SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 September 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-2022-32845	This issue was addressed with improved checks. This issue is fixed in watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to break out of its sandbox.	10.0	More Details
CVE-2022-2970	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) does not sanitize input before memcpy is used, which could allow an attacker to crash the device or remotely execute arbitrary code.	10.0	More Details
CVE-2022-2972	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) is vulnerable to a stack-based buffer overflow, which could allow an attacker to crash the device or remotely execute arbitrary code.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28802	Code by Zapier before 2022-08-17 allowed intra-account privilege escalation that included execution of Python or JavaScript code. In other words, Code by Zapier was providing a customer-controlled general-purpose virtual machine that unintentionally granted full access to all users of a company's account, but was supposed to enforce role-based access control within that company's account. Before 2022-08-17, a customer could have resolved this by (in effect) using a separate virtual machine for an application that held credentials - or other secrets - that weren't supposed to be shared among all of its employees. (Multiple accounts would have been needed to operate these independent virtual machines.)	9.9	More Details
CVE-2022-38619	SmartVista SVFE2 v2.2.22 was discovered to contain a SQL injection vulnerability via the UserForm:j_id90 parameter at /SVFE2/pages/feegroups/mcc_group.jsf.	9.8	More Details
CVE-2022-40116	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search parameter at /net-banking/beneficiary.php.	9.8	More Details
CVE-2022-40115	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/delete_beneficiary.php.	9.8	More Details
CVE-2022-40114	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/edit_customer.php.	9.8	More Details
CVE-2022-40113	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/send_funds.php.	9.8	More Details
CVE-2022-40100	Tenda i9 v1.0.0.8(3828) was discovered to contain a command injection vulnerability via the FormexeCommand function.	9.8	More Details
CVE-2022-36944	Scala 2.13.x before 2.13.9 has a Java deserialization chain in its JAR file. On its own, it cannot be exploited. There is only a risk in conjunction with Java object deserialization within an application. In such situations, it allows attackers to erase contents of arbitrary files, make network connections, or possibly run arbitrary code (specifically, Function0 functions) via a gadget chain.	9.8	More Details
CVE-2022-40118	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/send_funds_action.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40628	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper control of code generation in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to execute arbitrary commands on the targeted device.	9.8	More Details
CVE-2022-2070	In Grandstream GSD3710 in its 1.0.11.13 version, it's possible to overflow the stack since it doesn't check the param length before using the sscanf instruction. Because of that, an attacker could create a socket and connect with a remote IP:port by opening a shell and getting full access to the system. The exploit affects daemons dbmng and logsrv that are running on ports 8000 and 8001 by default.	9.8	More Details
CVE-2022-2025	an attacker with knowledge of user/pass of Grandstream GSD3710 in its 1.0.11.13 version, could overflow the stack since it doesn't check the param length before use the strcopy instruction. The explotation of this vulnerability may lead an attacker to execute a shell with full access.	9.8	More Details
CVE-2022-40868	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formDelDhcpRule with the request /goform/delDhcpRules/	9.8	More Details
CVE-2022-41220	md2roff 1.9 has a stack-based buffer overflow via a Markdown file, a different vulnerability than CVE-2022-34913. NOTE: the vendor's position is that the product is not intended for untrusted input	9.8	More Details
CVE-2022-40117	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/delete_customer.php.	9.8	More Details
CVE-2022-40119	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search_term parameter at /net-banking/transactions.php.	9.8	More Details
CVE-2022-40855	Tenda W20E router V15.11.0.6 contains a stack overflow in the function formSetPortMapping with post request 'goform/setPortMapping/'. This vulnerability allows attackers to cause a Denial of Service (DoS) or Remote Code Execution (RCE) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28722	Certain HP Print Products are potentially vulnerable to Buffer Overflow.	9.8	More Details
CVE-2022-41570	An issue was discovered in EyesOfNetwork (EON) through 5.3.11. Unauthenticated SQL injection can occur.	9.8	More Details
CVE-2022-40877	Exam Reviewer Management System 1.0 is vulnerable to SQL Injection via the ‘id’ parameter.	9.8	More Details
CVE-2022-37346	EC-CUBE plugin 'Product Image Bulk Upload Plugin' 1.0.0 and 4.1.0 contains an insufficient verification vulnerability when uploading files. Exploiting this vulnerability allows a remote unauthenticated attacker to upload arbitrary files other than image files. If a user with an administrative privilege of EC-CUBE where the vulnerable plugin is installed is led to upload a specially crafted file, an arbitrary script may be executed on the system.	9.8	More Details
CVE-2021-41433	SQL Injection vulnerability exists in version 1.0 of the Resumes Management and Job Application Website application login form by EGavilan Media that allows authentication bypass through login.php.	9.8	More Details
