injection vulnerability via the component /fastfood/purchase.php.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42252	If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.	7.5	More Details
CVE-2022-25892	The package muhammara before 2.6.1, from 3.0.0 and before 3.1.1; all versions of package hummus are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted PDF file to be parsed.	7.5	More Details
CVE-2022-25885	The package muhammara before 2.6.0; all versions of package hummus are vulnerable to Denial of Service (DoS) when PDFStreamForResponse() is used with invalid data.	7.5	More Details
CVE-2021-40661	A remote, unauthenticated, directory traversal vulnerability was identified within the web interface used by IND780 Advanced Weighing Terminals Build 8.0.07 March 19, 2018 (SS Label 'IND780_8.0.07'), Version 7.2.10 June 18, 2012 (SS Label 'IND780_7.2.10'). It was possible to traverse the folders of the affected host by providing a traversal path to the 'webpage' parameter in AutoCE.ini This could allow a remote unauthenticated adversary to access additional files on the affected system. This could also allow the adversary to perform further enumeration against the affected host to identify the versions of the systems in use, in order to launch further attacks in future.	7.5	More Details
CVE-2022-37620	A Regular Expression Denial of Service (ReDoS) flaw was found in kangax html-minifier 4.0.0 via the candidate variable in htmlminifier.js.	7.5	More Details
CVE-2022-40874	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow vulnerability in the GetParentControlInfo function, which can cause a denial of service attack through a carefully constructed http request.	7.5	More Details
CVE-2022-40875	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow in the function GetParentControlInfo.	7.5	More Details
CVE-2022-43364	An access control issue in the password reset page of IP-COM EW9 V15.11.0.14(9732) allows unauthenticated attackers to arbitrarily change the admin password.	7.5	More Details
CVE-2022-43365	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a buffer overflow in the formSetDebugCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43366	IP-COM EW9 V15.11.0.14(9732) allows unauthenticated attackers to access sensitive information via the checkLoginUser, ate, telnet, version, setDebugCfg, and boot interfaces.	7.5	More Details
CVE-2022-41776	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior allow unauthenticated users to trigger the WriteConfiguration method, which could allow an attacker to provide new values for user configuration files such as UserListInfo.xml. This could lead to the changing of administrative passwords.	7.5	More Details
CVE-2022-41629	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior allow unauthenticated users to access the aprunning endpoint, which could allow an attacker to retrieve any file from the “RunningConfigs” directory. The attacker could then view and modify configuration files such as UserListInfo.xml, which would allow them to see existing administrative passwords.	7.5	More Details
CVE-2022-38744	An unauthenticated attacker with network access to a victim's Rockwell Automation FactoryTalk Alarm and Events service could open a connection, causing the service to fault and become unavailable. The affected port could be used as a server ping port and uses messages structured with XML.	7.5	More Details
CVE-2021-38399	Honeywell Experion PKS C200, C200E, C300, and ACE controllers are vulnerable to relative path traversal, which may allow an attacker access to unauthorized files and directories.	7.5	More Details
CVE-2022-3697	A flaw was found in Ansible in the amazon.aws collection when using the tower_callback parameter from the amazon.aws.ec2_instance module. This flaw allows an attacker to take advantage of this issue as the module is handling the parameter insecurely, leading to the password leaking in the logs.	7.5	More Details
CVE-2022-42999	D-Link DIR-816 A2 1.10 B05 was discovered to contain multiple command injection vulnerabilities via the admuser and admpass parameters at /goform/setSysAdm.	7.5	More Details
CVE-2022-32927	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. Joining a malicious Wi-Fi network may result in a denial-of-service of the Settings app.	7.5	More Details
CVE-2022-43766	Apache IoTDB version 0.12.2 to 0.12.6, 0.13.0 to 0.13.2 are vulnerable to a Denial of Service attack when accepting untrusted patterns for REGEXP queries with Java 8. Users should upgrade to 0.13.3 which addresses this issue or use a later version of Java to avoid it.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3308	Insufficient policy enforcement in developer tools in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	7.4	More Details
CVE-2022-3666	A vulnerability, which was classified as critical, has been found in Axiomatic Bento4. Affected by this issue is the function AP4_LinearReader::Advance of the file Ap4LinearReader.cpp of the component mp42ts. The manipulation leads to use after free. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-212006 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-43990	Password recovery vulnerability in SICK SIM1012 Partnumber 1098146 with firmware version <2.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 2.2.0 as soon as possible (available in SICK Support Portal).	7.3	More Details
CVE-2022-3674	A vulnerability has been found in SourceCodester Sanitization Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to missing authentication. The attack can be launched remotely. The identifier VDB-212017 was assigned to this vulnerability.	7.3	More Details
CVE-2022-43989	Password recovery vulnerability in SICK SIM2x00 (ARM) Partnumber 1092673 and 1081902 with firmware version < 1.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.2.0 as soon as possible (available in SICK Support Portal).	7.3	More Details
CVE-2022-3670	A vulnerability was found in Axiomatic Bento4. It has been classified as critical. Affected is the function WriteSample of the component mp42hevc. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-212010 is the identifier assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3662	A vulnerability was found in Axiomatic Bento4. It has been declared as critical. This vulnerability affects the function GetOffset of the file Ap4Sample.h of the component mp42hls. The manipulation leads to use after free. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-212002 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-3664	A vulnerability classified as critical has been found in Axiomatic Bento4. Affected is the function AP4_BitStream::WriteBytes of the file Ap4BitStream.cpp of the component avcinfo. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212004.	7.3	More Details
CVE-2022-3665	A vulnerability classified as critical was found in Axiomatic Bento4. Affected by this vulnerability is an unknown functionality of the file AvcInfo.cpp of the component avcinfo. The manipulation leads to heap-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212005 was assigned to this vulnerability.	7.3	More Details
CVE-2022-3667	A vulnerability, which was classified as critical, was found in Axiomatic Bento4. This affects the function AP4_MemoryByteStream::WritePartial of the file Ap4ByteStream.cpp of the component mp42aac. The manipulation leads to heap-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212007.	7.3	More Details
CVE-2022-3366	The PublishPress Capabilities WordPress plugin before 2.5.2, PublishPress Capabilities Pro WordPress plugin before 2.5.2 unserializes the content of imported files, which could lead to PHP object injection attacks by administrators, on multisite WordPress configurations. Successful exploitation in this case requires other plugins with a suitable gadget chain to be present on the site.	7.2	More Details
CVE-2022-43232	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the userid parameter at /php_action/fetchOrderData.php.	7.2	More Details
CVE-2022-43275	Canteen Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via /youthappam/php_action/editProductImage.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43355	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-sms/classes/Master.php?f=delete_service.	7.2	More Details
CVE-2022-43276	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the productId parameter at /php_action/fetchSelectedfood.php.	7.2	More Details
CVE-2022-39978	Online Pet Shop We App v1.0 was discovered to contain an arbitrary file upload vulnerability via the Editing function in the Product List module. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file uploaded through the picture upload point.	7.2	More Details