CVE-2022-40050	ZFile v4.1.1 was discovered to contain an arbitrary file upload vulnerability via the component /file/upload/1.	9.8	More Details
CVE-2022-30004	Sourcecodester Online Market Place Site v1.0 suffers from an unauthenticated blind SQL Injection Vulnerability allowing remote attackers to dump the SQL database via time-based SQL injection..	9.8	More Details
CVE-2022-28721	Certain HP Print Products are potentially vulnerable to Remote Code Execution.	9.8	More Details
CVE-2022-40120	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search_term parameter at /net-banking/customer_transactions.php.	9.8	More Details
CVE-2022-40485	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /package_detail.php.	9.8	More Details
CVE-2022-40484	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the booking parameter at /admin/client_edit.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40483	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /wedding_details.php.	9.8	More Details
CVE-2022-41352	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. An attacker can upload arbitrary files through amavis via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can lead to incorrect access to any other user accounts. Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavis automatically prefers it over cpio.	9.8	More Details
CVE-2022-40122	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/edit_customer_action.php.	9.8	More Details
CVE-2022-40121	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search parameter at /net-banking/manage_customers.php.	9.8	More Details
CVE-2022-40866	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formSetDebugCfg with request /goform/setDebugCfg/	9.8	More Details
CVE-2022-40867	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formIPMacBindDel with the request /goform/delIpMacBind/	9.8	More Details
CVE-2022-40854	Tenda AC18 router contained a stack overflow vulnerability in /goform/fast_setting_wifi_set	9.8	More Details
CVE-2022-37235	Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncat	9.8	More Details
CVE-2022-37026	In Erlang/OTP before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2, there is a Client Authentication Bypass in certain client-certification situations for SSL, TLS, and DTLS.	9.8	More Details
CVE-2022-41226	Jenkins Compuware Common Configuration Plugin 1.0.14 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41237	Jenkins DotCi Plugin 2.40.00 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	9.8	More Details
CVE-2022-41238	A missing permission check in Jenkins DotCi Plugin 2.40.00 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository for attacker-specified commits.	9.8	More Details
CVE-2022-40030	SourceCodester Simple Task Managing System v1.0 was discovered to contain a SQL injection vulnerability via the bookId parameter at changeStatus.php.	9.8	More Details
CVE-2021-43310	A vulnerability in Keylime before 6.3.0 allows an attacker to craft a request to the agent that resets the U and V keys as if the agent were being re-added to a verifier. This could lead to a remote code execution.	9.8	More Details
CVE-2022-3268	Weak Password Requirements in GitHub repository ikus060/minarca prior to 4.2.2.	9.8	More Details
CVE-2022-31937	Netgear N300 wireless router wnr2000v4-V1.0.0.70 was discovered to contain a stack overflow via strcpy in uhttpd.	9.8	More Details
CVE-2022-36934	An integer overflow in WhatsApp could result in remote code execution in an established video call.	9.8	More Details
CVE-2022-40851	Tenda AC15 V15.03.05.19 contained a stack overflow via the function fromAddressNat.	9.8	More Details
CVE-2022-40089	A remote file inclusion (RFI) vulnerability in Simple College Website v1.0 allows attackers to execute arbitrary code via a crafted PHP file. This vulnerability is exploitable when the directive allow_url_include is set to On.	9.8	More Details
CVE-2022-38573	10-Strike Network Inventory Explorer v9.3 was discovered to contain a buffer overflow via the Add Computers function.	9.8	More Details
CVE-2022-37232	Netgear N300 wireless router wnr2000v4-V1.0.0.70 is vulnerable to Buffer Overflow via uhttpd. There is a stack overflow vulnerability caused by strcpy.	9.8	More Details
CVE-2022-40087	Simple College Website v1.0 was discovered to contain an arbitrary file write vulnerability via the function file_put_contents(). This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40860	Tenda AC15 router V15.03.05.19 contains a stack overflow vulnerability in the function formSetQosBand->FUN_0007dd20 with request /goform/SetNetControlList	9.8	More Details
CVE-2022-40853	Tenda AC15 router V15.03.05.19 contains a stack overflow via the list parameter at /goform/fast_setting_wifi_set	9.8	More Details
CVE-2022-40869	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function fromDhcpListClient with a combined parameter "list*" ("%s%d","list").	9.8	More Details
CVE-2022-40865	Tenda AC15 and AC18 routers V15.03.05.19 contain heap overflow vulnerabilities in the function setSchedWifi with the request /goform/openSchedWifi/	9.8	More Details
CVE-2022-40864	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function setSmartPowerManagement with the request /goform/PowerSaveSet	9.8	More Details
CVE-2022-40862	Tenda AC15 and AC18 router V15.03.05.19 contains stack overflow vulnerability in the function fromNatStaticSetting with the request /goform/NatStaticSetting	9.8	More Details
CVE-2022-26112	In 0.10.0 or older versions of Apache Pinot, Pinot query endpoint and realtime ingestion layer has a vulnerability in unprotected environments due to a groovy function support. In order to avoid this, we disabled the groovy function support by default from Pinot release 0.11.0. See https://docs.pinot.apache.org/basics/releases/0.11.0	9.8	More Details
CVE-2022-41571	An issue was discovered in EyesOfNetwork (EON) through 5.3.11. Local file inclusion can occur.	9.8	More Details
CVE-2022-3236	A code injection vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sophos Firewall version v19.0 MR1 and older.	9.8	More Details
CVE-2022-3269	Session Fixation in GitHub repository ikus060/rdiffweb prior to 2.4.7.	9.8	More Details
CVE-2022-3075	Insufficient data validation in Mojo in Google Chrome prior to 105.0.5195.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23463	Nepxion Discovery is a solution for Spring Cloud. Discover is vulnerable to SpEL Injection in discovery-commons. DiscoveryExpressionResolver's eval method is evaluating expression with a StandardEvaluationContext, allowing the expression to reach and interact with Java classes such as java.lang.Runtime, leading to Remote Code Execution. There is no patch available for this issue at time of publication. There are no known workarounds.	9.4	More Details
CVE-2022-0495	The library automation system product KOHA developed by Parantez Teknoloji before version 19.05.03 has an unauthenticated SQL Injection vulnerability. This has been fixed in the version 19.05.03.01.	9.4	More Details
CVE-2022-2315	Database Software Accreditation Tracking/Presentation Module product before version 2 has an unauthenticated SQL Injection vulnerability. This is fixed in version 2.	9.4	More Details
CVE-2022-40186	An issue was discovered in HashiCorp Vault and Vault Enterprise before 1.11.3. A vulnerability in the Identity Engine was found where, in a deployment where an entity has multiple mount accessors with shared alias names, Vault may overwrite metadata to the wrong alias due to an issue with checking the proper alias assigned to an entity. This may allow for unintended access to key/value paths using that metadata in Vault.	9.1	More Details
CVE-2022-36386	Authenticated Arbitrary Code Execution vulnerability in Soflyy Import any XML or CSV File to WordPress plugin <= 3.6.7 at WordPress.	9.1	More Details
CVE-2022-36025	Besu is a Java-based Ethereum client. In versions newer than 22.1.3 and prior to 22.7.1, Besu is subject to an Incorrect Conversion between Numeric Types. An error in 32 bit signed and unsigned types in the calculation of available gas in the CALL operations (including DELEGATECALL) results in incorrect gas being passed into called contracts and incorrect gas being returned after call execution. Where the amount of gas makes a difference in the success or failure, or if the gas is a negative 64 bit value, the execution will result in a different state root than expected, resulting in a consensus failure in networks with multiple EVM implementations. In networks with a single EVM implementation this can be used to execute with significantly more gas than then transaction requested, possibly exceeding gas limitations. This issue is patched in version 22.7.1. As a workaround, reverting to version 22.1.3 or earlier will prevent incorrect execution.	9.1	More Details
CVE-2022-41241	Jenkins RQM Plugin 2.8 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32847	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	9.1	More Details
CVE-2022-23144	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system.	9.1	More Details
CVE-2022-39227	python-jwt is a module for generating and verifying JSON Web Tokens. Versions prior to 3.3.4 are subject to Authentication Bypass by Spoofing, resulting in identity spoofing, session hijacking or authentication bypass. An attacker who obtains a JWT can arbitrarily forge its contents without knowing the secret key. Depending on the application, this may for example enable the attacker to spoof other user's identities, hijack their sessions, or bypass authentication. Users should upgrade to version 3.3.4. There are no known workarounds.	9.1	More Details
CVE-2022-2566	A heap out-of-bounds memory write exists in FFMPEG since version 5.1. The size calculation in `build_open_gop_key_points()` goes through all entries in the loop and adds `sc->ctts_data[i].count` to `sc->sample_offsets_count`. This can lead to an integer overflow resulting in a small allocation with `av_calloc()`. An attacker can cause remote code execution via a malicious mp4 file. We recommend upgrading past commit c953baa084607dd1d84c3bfcce3cf6a87c3e6e05	9.0	More Details
CVE-2022-39256	Orckestra C1 CMS is a .NET based Web Content Management System. A vulnerability in versions prior to 6.13 allows remote attackers to execute arbitrary code on affected installations of Orckestra C1 CMS. Authentication is required to exploit this vulnerability. The authenticated user may perform the actions unknowingly by visiting a specially crafted site. This issue is patched in C1 CMS v6.13. There are no known workarounds.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-41604	Check Point ZoneAlarm Extreme Security before 15.8.211.19229 allows local users to escalate privileges. This occurs because of weak permissions for the %PROGRAMDATA%\CheckPoint\ZoneAlarm\Data\Updates directory, and a self-protection driver bypass that allows creation of a junction directory. This can be leveraged to perform an arbitrary file move as NT AUTHORITY\SYSTEM.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3045	Insufficient validation of untrusted input in V8 in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2998	Use after free in Browser Creation in Google Chrome prior to 104.0.5112.101 allowed a remote attacker who had convinced a user to engage in a specific UI interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-40784	Unlimited strcpy on user input when setting a locale file leads to stack buffer overflow in mIPC camera firmware 5.3.1.2003161406.	8.8	More Details