CVE-2022-3380	The Customizer Export/Import WordPress plugin before 0.9.5 unserializes the content of an imported file, which could lead to PHP object injection issues when an admin imports (intentionally or not) a malicious file and a suitable gadget chain is present on the blog.	7.2	More Details
CVE-2022-43354	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/manage_request.	7.2	More Details
CVE-2022-43083	An arbitrary file upload vulnerability in admin-add-vehicle.php of Vehicle Booking System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-3374	The Ocean Extra WordPress plugin before 2.0.5 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import (intentionally or not) a malicious Customizer Styling file and a suitable gadget chain is present on the blog.	7.2	More Details
CVE-2022-39977	Online Pet Shop We App v1.0 was discovered to contain an arbitrary file upload vulnerability via the Editing function in the User module. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file uploaded through the picture upload point.	7.2	More Details
CVE-2022-3334	The Easy WP SMTP WordPress plugin before 1.5.0 unserialises the content of an imported file, which could lead to PHP object injection issue when an admin import (intentionally or not) a malicious file and a suitable gadget chain is present on the blog.	7.2	More Details
CVE-2022-43353	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/view_order.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43231	Canteen Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via /youthappam/manage_website.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-43085	An arbitrary file upload vulnerability in add_product.php of Restaurant POS System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-43329	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /print.php.	7.2	More Details
CVE-2022-43233	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the userid parameter at /php_action/fetchSelectedUser.php.	7.2	More Details
CVE-2022-43230	Simple Cold Storage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=bookings/view_details.	7.2	More Details
CVE-2022-43229	Simple Cold Storage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /bookings/update_status.php.	7.2	More Details
CVE-2022-43362	Senayan Library Management System v9.4.2 was discovered to contain a SQL injection vulnerability via the collType parameter at loan_by_class.php.	7.2	More Details
CVE-2022-43331	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php_action/printOrder.php.	7.2	More Details
CVE-2022-43228	Barangay Management System v1.0 was discovered to contain a SQL injection vulnerability via the hidden_id parameter at /clearance/clearance.php.	7.2	More Details
CVE-2022-43330	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /editorder.php.	7.2	More Details
CVE-2022-43124	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=user/manage_user.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43328	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /editorder.php.	7.2	More Details
CVE-2022-43127	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /appointments/update_status.php.	7.2	More Details
CVE-2022-43125	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /appointments/manage_appointment.php.	7.2	More Details
CVE-2022-43126	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/tests/manage_test.php.	7.2	More Details
CVE-2022-42327	x86: unintended memory sharing between guests On Intel systems that support the "virtualize APIC accesses" feature, a guest can read and write the global shared xAPIC page by moving the local APIC out of xAPIC mode. Access to this shared page bypasses the expected isolation that should exist between two guests.	7.1	More Details
CVE-2022-32925	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2022-43282	wasm-interp v1.0.29 was discovered to contain an out-of-bounds read via the component OnReturnCallIndirectExpr->GetReturnCallDropKeepCount.	7.1	More Details
CVE-2022-20822	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read and delete files on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains certain character sequences to an affected system. A successful exploit could allow the attacker to read or delete specific files on the device that their configured administrative level should not have access to. Cisco plans to release software updates that address this vulnerability.	7.1	More Details
CVE-2022-24670	An attacker can use the unrestricted LDAP queries to determine configuration entries	7.1	More Details
CVE-2022-43280	wasm-interp v1.0.29 was discovered to contain an out-of-bounds read via the component OnReturnCallExpr->GetReturnCallDropKeepCount.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42806	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.0	More Details
CVE-2022-42803	A race condition was addressed with improved locking. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges.	7.0	More Details
CVE-2022-42791	A race condition was addressed with improved state handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.0	More Details
CVE-2022-42320	Xenstore: Guests can get access to Xenstore nodes of deleted domains Access rights of Xenstore nodes are per domid. When a domain is gone, there might be Xenstore nodes left with access rights containing the domid of the removed domain. This is normally no problem, as those access right entries will be corrected when such a node is written later. There is a small time window when a new domain is created, where the access rights of a past domain with the same domid as the new one will be regarded to be still valid, leading to the new domain being able to get access to a node which was meant to be accessible by the removed domain. For this to happen another domain needs to write the node before the newly created domain is being introduced to Xenstore by dom0.	7.0	More Details
CVE-2022-31898	gl-inet GL-MT300N-V2 Mango v3.212 and GL-AX1800 Flint v3.214 were discovered to contain multiple command injection vulnerabilities via the ping_addr and trace_addr function parameters.	6.8	More Details
CVE-2022-3018	An information disclosure vulnerability in GitLab CE/EE affecting all versions starting from 9.3 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 allows a project maintainer to access the DataDog integration API key from webhook logs.	6.8	More Details
CVE-2022-32926	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2022-43750	drivers/usb/mon/mon_bin.c in usbmon in the Linux kernel before 5.19.15 and 6.x before 6.0.1 allows a user-space client to corrupt the monitor's internal memory.	6.7	More Details
CVE-2022-42830	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42829	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2022-3512	Using warp-cli command "add-trusted-ssid", a user was able to disconnect WARP client and bypass the "Lock WARP switch" feature resulting in Zero Trust policies not being enforced on an affected endpoint.	6.7	More Details
CVE-2022-3337	It was possible for a user to delete a VPN profile from WARP mobile client on iOS platform despite the Lock WARP switch https://developers.cloudflare.com/cloudflare-one/connections/connect-devices/warp/warp-settings/#lock-warp-switch feature being enabled on Zero Trust Platform. This led to bypassing policies and restrictions enforced for enrolled devices by the Zero Trust platform.	6.7	More Details
CVE-2022-3321	It was possible to bypass Lock WARP switch feature https://developers.cloudflare.com/cloudflare-one/connections/connect-devices/warp/warp-settings/#lock-warp-switch on the WARP iOS mobile client by enabling both "Disable for cellular networks" and "Disable for Wi-Fi networks" switches at once in the application settings. Such configuration caused the WARP client to disconnect and allowed the user to bypass restrictions and policies enforced by the Zero Trust platform.	6.7	More Details
CVE-2022-3320	It was possible to bypass policies configured for Zero Trust Secure Web Gateway by using warp-cli 'set-custom-endpoint' subcommand. Using this command with an unreachable endpoint caused the WARP Client to disconnect and allowed bypassing administrative restrictions on a Zero Trust enrolled endpoint.	6.7	More Details
CVE-2022-3322	Lock Warp switch is a feature of Zero Trust platform which, when enabled, prevents users of enrolled devices from disabling WARP client. Due to insufficient policy verification by WARP iOS client, this feature could be bypassed by using the "Disable WARP" quick action.	6.7	More Details
CVE-2022-3191	Insertion of Sensitive Information into Log File vulnerability in Hitachi Ops Center Analyzer on Linux (Virtual Strage Software Agent component) allows local users to gain sensitive information. This issue affects Hitachi Ops Center Analyzer: from 10.8.1-00 before 10.9.0-00	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36605	Incorrect Default Permissions vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Analytics probe component), Hitachi Ops Center Analyzer on Linux (Analyzer probe component), Hitachi Ops Center Viewpoint on Linux (Viewpoint RAID Agent component) allows local users to read and write specific files. This issue affects Hitachi Infrastructure Analytics Advisor: from 2.0.0-00 through 4.4.0-00; Hitachi Ops Center Analyzer: from 10.0.0-00 before 10.9.0-00; Hitachi Ops Center Viewpoint: from 10.8.0-00 before 10.9.0-00.	6.6	More Details