CVE-2022-41234	Jenkins Rundeck Plugin 3.6.11 and earlier does not protect access to the /plugin/rundeck/webhook/ endpoint, allowing users with Overall/Read permission to trigger jobs that are configured to be triggerable via Rundeck.	8.8	More Details
CVE-2022-40043	Centreon v20.10.18 was discovered to contain a SQL injection vulnerability via the esc_name (Escalation Name) parameter at Configuration/Notifications/Escalations.	8.8	More Details
CVE-2022-41236	A cross-site request forgery (CSRF) vulnerability in Jenkins Security Inspector Plugin 117.v6eecc36919c2 and earlier allows attackers to replace the generated report stored in a per-session cache and displayed to authorized users at the .../report URL with a report based on attacker-specified report generation options.	8.8	More Details
CVE-2022-3200	Heap buffer overflow in Internals in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3199	Use after free in Frames in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3198	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2022-3038	Use after free in Network Service in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-3039	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41245	A cross-site request forgery (CSRF) vulnerability in Jenkins Worksoft Execution Manager Plugin 10.0.3.503 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2022-3197	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2022-3196	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2022-3195	Out of bounds write in Storage in Google Chrome prior to 105.0.5195.125 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-2022-41249	A cross-site request forgery (CSRF) vulnerability in Jenkins SCM HttpClient Plugin 1.5 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2022-3071	Use after free in Tab Strip in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interaction.	8.8	More Details
CVE-2022-3058	Use after free in Sign-In Flow in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interaction.	8.8	More Details
CVE-2022-3055	Use after free in Passwords in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-41253	A cross-site request forgery (CSRF) vulnerability in Jenkins CONS3RT Plugin 1.0.0 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2022-3052	Heap buffer overflow in Window Manager in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3051	Heap buffer overflow in Exosphere in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions.	8.8	More Details
CVE-2022-3040	Use after free in Layout in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-3050	Heap buffer overflow in WebUI in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions.	8.8	More Details
CVE-2022-3049	Use after free in SplitScreen in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-3041	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-3042	Use after free in PhoneHub in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-3043	Heap buffer overflow in Screen Capture in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2859	Use after free in Chrome OS Shell in Google Chrome prior to 104.0.5112.101 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-2858	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via specific UI interaction.	8.8	More Details
CVE-2022-2857	Use after free in Blink in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-41228	A missing permission check in Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.129 and earlier allows attackers with Overall/Read permissions to connect to an attacker-specified webserver using attacker-specified credentials.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40878	In Exam Reviewer Management System 1.0, an authenticated attacker can upload a web-shell php file in profile page to achieve Remote Code Execution (RCE).	8.8	More Details
CVE-2022-22610	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution.	8.8	More Details
CVE-2022-22624	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4, tvOS 15.4, Safari 15.4. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-22628	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-22637	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior.	8.8	More Details
CVE-2022-26700	A memory corruption issue was addressed with improved state 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. Processing maliciously crafted web content may lead to code execution.	8.8	More Details
CVE-2022-32211	A SQL injection vulnerability exists in Rocket.Chat <v3.18.6, <v4.4.4 and <v4.7.3 which can allow an attacker to retrieve a reset password token through or a 2fa secret.	8.8	More Details
CVE-2022-32787	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-37209	JFinal CMS 5.1.0 is affected by: SQL Injection. These interfaces do not use the same component, nor do they have filters, but each uses its own SQL concatenation method, resulting in SQL injection.	8.8	More Details
CVE-2022-32792	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35248	A improper authentication vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 that allowed two factor authentication can be bypassed when telling the server to use CAS during login.	8.8	More Details
CVE-2022-40298	Crestron AirMedia for Windows before 5.5.1.84 has insecure inherited permissions, which leads to a privilege escalation vulnerability found in the AirMedia Windows Application, version 4.3.1.39. A low privileged user can initiate a repair of the system and gain a SYSTEM level shell.	8.8	More Details
CVE-2022-22629	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-36159	Contec FXA3200 version 1.13 and under were discovered to contain a hard coded hash password for root stored in the component /etc/shadow. As the password strength is weak, it can be cracked in few minutes. Through this credential, a malicious actor can access the Wireless LAN Manager interface and open the telnet port then sniff the traffic or inject any malware.	8.8	More Details
CVE-2021-24890	The Scripts Organizer WordPress plugin before 3.0 does not have capability and CSRF checks in the saveScript AJAX action, available to both unauthenticated and authenticated users, and does not validate user input in any way, which could allow unauthenticated users to put arbitrary PHP code in a file	8.8	More Details
CVE-2022-31367	Strapi before 3.6.10 and 4.x before 4.1.10 mishandles hidden attributes within admin API responses.	8.8	More Details
CVE-2022-3068	Improper Privilege Management in GitHub repository octoprint/octoprint prior to 1.8.3.	8.8	More Details
CVE-2022-40402	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the booking parameter at /admin/client_assign.php.	8.8	More Details
CVE-2022-40404	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/select.php.	8.8	More Details
CVE-2022-40785	Unsanitized input when setting a locale file leads to shell injection in mIPC camera firmware 5.3.1.2003161406. This allows an attacker to gain remote code execution on cameras running the firmware when a victim logs into a specially crafted mobile app.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2852	Use after free in FedCM in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2853	Heap buffer overflow in Downloads in Google Chrome on Android prior to 104.0.5112.101 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2854	Use after free in SwiftShader in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2855	Use after free in ANGLE in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-41227	A cross-site request forgery (CSRF) vulnerability in Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.129 and earlier allows attackers to connect to an attacker-specified webserver using attacker-specified credentials.	8.8	More Details
CVE-2022-3046	Use after free in Browser Tag in Google Chrome prior to 105.0.5195.52 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2973	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) uses a NULL pointer in certain situations. which could allow an attacker to crash the server.	8.6	More Details
CVE-2022-2971	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) accesses a resource using an incompatible type, which could allow an attacker to crash the server with a malicious payload.	8.6	More Details
CVE-2022-39219	Bifrost is a middleware package which can synchronize MySQL/MariaDB binlog data to other types of databases. Versions 1.8.6-release and prior are vulnerable to authentication bypass when using HTTP basic authentication. This may allow group members who only have read permissions to write requests when they are normally forbidden from doing so. Version 1.8.7-release contains a patch. There are currently no known workarounds.	8.5	More Details
CVE-2022-22058	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39243	NuProcess is an external process execution implementation for Java. In all the versions of NuProcess where it forks processes by using the JVM's Java_java_lang_UNIXProcess_forkAndExec method (1.2.0+), attackers can use NUL characters in their strings to perform command line injection. Java's ProcessBuilder isn't vulnerable because of a check in ProcessBuilder.start. NuProcess is missing that check. This vulnerability can only be exploited to inject command line arguments on Linux. Version 2.0.5 contains a patch. As a workaround, users of the library can sanitize command strings to remove NUL characters prior to passing them to NuProcess for execution.	8.4	More Details
CVE-2022-39245	Mist is the command-line interface for the makedeb Package Repository. Prior to version 0.9.5, a user-provided `sudo` binary via the `PATH` variable can allow a local user to run arbitrary commands on the user's system with root permissions. Versions 0.9.5 and later contain a patch. No known workarounds exist.	8.4	More Details
CVE-2022-35408	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.)	8.2	More Details
CVE-2022-35893	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntimeDxe driver allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2022-36338	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver FwBlockServiceSmm, creating SMM, leads to arbitrary code execution. An attacker can replace the pointer to the UEFI boot service GetVariable with a pointer to malware, and then generate a software SMI.	8.2	More Details
CVE-2022-35895	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution.	8.2	More Details
CVE-2022-40616	IBM Maximo Asset Management 7.6.1.1, 7.6.1.2, and 7.6.1.3 could allow a user to bypass authentication and obtain sensitive information or perform tasks they should not have access to. IBM X-Force ID: 236311.	8.1	More Details
CVE-2022-41244	Jenkins View26 Test-Reporting Plugin 1.0.7 and earlier does not perform hostname validation when connecting to the configured View26 server that could be abused using a man-in-the-middle attack to intercept these connections.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41243	Jenkins SmallTest Plugin 1.0.4 and earlier does not perform hostname validation when connecting to the configured View26 server that could be abused using a man-in-the-middle attack to intercept these connections.	8.1	More Details
CVE-2022-39258	mailcow is a mailserver suite. A vulnerability innversions prior to 2022-09 allows an attacker to craft a custom Swagger API template to spoof Authorize links. This could redirect a victim to an attacker controller place to steal Swagger authorization credentials or create a phishing page to steal other information. The issue has been fixed with the 2022-09 mailcow Mootember Update. As a workaround, one may delete the Swapper API Documentation from their e-mail server.	8.1	More Details