CVE-2022-39023	U-Office Force Download function has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to download arbitrary system file.	6.5	More Details
CVE-2022-22658	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 16.0.3. Processing a maliciously crafted email message may lead to a denial-of-service.	6.5	More Details
CVE-2022-3400	The Bricks theme for WordPress is vulnerable to authorization bypass due to a missing capability check on the bricks_save_post AJAX action in versions 1.0 to 1.5.3. This makes it possible for authenticated attackers with minimal permissions, such as a subscriber, to edit any page, post, or template on the vulnerable WordPress website.	6.5	More Details
CVE-2022-32923	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app.	6.5	More Details
CVE-2022-3228	Using custom code, an attacker can write into name or description fields larger than the appropriate buffer size causing a stack-based buffer overflow on Host Engineering H0-ECOM100 Communications Module Firmware versions v5.0.155 and prior. This may allow an attacker to crash the affected device or cause it to become unresponsive.	6.5	More Details
CVE-2022-42321	Xenstore: Guests can crash xenstored via exhausting the stack Xenstored is using recursion for some Xenstore operations (e.g. for deleting a sub-tree of Xenstore nodes). With sufficiently deep nesting levels this can result in stack exhaustion on xenstored, leading to a crash of xenstored.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42319	Xenstore: Guests can cause Xenstore to not free temporary memory When working on a request of a guest, xenstored might need to allocate quite large amounts of memory temporarily. This memory is freed only after the request has been finished completely. A request is regarded to be finished only after the guest has read the response message of the request from the ring page. Thus a guest not reading the response can cause xenstored to not free the temporary memory. This can result in memory shortages causing Denial of Service (DoS) of xenstored.	6.5	More Details
CVE-2022-42318	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-40488	ProcessWire v3.0.200 was discovered to contain a Cross-Site Request Forgery (CSRF).	6.5	More Details
CVE-2022-42317	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42311	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-3781	Dashlane password and Keepass Server password in My Account Settings are not encrypted in the database in Devolutions Remote Desktop Manager 2022.2.26 and prior versions and Devolutions Server 2022.3.1 and prior versions which allows database users to read the data. This issue affects : Remote Desktop Manager 2022.2.26 and prior versions. Devolutions Server 2022.3.1 and prior versions.	6.5	More Details
CVE-2022-42316	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-41553	Insertion of Sensitive Information into Temporary File vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Analytics probe component), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer probe component) allows local users to gain sensitive information. This issue affects Hitachi Infrastructure Analytics Advisor: from 2.0.0-00 through 4.4.0-00; Hitachi Ops Center Analyzer: from 10.0.0-00 before 10.9.0-00.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42315	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-40742	Mail SQR Expert system has a Local File Inclusion vulnerability. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary PHP file with .asp file extension under specific system paths, to access and modify partial system information but does not affect service availability.	6.5	More Details
CVE-2022-42314	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-24669	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42313	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-42055	Multiple command injection vulnerabilities in GL.iNet GoodCloud IoT Device Management System Version 1.00.220412.00 via the ping and traceroute tools allow attackers to read arbitrary files on the system.	6.5	More Details
CVE-2022-39360	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login.	6.5	More Details
CVE-2022-34662	When users add resources to the resource center with a relation path will cause path traversal issues and only for logged-in users. You could upgrade to version 3.0.0 or higher	6.5	More Details
CVE-2022-26884	Users can read any files by log server, Apache DolphinScheduler users should upgrade to version 2.0.6 or higher.	6.5	More Details
CVE-2022-39022	U-Office Force Download function has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to download arbitrary system file.	6.5	More Details
CVE-2022-42817	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. Visiting a maliciously crafted website may leak sensitive data.	6.5	More Details
CVE-2022-37424	Files or Directories Accessible to External Parties vulnerability in OpenNebula on Linux allows File Discovery.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3419	The Automatic User Roles Switcher WordPress plugin before 1.1.2 does not have authorisation and proper CSRF checks, allowing any authenticated users like subscriber to add any role to themselves, such as administrator	6.5	More Details
CVE-2022-43776	The url parameter of the /api/geojson endpoint in Metabase versions <44.5 can be used to perform Server Side Request Forgery attacks. Previously implemented blacklists could be circumvented by leveraging 301 and 302 redirects.	6.5	More Details
CVE-2022-3499	An authenticated attacker could utilize the identical agent and cluster node linking keys to potentially allow for a scenario where unauthorized disclosure of agent logs and data is present.	6.5	More Details
CVE-2022-3387	Advantech R-SeeNet Versions 2.4.19 and prior are vulnerable to path traversal attacks. An unauthorized attacker could remotely exploit vulnerable PHP code to delete .PDF files.	6.5	More Details
CVE-2022-39359	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default).	6.5	More Details
CVE-2022-39358	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was possible to circumvent locked parameters when requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6.	6.5	More Details
CVE-2022-3314	Use after free in logging in Google Chrome prior to 106.0.5249.62 allowed a remote attacker who had compromised a WebUI process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-3313	Incorrect security UI in full screen in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-3311	Use after free in import in Google Chrome prior to 106.0.5249.62 allowed a remote attacker who had compromised a WebUI process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3310	Insufficient policy enforcement in custom tabs in Google Chrome on Android prior to 106.0.5249.62 allowed an attacker who convinced the user to install an application to bypass same origin policy via a crafted application. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-3309	Use after free in assistant in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via specific UI gestures. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-42312	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction	6.5	More Details
CVE-2022-44032	An issue was discovered in the Linux kernel through 6.0.6. drivers/char/pcmcia/cm4000_cs.c has a race condition and resultant use-after-free if a physically proximate attacker removes a PCMCIA device while calling open(), aka a race condition between cmm_open() and cm4000_detach().	6.4	More Details
CVE-2022-44033	An issue was discovered in the Linux kernel through 6.0.6. drivers/char/pcmcia/cm4040_cs.c has a race condition and resultant use-after-free if a physically proximate attacker removes a PCMCIA device while calling open(), aka a race condition between cm4040_open() and reader_detach().	6.4	More Details
CVE-2022-44034	An issue was discovered in the Linux kernel through 6.0.6. drivers/char/pcmcia/scr24x_cs.c has a race condition and resultant use-after-free if a physically proximate attacker removes a PCMCIA device while calling open(), aka a race condition between scr24x_open() and scr24x_remove().	6.4	More Details
CVE-2022-42831	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42832	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.4	More Details