CVE-2022-38742	Rockwell Automation ThinManager ThinServer versions 11.0.0 - 13.0.0 is vulnerable to a heap-based buffer overflow. An attacker could send a specifically crafted TFTP or HTTPS request, causing a heap-based buffer overflow that crashes the ThinServer process. If successfully exploited, this could expose the server to arbitrary remote code execution.	8.1	More Details
CVE-2020-36604	hoek before 8.5.1 and 9.x before 9.0.3 allows prototype poisoning in the clone function.	8.1	More Details
CVE-2022-30578	The Web Server component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 5.4.1 and below.	8.0	More Details
CVE-2022-36158	Contec FXA3200 version 1.13.00 and under suffers from Insecure Permissions in the Wireless LAN Manager interface which allows malicious actors to execute Linux commands with root privilege via a hidden web page (/usr/www/ja/mnt_cmd.cgi).	8.0	More Details
CVE-2022-30577	The Web Server component of TIBCO Software Inc.'s TIBCO EBX contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 6.0.0 through 6.0.8.	8.0	More Details
CVE-2022-41232	A cross-site request forgery (CSRF) vulnerability in Jenkins Build-Publisher Plugin 1.22 and earlier allows attackers to replace any config.xml file on the Jenkins controller file system with an empty file by providing a crafted file name to an API endpoint.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32796	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-37234	Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncpy.	7.8	More Details
CVE-2022-38932	readelf in ToaruOS 2.0.1 has a global overflow allowing RCE when parsing a crafted ELF file.	7.8	More Details
CVE-2022-35257	A local privilege escalation vulnerability in UI Desktop for Windows (Version 0.55.1.2 and earlier) allows a malicious actor with local access to a Windows device with UI Desktop to run arbitrary commands as SYSTEM.	7.8	More Details
CVE-2022-3296	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0577.	7.8	More Details
CVE-2022-3297	Use After Free in GitHub repository vim/vim prior to 9.0.0579.	7.8	More Details
CVE-2022-41347	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.x and 9.x (e.g., 8.8.15). The Sudo configuration permits the zimbra user to execute the NGINX binary as root with arbitrary parameters. As part of its intended functionality, NGINX can load a user-defined configuration file, which includes plugins in the form of .so files, which also execute as root.	7.8	More Details
CVE-2022-32814	A type confusion issue was addressed with improved state handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-41322	In Kitty before 0.26.2, insufficient validation in the desktop notification escape sequence can lead to arbitrary code execution. The user must display attacker-controlled content in the terminal, then click on a notification popup.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30426	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir.	7.8	More Details
CVE-2022-3263	The security descriptor of Measuresoft ScadaPro Server version 6.7 has inconsistent permissions, which could allow a local user with limited privileges to modify the service binary path and start malicious commands with SYSTEM privileges.	7.8	More Details
CVE-2022-32798	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.5. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2022-3324	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0598.	7.8	More Details
CVE-2022-32801	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.5. An app may be able to gain root privileges.	7.8	More Details
CVE-2022-27492	An integer underflow in WhatsApp could have caused remote code execution when receiving a crafted video file.	7.8	More Details
CVE-2022-32842	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. An app may be able to gain elevated privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32815	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32829	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32826	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges.	7.8	More Details
CVE-2022-32821	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32820	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-38928	XPDF 4.04 is vulnerable to Null Pointer Dereference in FoFiType1C.cc:2393.	7.8	More Details
CVE-2022-32819	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges.	7.8	More Details
CVE-2022-3103	off-by-one in io_uring module.	7.8	More Details
CVE-2022-3256	Use After Free in GitHub repository vim/vim prior to 9.0.0530.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2347	There exists an unchecked length field in UBoot. The U-Boot DFU implementation does not bound the length field in USB DFU download setup packets, and it does not verify that the transfer direction corresponds to the specified command. Consequently, if a physical attacker crafts a USB DFU download setup packet with a `wLength` greater than 4096 bytes, they can write beyond the heap-allocated request buffer.	7.7	More Details
CVE-2022-36062	Grafana is an open-source platform for monitoring and observability. In versions prior to 8.5.13, 9.0.9, and 9.1.6, Grafana is subject to Improper Preservation of Permissions resulting in privilege escalation on some folders where Admin is the only used permission. The vulnerability impacts Grafana instances where RBAC was disabled and enabled afterwards, as the migrations which are translating legacy folder permissions to RBAC permissions do not account for the scenario where the only user permission in the folder is Admin, as a result RBAC adds permissions for Editors and Viewers which allow them to edit and view folders accordingly. This issue has been patched in versions 8.5.13, 9.0.9, and 9.1.6. A workaround when the impacted folder/dashboard is known is to remove the additional permissions manually.	7.6	More Details
CVE-2022-1941	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated.	7.5	More Details
CVE-2022-2265	The Identity and Directory Management System developed by Çekino Bilgi Teknolojileri before version 2.1.25 has an unauthenticated Path traversal vulnerability. This has been fixed in the version 2.1.25	7.5	More Details
CVE-2022-40105	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formWifiMacFilterGet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details
CVE-2022-28981	Path traversal vulnerability in the Hypermedia REST APIs module in Liferay Portal 7.4.0 through 7.4.2 allows remote attackers to access files outside of com.liferay.headless.discovery.web/META-INF/resources via the `parameter` parameter.	7.5	More Details
CVE-2022-40104	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formwrlSSIDget 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-2022-40102	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formwrlSSIDset function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details
CVE-2022-40101	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formWifiMacFilterSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details
CVE-2022-3204	A vulnerability named 'Non-Responsive Delegation Attack' (NRDelegation Attack) has been discovered in various DNS resolving software. The NRDelegation Attack works by having a malicious delegation with a considerable number of non responsive nameservers. The attack starts by querying a resolver for a record that relies on those unresponsive nameservers. The attack can cause a resolver to spend a lot of time/resources resolving records under a malicious delegation point where a considerable number of unresponsive NS records reside. It can trigger high CPU usage in some resolver implementations that continually look in the cache for resolved NS records in that delegation. This can lead to degraded performance and eventually denial of service in orchestrated attacks. Unbound does not suffer from high CPU usage, but resources are still needed for resolving the malicious delegation. Unbound will keep trying to resolve the record until hard limits are reached. Based on the nature of the attack and the replies, different limits could be reached. From version 1.16.3 on, Unbound introduces fixes for better performance when under load, by cutting opportunistic queries for nameserver discovery and DNSKEY prefetching and limiting the number of times a delegation point can issue a cache lookup for missing records.	7.5	More Details
CVE-2022-2906	An attacker can leverage this flaw to gradually erode available memory to the point where named crashes for lack of resources. Upon restart the attacker would have to begin again, but nevertheless there is the potential to deny service.	7.5	More Details
CVE-2022-34326	In ambiot amb1_sdk (aka SDK for Ameba1) before 2022-06-20 on Realtek RTL8195AM devices before 284241d70308ff2519e40afd7b284ba892c730a3, the timer task and RX task would be locked when there are frequent and continuous Wi-Fi connection (with four-way handshake) failures in Soft AP mode.	7.5	More Details
CVE-2022-40146	Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to access files using a Jar url. This issue affects Apache XML Graphics Batik 1.14.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28052	A tenant administrator Hitachi Content Platform (HCP) may modify the configuration in another tenant without authorization, potentially allowing unauthorized access to data in the other tenant. Also, a tenant user (non-administrator) may view configuration in another tenant without authorization. This issue affects: Hitachi Vantara Hitachi Content Platform versions prior to 8.3.7; 9.0.0 versions prior to 9.2.3.	7.5	More Details
CVE-2022-3298	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.4.8.	7.5	More Details
CVE-2022-40188	Knot Resolver before 5.5.3 allows remote attackers to cause a denial of service (CPU consumption) because of algorithmic complexity. During an attack, an authoritative server must return large NS sets or address sets.	7.5	More Details
CVE-2022-3290	Improper Handling of Length Parameter Inconsistency in GitHub repository ikus060/rdiffweb prior to 2.4.8.	7.5	More Details
CVE-2022-3272	Improper Handling of Length Parameter Inconsistency in GitHub repository ikus060/rdiffweb prior to 2.4.8.	7.5	More Details
CVE-2022-3252	Improper detection of complete HTTP body decompression SwiftNIO Extras provides a pair of helpers for transparently decompressing received HTTP request or response bodies. These two objects (HTTPRequestDecompressor and HTTPResponseDecompressor) both failed to detect when the decompressed body was considered complete. If trailing junk data was appended to the HTTP message body, the code would repeatedly attempt to decompress this data and fail. This would lead to an infinite loop making no forward progress, leading to livelock of the system and denial-of-service. This issue can be triggered by any attacker capable of sending a compressed HTTP message. Most commonly this is HTTP servers, as compressed HTTP messages cannot be negotiated for HTTP requests, but it is possible that users have configured decompression for HTTP requests as well. The attack is low effort, and likely to be reached without requiring any privilege or system access. The impact on availability is high: the process immediately becomes unavailable but does not immediately crash, meaning that it is possible for the process to remain in this state until an administrator intervenes or an automated circuit breaker fires. If left unchecked this issue will very slowly exhaust memory resources due to repeated buffer allocation, but the buffers are not written to and so it is possible that the processes will not terminate for quite some time. This risk can be mitigated by removing transparent HTTP message decompression. The issue is fixed by correctly detecting the termination of the compressed body as reported by zlib and refusing to decompress further data. The issue was found by Vojtech Rylko (https://github.com/vojtarylko) and reported publicly on GitHub.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23952	In Keylime before 6.3.0, current keylime installer installs the keylime.conf file, which can contain sensitive data, as world-readable.	7.5	More Details