CVE-2022-3730	A vulnerability, which was classified as critical, was found in seccome Ehoney. Affected is an unknown function of the file /api/v1/attack/falco. The manipulation of the argument Payload leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-212412.	6.3	More Details
CVE-2022-3800	A vulnerability, which was classified as critical, has been found in IBAX go-ibax. Affected by this issue is some unknown functionality of the file /api/v2/open/rowsInfo. The manipulation of the argument table_name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212636.	6.3	More Details
CVE-2022-3799	A vulnerability classified as critical was found in IBAX go-ibax. Affected by this vulnerability is an unknown functionality of the file /api/v2/open/tablesInfo. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212635.	6.3	More Details
CVE-2022-3798	A vulnerability classified as critical has been found in IBAX go-ibax. Affected is an unknown function of the file /api/v2/open/tablesInfo. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-212634 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3797	A vulnerability was found in eolinker apinto-dashboard. It has been rated as problematic. This issue affects some unknown processing of the file /login. The manipulation of the argument callback leads to open redirect. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212633 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3770	A vulnerability classified as critical was found in Yunjing CMS. This vulnerability affects unknown code of the file /index/user/upload_img.html. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212500.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3801	A vulnerability, which was classified as critical, was found in IBAX go-ibax. This affects an unknown part of the file /api/v2/open/rowsInfo. The manipulation of the argument order leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212637 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3771	A vulnerability, which was classified as critical, has been found in easyii CMS. This issue affects the function file of the file helpers/Upload.php of the component File Upload Management. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The identifier VDB-212501 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3671	A vulnerability classified as critical was found in SourceCodester eLearning System 1.0. This vulnerability affects unknown code of the file /admin/students/manage.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-212014 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3729	A vulnerability, which was classified as critical, has been found in seccome Ehoney. This issue affects some unknown processing of the file /api/v1/attack. The manipulation of the argument AttackIP leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-212411.	6.3	More Details
CVE-2022-39019	Broken access controls on PDFtron WebviewerUI in M-Files Hubshare before 3.3.11.3 allows unauthenticated attackers to upload malicious files to the application server.	6.3	More Details
CVE-2022-3784	A vulnerability classified as critical was found in Axiomatic Bento4 5e7bb34. Affected by this vulnerability is the function AP4_Mp4AudioDsiParser::ReadBits of the file Ap4Mp4AudioInfo.cpp of the component mp4hls. The manipulation leads to heap-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212563.	6.3	More Details
CVE-2022-3802	A vulnerability has been found in IBAX go-ibax and classified as critical. This vulnerability affects unknown code of the file /api/v2/open/rowsInfo. The manipulation of the argument where leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-212638 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3735	A vulnerability was found in seccome Ehoney. It has been rated as critical. This issue affects some unknown processing of the file /api/public/signup. The manipulation leads to improper access controls. The identifier VDB-212417 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3785	A vulnerability, which was classified as critical, has been found in Axiomatic Bento4. Affected by this issue is the function AP4_DataBuffer::SetDataSize of the component Avcinfo. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212564.	6.3	More Details
CVE-2022-3734	A vulnerability was found in a port or fork of Redis. It has been declared as critical. This vulnerability affects unknown code in the library C:/Program Files/Redis/dbghelp.dll. The manipulation leads to uncontrolled search path. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier of this vulnerability is VDB-212416. NOTE: The official Redis release is not affected. This issue might affect an unofficial fork or port on Windows only.	6.3	More Details
CVE-2022-3732	A vulnerability was found in seccome Ehoney and classified as critical. Affected by this issue is some unknown functionality of the file /api/v1/bait/set. The manipulation of the argument Payload leads to sql injection. The attack may be launched remotely. VDB-212414 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3731	A vulnerability has been found in seccome Ehoney and classified as critical. Affected by this vulnerability is an unknown functionality of the file /api/v1/attack/token. The manipulation of the argument Payload leads to sql injection. The attack can be launched remotely. The identifier VDB-212413 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3725	Crash in the OPUS protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2022-36182	Hashicorp Boundary v0.8.0 is vulnerable to Clickjacking which allow for the interception of login credentials, re-direction of users to malicious sites, or causing users to perform malicious actions on the site.	6.1	More Details
CVE-2022-39024	U-Office Force Bulletin function has insufficient filtering for special characters. An unauthenticated remote attacker can exploit this vulnerability to inject JavaScript and perform XSS (Reflected Cross-Site Scripting) attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3402	The Log HTTP Requests plugin for WordPress is vulnerable to Stored Cross-Site Scripting via logged HTTP requests in versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers who can trick a site's administrator into performing an action like clicking on a link, or an authenticated user with access to a page that sends a request using user-supplied data via the server, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2022-42799	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website may lead to user interface spoofing.	6.1	More Details
CVE-2021-38728	SEMCMS SHOP v 1.1 is vulnerable to Cross Site Scripting (XSS) via Ant_M_Coup.php.	6.1	More Details
CVE-2022-39021	U-Office Force login function has an Open Redirect vulnerability. An unauthenticated remote attacker can exploit this vulnerability to redirect user to arbitrary website.	6.1	More Details
CVE-2022-20959	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-43082	A cross-site scripting (XSS) vulnerability in /fastfood/purchase.php of Fast Food Ordering System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the customer parameter.	6.1	More Details
CVE-2022-3440	The Rock Convert WordPress plugin before 2.11.0 does not sanitise and escape an URL before outputting it back in an attribute when a specific widget is present on a page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-43079	A cross-site scripting (XSS) vulnerability in /admin/add-fee.php of Train Scheduler App v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40487	ProcessWire v3.0.200 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via the Search Users and Search Pages function. These vulnerabilities allow attackers to execute arbitrary web scripts or HTML via injection of a crafted payload.	6.1	More Details
CVE-2022-32407	Softr v2.0 was discovered to contain a Cross-Site Scripting (XSS) vulnerability via the First Name parameter under the Create A New Account module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2022-3766	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.8.	6.1	More Details
CVE-2022-40290	The application was vulnerable to an unauthenticated Reflected Cross-Site Scripting (XSS) vulnerability in the barcode generation functionality, allowing attackers to generate an unsafe link that could compromise users.	6.1	More Details
CVE-2022-2627	The Newspaper WordPress theme before 12 does not sanitise a parameter before outputting it back in an HTML attribute via an AJAX action, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-2190	The Gallery Plugin for WordPress plugin before 1.8.4.7 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	6.1	More Details
CVE-2022-2167	The Newspaper WordPress theme before 12 does not sanitise a parameter before outputting it back in an HTML attribute via an AJAX action, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-39025	U-Office Force PrintMessage function has insufficient filtering for special characters. An unauthenticated remote attacker can exploit this vulnerability to inject JavaScript and perform XSS (Reflected Cross-Site Scripting) attack.	6.1	More Details
CVE-2020-4099	The application was signed using a key length less than or equal to 1024 bits, making it potentially vulnerable to forged digital signatures. An attacker could forge the same digital signature of the app after maliciously modifying the app.	5.9	More Details
CVE-2022-42818	This issue was addressed with improved data protection. This issue is fixed in macOS Ventura 13. A user in a privileged network position may be able to track user activity.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27784	The provided HCL Launch Container images contain non-unique HTTPS certificates and a database encryption key. The fix provides directions and tools to replace the non-unique keys and certificates. This does not affect the standard installer packages.	5.9	More Details
CVE-2022-40183	An error in the URL handler of the VIDEOJET multi 4000 may lead to a reflected cross site scripting (XSS) in the web-based interface. An attacker with knowledge of the encoder address can send a crafted link to a user, which will execute JavaScript code in the context of the user.	5.8	More Details
CVE-2022-43748	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in file operation management in Synology Presto File Server before 2.1.2-1601 allows remote attackers to write arbitrary files via unspecified vectors.	5.8	More Details
CVE-2022-0072	Directory Traversal vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server and LiteSpeed Web Server dashboards allows Path Traversal. This affects versions from 1.5.11 through 1.5.12, from 1.6.5 through 1.6.20.1, from 1.7.0 before 1.7.16.1	5.8	More Details
CVE-2022-23738	An improper cache key vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to access private repository files through a public repository. To exploit this, an actor would need to already be authorized on the GitHub Enterprise Server instance, be able to create a public repository, and have a site administrator visit a specially crafted URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program.	5.7	More Details
CVE-2022-42790	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. A user may be able to view restricted content from the lock screen.	5.5	More Details
CVE-2022-43148	rtf2html v0.2.0 was discovered to contain a heap overflow in the component /rtf2html/./rtf_tools.h.	5.5	More Details
CVE-2022-42819	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to read sensitive location information.	5.5	More Details
CVE-2022-32858	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. An app may be able to leak sensitive kernel state.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42789	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2022-32946	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to record audio using a pair of connected AirPods.	5.5	More Details
CVE-2022-32827	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2022-32862	This issue was addressed with improved data protection. This issue is fixed in macOS Big Sur 11.7.1, macOS Ventura 13, macOS Monterey 12.6.1. An app with root privileges may be able to access private information.	5.5	More Details
CVE-2022-42815	This issue was addressed with improved data protection. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2022-32904	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2022-32918	This issue was addressed with improved data protection. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2022-42798	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing a maliciously crafted audio file may lead to disclosure of user information.	5.5	More Details
CVE-2022-44081	Lodepng v20220717 was discovered to contain a segmentation fault via the function pngdetail.	5.5	More Details
CVE-2022-32929	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 15.7 and iPadOS 15.7, iOS 16.1 and iPadOS 16. An app may be able to access iOS backups.	5.5	More Details
CVE-2022-32909	The issue was addressed with improved handling of caches. This issue is fixed in iOS 16. An app may be able to access user-sensitive data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44079	pycdc commit 44a730f3a889503014fec94ae6e62d8401cb75e5 was discovered to contain a stack overflow via the component __sanitizer::StackDepotBase<__sanitizer::StackDepotNode.	5.5	More Details
CVE-2022-32936	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-42824	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information.	5.5	More Details
CVE-2022-43152	tsMuxer v2.6.16 was discovered to contain a heap overflow via the function BitStreamWriter::flushBits() at /tsMuxer/bitStream.h.	5.5	More Details
CVE-2022-43151	timg v1.4.4 was discovered to contain a memory leak via the function timg::QueryBackgroundColor() at /timg/src/term-query.cc.	5.5	More Details
CVE-2022-42810	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2022-32881	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2022-42811	An access issue was addressed with additional sandbox restrictions. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2022-32877	A configuration issue was addressed with additional restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Monterey 12.6. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2022-42814	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2022-42793	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. An app may be able to bypass code signing checks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42324	Oxenstored 32->31 bit integer truncation issues Integers in Ocaml are 63 or 31 bits of signed precision. The Ocaml Xenbus library takes a C uint32_t out of the ring and casts it directly to an Ocaml integer. In 64-bit Ocaml builds this is fine, but in 32-bit builds, it truncates off the most significant bit, and then creates unsigned/signed confusion in the remainder. This in turn can feed a negative value into logic not expecting a negative value, resulting in unexpected exceptions being thrown. The unexpected exception is not handled suitably, creating a busy-loop trying (and failing) to take the bad packet out of the xenstore ring.	5.5	More Details
CVE-2022-3789	A vulnerability has been found in Tim Campus Confession Wall and classified as critical. Affected by this vulnerability is an unknown functionality of the file share.php. The manipulation of the argument post_id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212611.	5.5	More Details
CVE-2022-42323	Xenstore: Cooperating guests can create arbitrary numbers of nodes T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Since the fix of XSA-322 any Xenstore node owned by a removed domain will be modified to be owned by Dom0. This will allow two malicious guests working together to create an arbitrary number of Xenstore nodes. This is possible by domain A letting domain B write into domain A's local Xenstore tree. Domain B can then create many nodes and reboot. The nodes created by domain B will now be owned by Dom0. By repeating this process over and over again an arbitrary number of nodes can be created, as Dom0's number of nodes isn't limited by Xenstore quota.	5.5	More Details
CVE-2022-42322	Xenstore: Cooperating guests can create arbitrary numbers of nodes T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Since the fix of XSA-322 any Xenstore node owned by a removed domain will be modified to be owned by Dom0. This will allow two malicious guests working together to create an arbitrary number of Xenstore nodes. This is possible by domain A letting domain B write into domain A's local Xenstore tree. Domain B can then create many nodes and reboot. The nodes created by domain B will now be owned by Dom0. By repeating this process over and over again an arbitrary number of nodes can be created, as Dom0's number of nodes isn't limited by Xenstore quota.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42326	Xenstore: Guests can create arbitrary number of nodes via transactions T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] In case a node has been created in a transaction and it is later deleted in the same transaction, the transaction will be terminated with an error. As this error is encountered only when handling the deleted node at transaction finalization, the transaction will have been performed partially and without updating the accounting information. This will enable a malicious guest to create arbitrary number of nodes.	5.5	More Details
CVE-2022-44020	An issue was discovered in OpenStack Sushy-Tools through 0.21.0 and VirtualBMC through 2.2.2. Changing the boot device configuration with these packages removes password protection from the managed libvirt XML domain. NOTE: this only affects an "unsupported, production-like configuration."	5.5	More Details
CVE-2022-42310	Xenstore: Guests can create orphaned Xenstore nodes By creating multiple nodes inside a transaction resulting in an error, a malicious guest can create orphaned nodes in the Xenstore data base, as the cleanup after the error will not remove all nodes already created. When the transaction is committed after this situation, nodes without a valid parent can be made permanent in the data base.	5.5	More Details
CVE-2022-20954	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-42788	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in macOS Ventura 13. A malicious application may be able to read sensitive location information.	5.5	More Details
CVE-2022-20953	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-20811	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20776	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-2882	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A malicious maintainer could exfiltrate a GitHub integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server.	5.5	More Details
CVE-2022-43283	wasm2c v1.0.29 was discovered to contain an abort in CWriter::Write.	5.5	More Details
CVE-2022-20955	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-42825	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2022-42325	Xenstore: Guests can create arbitrary number of nodes via transactions T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] In case a node has been created in a transaction and it is later deleted in the same transaction, the transaction will be terminated with an error. As this error is encountered only when handling the deleted node at transaction finalization, the transaction will have been performed partially and without updating the accounting information. This will enable a malicious guest to create arbitrary number of nodes.	5.5	More Details
CVE-2022-3096	The WP Total Hacks WordPress plugin through 4.7.2 does not prevent low privilege users from modifying the plugin's settings. This could allow users such as subscribers to perform Stored Cross-Site Scripting attacks against other users, like administrators, due to the lack of sanitisation and escaping as well.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25849	The package joyqi/hyper-down from 0.0.0 are vulnerable to Cross-site Scripting (XSS) because the module of parse markdown does not filter the href attribute very well.	5.4	More Details
CVE-2022-42054	Multiple stored cross-site scripting (XSS) vulnerabilities in GL.iNet GoodCloud IoT Device Management System Version 1.00.220412.00 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Company Name and Description text fields.	5.4	More Details
CVE-2022-39348	Twisted is an event-based framework for internet applications. Started with version 0.9.4, when the host header does not match a configured host `twisted.web.vhost.NameVirtualHost` will return a `NoResource` resource which renders the Host header unescaped into the 404 response allowing HTML and script injection. In practice this should be very difficult to exploit as being able to modify the Host header of a normal HTTP request implies that one is already in a privileged position. This issue was fixed in version 22.10.0rc1. There are no known workarounds.	5.4	More Details
CVE-2022-43169	A stored cross-site scripting (XSS) vulnerability in the Users Access Groups feature (/index.php?module=users_groups/users_groups) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter after clicking "Add New Group".	5.4	More Details
CVE-2022-43167	A stored cross-site scripting (XSS) vulnerability in the Users Alerts feature (/index.php?module=users_alerts/users_alerts) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title parameter after clicking "Add".	5.4	More Details
CVE-2022-43166	A stored cross-site scripting (XSS) vulnerability in the Global Entities feature (/index.php?module=entities/entities) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter after clicking "Add New Entity".	5.4	More Details
CVE-2022-31777	A stored cross-site scripting (XSS) vulnerability in Apache Spark 3.2.1 and earlier, and 3.3.0, allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the logs which would be returned in logs rendered in the UI.	5.4	More Details
CVE-2022-42993	Password Storage Application v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Setup page.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40739	Ragic report generation page has insufficient filtering for special characters. A remote attacker with general user privilege can inject JavaScript to perform XSS (Reflected Cross-Site Scripting) attack.	5.4	More Details
CVE-2022-43165	A stored cross-site scripting (XSS) vulnerability in the Global Variables feature (/index.php?module=global_vars/vars) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Value parameter after clicking "Create".	5.4	More Details
CVE-2022-42992	Multiple stored cross-site scripting (XSS) vulnerabilities in Train Scheduler App v1.0 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Train Code, Train Name, and Destination text fields.	5.4	More Details
CVE-2021-36863	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ExpressTech Quiz And Survey Master plugin <= 7.3.4 on WordPress.	5.4	More Details
CVE-2022-3616	Attackers can create long chains of CAs that would lead to OctoRPKI exceeding its max iterations parameter. In consequence it would cause the program to crash, preventing it from finishing the validation and leading to a denial of service. Credits to Donika Mirdita and Haya Shulman - Fraunhofer SIT, ATHENE, who discovered and reported this vulnerability.	5.4	More Details
CVE-2022-3774	A vulnerability was found in SourceCodester Train Scheduler App 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /train_scheduler_app/?action=delete. The manipulation of the argument id leads to improper control of resource identifiers. The attack may be launched remotely. The identifier of this vulnerability is VDB-212504.	5.4	More Details
CVE-2021-37781	Employee Record Management System v 1.2 is vulnerable to Cross Site Scripting (XSS) via editempprofile.php.	5.4	More Details
CVE-2022-3765	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.8.	5.4	More Details
CVE-2022-42991	A stored cross-site scripting (XSS) vulnerability in Simple Online Public Access Catalog v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Edit Account Full Name field.	5.4	More Details
CVE-2021-35388	Hospital Management System v 4.0 is vulnerable to Cross Site Scripting (XSS) via /hospital/hms/admin/patient-search.php.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39027	U-Office Force Forum function has insufficient filtering for special characters. A remote attacker with general user privilege can inject JavaScript and perform XSS (Stored Cross-Site Scripting) attack.	5.4	More Details
CVE-2022-39026	U-Office Force UserDefault page has insufficient filtering for special characters in the HTTP header fields. A remote attacker with general user privilege can exploit this vulnerability to inject JavaScript and perform XSS (Stored Cross-Site Scripting) attack.	5.4	More Details
CVE-2022-43170	A stored cross-site scripting (XSS) vulnerability in the Dashboard Configuration feature (index.php?module=dashboard_configure/index) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title parameter after clicking "Add info block".	5.4	More Details
CVE-2022-43164	A stored cross-site scripting (XSS) vulnerability in the Global Lists feature (/index.php?module=global_lists/lists) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter after clicking "Add".	5.4	More Details
CVE-2022-3663	A vulnerability was found in Axiomatic Bento4. It has been rated as problematic. This issue affects the function AP4_StsdAtom of the file Ap4StsdAtom.cpp of the component MP4fragment. The manipulation leads to null pointer dereference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212003.	5.3	More Details
CVE-2022-32928	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user in a privileged network position may be able to intercept mail credentials.	5.3	More Details
CVE-2022-32938	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. A shortcut may be able to check the existence of an arbitrary path on the file system.	5.3	More Details
CVE-2022-3668	A vulnerability has been found in Axiomatic Bento4 and classified as problematic. This vulnerability affects the function AP4_AtomFactory::CreateAtomFromStream of the component mp4edit. The manipulation leads to memory leak. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212008.	5.3	More Details
CVE-2022-40292	The application allowed for Unauthenticated User Enumeration by interacting with an unsecured endpoint to retrieve information on each account within the system.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45475	Yordam Library Information Document Automation product before version 19.02 has an unauthenticated Information disclosure vulnerability.	5.3	More Details
CVE-2022-25918	The package shescape from 1.5.10 and before 1.6.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the escape function in index.js, due to the usage of insecure regex in the escapeArgBash function.	5.3	More Details
CVE-2022-2508	In affected versions of Octopus Server it is possible to reveal the existence of resources in a space that the user does not have access to due to verbose error messaging.	5.3	More Details
CVE-2022-3669	A vulnerability was found in Axiomatic Bento4 and classified as problematic. This issue affects the function AP4_AvccAtom::Create of the component mp4edit. The manipulation leads to memory leak. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212009 was assigned to this vulnerability.	5.3	More Details
CVE-2022-32859	A logic issue was addressed with improved state management. This issue is fixed in iOS 16. Deleted contacts may still appear in spotlight search results.	5.3	More Details
CVE-2022-44023	PwnDoc through 0.5.3 might allow remote attackers to identify disabled user account names by leveraging response messages for authentication attempts.	5.3	More Details
CVE-2022-44022	PwnDoc through 0.5.3 might allow remote attackers to identify valid user account names by leveraging response timings for authentication attempts.	5.3	More Details
CVE-2022-40703	CWE-302 Authentication Bypass by Assumed-Immutable Data in AliveCor Kardia App version 5.17.1-754993421 and prior on Android allows an unauthenticated attacker with physical access to the Android device containing the app to bypass application authentication and alter information in the app.	5.2	More Details
CVE-2022-40184	Incomplete filtering of JavaScript code in different configuration fields of the web based interface of the VIDEOJET multi 4000 allows an attacker with administrative credentials to store JavaScript code which will be executed for all administrators accessing the same configuration option.	5.1	More Details
CVE-2022-32875	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6. An app may be able to read sensitive location information.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3733	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been classified as critical. This affects an unknown part of the file Admin/edit-admin.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212415.	5.0	More Details
CVE-2022-3705	A vulnerability was found in vim and classified as problematic. Affected by this issue is the function qf_update_buffer of the file quickfix.c of the component autocmd Handler. The manipulation leads to use after free. The attack may be launched remotely. Upgrading to version 9.0.0805 is able to address this issue. The name of the patch is d0fab10ed2a86698937e3c3fed2f10bd9bb5e731. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-212324.	5.0	More Details
CVE-2022-3714	A vulnerability classified as critical has been found in SourceCodester Online Medicine Ordering System 1.0. Affected is an unknown function of the file admin/?page=orders/view_order. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. VDB-212346 is the identifier assigned to this vulnerability.	5.0	More Details
CVE-2022-43086	Restaurant POS System v1.0 was discovered to contain a SQL injection vulnerability via update_customer.php.	4.9	More Details
CVE-2022-40295	The application was vulnerable to an authenticated information disclosure, allowing administrators to view unsalted user passwords, which could lead to the compromise of plaintext passwords via offline attacks.	4.9	More Details
CVE-2022-41627	The physical IoT device of the AliveCor's KardiaMobile, a smartphone-based personal electrocardiogram (EKG) has no encryption for its data-over-sound protocols. Exploiting this vulnerability could allow an attacker to read patient EKG results or create a denial-of-service condition by emitting sounds at similar frequencies as the device, disrupting the smartphone microphone’s ability to accurately read the data. To carry out this attack, the attacker must be close (less than 5 feet) to pick up and emit sound waves.	4.8	More Details
CVE-2021-36858	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themepoints Testimonials plugin <= 2.6 on WordPress.	4.8	More Details
CVE-2022-3420	The Official Integration for Billingo WordPress plugin before 3.4.0 does not sanitise and escape some of its settings, which could allow high privilege users with a role as low as Shop Manager to perform Stored Cross-Site Scripting attacks.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3408	The WP Word Count WordPress plugin through 3.2.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2022-3237	The WP Contact Slider WordPress plugin before 2.4.8 does not sanitize and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-43078	A cross-site scripting (XSS) vulnerability in /admin/add-fee.php of Web-Based Student Clearance System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter.	4.8	More Details
CVE-2022-39330	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server prior to versions 23.0.10 and 24.0.6 and Nextcloud Enterprise Server prior to versions 22.2.10, 23.0.10, and 24.0.6 are vulnerable to a logged-in attacker slowing down the system by generating a lot of database/cpu load. Nextcloud Server versions 23.0.10 and 24.0.6 and Nextcloud Enterprise Server versions 22.2.10, 23.0.10, and 24.0.6 contain patches for this issue. As a workaround, disable the Circles app.	4.8	More Details
CVE-2022-43084	A cross-site scripting (XSS) vulnerability in admin-add-vehicle.php of Vehicle Booking System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the v_name parameter.	4.8	More Details
CVE-2022-43361	Senayan Library Management System v9.4.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the component pop_chart.php.	4.8	More Details
CVE-2022-3441	The Rock Convert WordPress plugin before 2.11.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-43076	A cross-site scripting (XSS) vulnerability in /admin/edit-admin.php of Web-Based Student Clearance System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtemail parameter.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41679	Forma LMS version 3.1.0 and earlier are affected by an Cross-Site scripting vulnerability, that could allow a remote attacker to inject javascript code on the “back_url” parameter in appLms/index.php?modname=faq&op=play function. The exploitation of this vulnerability could allow an attacker to steal the user´s cookies in order to log in to the application.	4.7	More Details
CVE-2021-45476	Yordam Library Information Document Automation product before version 19.02 has an unauthenticated reflected XSS vulnerability.	4.7	More Details
CVE-2022-32895	A race condition was addressed with improved state handling. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system.	4.7	More Details
CVE-2022-32935	A lock screen issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. A user may be able to view restricted content from the lock screen.	4.6	More Details
CVE-2022-3312	Insufficient validation of untrusted input in VPN in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a local attacker to bypass managed device restrictions via physical access to the device. (Chromium security severity: Medium)	4.6	More Details
CVE-2022-3474	A bad credential handling in the remote assets API for Bazel versions prior to 5.3.2 and 4.2.3 sends all user-provided credentials instead of only the required ones for the requests. We recommend upgrading to versions later than or equal to 5.3.2 or 4.2.3.	4.3	More Details
CVE-2022-3443	Insufficient data validation in File System API in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass File System restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2022-3661	Insufficient data validation in Extensions in Google Chrome prior to 107.0.5304.62 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted Chrome extension. (Chromium security severity: Low)	4.3	More Details
CVE-2022-3660	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 107.0.5304.62 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2022-3316	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass security feature via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43749	Improper privilege management vulnerability in summary report management in Synology Presto File Server before 2.1.2-1601 allows remote authenticated users to bypass security constraint via unspecified vectors.	4.3	More Details
CVE-2022-3817	A vulnerability has been found in Axiomatic Bento4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component mp4mux. The manipulation leads to memory leak. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212683.	4.3	More Details
CVE-2022-3816	A vulnerability, which was classified as problematic, was found in Axiomatic Bento4. Affected is an unknown function of the component mp4decrypt. The manipulation leads to memory leak. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-212682 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-3815	A vulnerability, which was classified as problematic, has been found in Axiomatic Bento4. This issue affects some unknown processing of the component mp4decrypt. The manipulation leads to memory leak. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212681 was assigned to this vulnerability.	4.3	More Details
CVE-2022-3814	A vulnerability classified as problematic was found in Axiomatic Bento4. This vulnerability affects unknown code of the component mp4decrypt. The manipulation leads to memory leak. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212680.	4.3	More Details
CVE-2022-3813	A vulnerability classified as problematic has been found in Axiomatic Bento4. This affects an unknown part of the component mp4edit. The manipulation leads to memory leak. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212679.	4.3	More Details
CVE-2022-3812	A vulnerability was found in Axiomatic Bento4. It has been rated as problematic. Affected by this issue is the function AP4_ContainerAtom::AP4_ContainerAtom of the component mp4encrypt. The manipulation leads to memory leak. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-212678 is the identifier assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3804	A vulnerability was found in eolinker apinto-dashboard. It has been classified as problematic. Affected is an unknown function of the file /login. The manipulation of the argument callback leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212640.	4.3	More Details
CVE-2022-22677	A logic issue in the handling of concurrent media was addressed with improved state handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. Video self-preview in a webRTC call may be interrupted if the user answers a phone call.	4.3	More Details
CVE-2022-3318	Use after free in ChromeOS Notifications in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker who convinced a user to reboot Chrome OS to potentially exploit heap corruption via UI interaction. (Chromium security severity: Low)	4.3	More Details
CVE-2022-3317	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 106.0.5249.62 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2022-37426	Unrestricted Upload of File with Dangerous Type vulnerability in OpenNebula OpenNebula core on Linux allows File Content Injection.	4.3	More Details
CVE-2022-3807	A vulnerability was found in Axiomatic Bento4. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Incomplete Fix CVE-2019-13238. The manipulation leads to resource consumption. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212660.	4.3	More Details
CVE-2022-3444	Insufficient data validation in File System API in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass File System restrictions via a crafted HTML page and malicious file. (Chromium security severity: Low)	4.3	More Details
CVE-2022-39364	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. In Nextcloud Server prior to versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server prior to versions 22.2.10.5, 23.0.9, and 24.0.5 an attacker reading `nextcloud.log` may gain knowledge of credentials to connect to a SharePoint service. Nextcloud Server versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server versions 22.2.10.5, 23.0.9, and 24.0.5 contain a patch for this issue. As a workaround, set `zend.exception_ignore_args = On` as an option in `php.ini`.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3704	A vulnerability classified as problematic has been found in Ruby on Rails. This affects an unknown part of the file actionpack/lib/action_dispatch/middleware/templates/routes/_table.html.erb. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The real existence of this vulnerability is still doubted at the moment. The name of the patch is be177e4566747b73ff63fd5f529fab564e475ed4. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-212319. NOTE: Maintainer declares that there isn't a valid attack vector. The issue was wrongly reported as a security vulnerability by a non-member of the Rails team.	3.5	More Details
CVE-2022-3803	A vulnerability was found in eolinker apinto-dashboard and classified as problematic. This issue affects some unknown processing of the file /api/discoveries/. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212639.	3.5	More Details
CVE-2022-39329	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server and Nextcloud Enterprise Server prior to versions 23.0.9 and 24.0.5 are vulnerable to exposure of information that cannot be controlled by administrators without direct database access. Versions 23.0.9 and 24.0.5 contains patches for this issue. No known workarounds are available.	3.5	More Details
CVE-2022-3716	A vulnerability classified as problematic was found in SourceCodester Online Medicine Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /omos/admin/?page=user/list. The manipulation of the argument First Name/Middle Name/Last Name leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-212347.	3.5	More Details
CVE-2022-3783	A vulnerability, which was classified as problematic, has been found in node-red-dashboard. This issue affects some unknown processing of the file components/ui-component/ui-component-ctrl.js of the component ui_text Format Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 9305d1a82f19b235dfad24a7d1dd4ed244db7743. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-212555.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3673	A vulnerability, which was classified as problematic, was found in SourceCodester Sanitization Management System 1.0. Affected is an unknown function of the file /php-sms/classes/Master.php. The manipulation of the argument message leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-212016.	3.5	More Details
CVE-2022-3672	A vulnerability, which was classified as problematic, has been found in SourceCodester Sanitization Management System 1.0. This issue affects some unknown processing of the file /php-sms/classes/SystemSettings.php. The manipulation of the argument name/shortname leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-212015.	3.5	More Details
CVE-2021-36864	Auth. (editor+) Reflected Cross-Site Scripting (XSS) vulnerability in ExpressTech Quiz And Survey Master plugin <= 7.3.4 on WordPress.	3.4	More Details
CVE-2022-32913	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. A sandboxed app may be able to determine which app is currently using the camera.	3.3	More Details
CVE-2022-32835	This issue was addressed with improved entitlements. This issue is fixed in iOS 16, watchOS 9. An app may be able to read a persistent device identifier.	3.3	More Details
CVE-2022-2826	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. TODO	2.7	More Details
CVE-2022-32867	This issue was addressed with improved data protection. This issue is fixed in iOS 16, macOS Ventura 13. A user with physical access to an iOS device may be able to read past diagnostic logs.	2.4	More Details
CVE-2022-32879	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, tvOS 16. A user with physical access to a device may be able to access contacts from the lock screen.	2.4	More Details
CVE-2022-32870	A logic issue was addressed with improved state management. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user with physical access to a device may be able to use Siri to obtain some call history information.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3788	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-2020-23255	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-2022-3718	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-2022-3791	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-2022-3808	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-2022-3790	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-2022-3757	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-2022-3756	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-2022-3796	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-2022-3719	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-2022-3772	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-36534. Reason: This candidate is a reservation duplicate of CVE-2020-36534. Notes: All CVE users should reference CVE-2020-36534 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-2022-3755	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-2022-3717	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-2022-3773	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