CVE-2022-23950	In Keylime before 6.3.0, Revocation Notifier uses a fixed /tmp path for UNIX domain socket which can allow unprivileged users a method to prohibit keylime operations.	7.5	More Details
CVE-2022-23949	In Keylime before 6.3.0, unsanitized UUIDs can be passed by a rogue agent and can lead to log spoofing on the verifier and registrar.	7.5	More Details
CVE-2022-23948	A flaw was found in Keylime before 6.3.0. The logic in the Keylime agent for checking for a secure mount can be fooled by previously created unprivileged mounts allowing secrets to be leaked to other processes on the host.	7.5	More Details
CVE-2022-40106	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the set_local_time function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details
CVE-2022-34026	ICEcoder v8.1 allows attackers to execute a directory traversal.	7.5	More Details
CVE-2022-40629	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to insecure design in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to view sensitive information on the targeted device.	7.5	More Details
CVE-2022-38178	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.	7.5	More Details
CVE-2022-39221	McWebserver mod runs a simple HTTP server alongside the Minecraft server in seperate threads. Path traversal in McWebserver Minecraft Mod for Fabric and Quilt up to and including 0.1.2.1 and McWebserver Minecraft Mod for Forge up to and including 0.1.1 allows all files, accessible by the program, to be read by anyone via HTTP request. Version 0.2.0 with patches are released to both platforms (Fabric and Quilt, Forge). As a workaround, the McWebserver mod can be disabled by removing the file from the `mods` directory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40604	In Apache Airflow 2.3.0 through 2.3.4, part of a url was unnecessarily formatted, allowing for possible information extraction.	7.5	More Details
CVE-2022-3295	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.4.8.	7.5	More Details
CVE-2022-38936	An issue has been found in PBC through 2022-8-27. A SEGV issue detected in the function pbc_wmessage_integer in src/wmessage.c:137.	7.5	More Details
CVE-2022-3323	An SQL injection vulnerability in Advantech iView 5.7.04.6469. The specific flaw exists within the ConfigurationServlet endpoint, which listens on TCP port 8080 by default. An unauthenticated remote attacker can craft a special column_value parameter in the setConfiguration action to bypass checks in com.imc.iview.utils.CUtils.checkSQLInjection() to perform SQL injection. For example, the attacker can exploit the vulnerability to retrieve the iView admin password.	7.5	More Details
CVE-2022-2987	The Ldap WP Login / Active Directory Integration WordPress plugin before 3.0.2 does not have any authorisation and CSRF checks when updating it's settings (which are hooked to the init action), allowing unauthenticated attackers to update them. Attackers could set their own LDAP server to be used to authenticated users, therefore bypassing the current authentication	7.5	More Details
CVE-2022-32790	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service.	7.5	More Details
CVE-2022-3080	By sending specific queries to the resolver, an attacker can cause named to crash.	7.5	More Details
CVE-2022-3119	The OAuth client Single Sign On WordPress plugin before 3.0.4 does not have authorisation and CSRF when updating its settings, which could allow unauthenticated attackers to update them and change the OAuth endpoints to ones they controls, allowing them to then be authenticated as admin if they know the correct email address	7.5	More Details
CVE-2022-41343	registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40705	An Improper Restriction of XML External Entity Reference vulnerability in RPCRouterServlet of Apache SOAP allows an attacker to read arbitrary files over HTTP. This issue affects Apache SOAP version 2.2 and later versions. It is unknown whether previous versions are also affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details
CVE-2022-41340	The secp256k1-js package before 1.1.0 for Node.js implements ECDSA without required r and s validation, leading to signature forgery.	7.5	More Details
CVE-2022-38177	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.	7.5	More Details
CVE-2022-40107	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formexeCommand function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details
CVE-2022-37193	Chipolo ONE Bluetooth tracker (2020) Chipolo iOS app version 4.13.0 is vulnerable to Incorrect Access Control. Chipolo devices suffer from access revocation evasion attacks once the malicious sharee obtains the access credentials.	7.4	More Details
CVE-2022-21797	The package joblib from 0 and before 1.2.0 are vulnerable to Arbitrary Code Execution via the pre_dispatch flag in Parallel() class due to the eval() statement.	7.3	More Details
CVE-2022-21169	The package express-xss-sanitizer before 1.1.3 are vulnerable to Prototype Pollution via the allowedTags attribute, allowing the attacker to bypass xss sanitization.	7.3	More Details
CVE-2022-40353	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/up_booking.php.	7.2	More Details
CVE-2022-40093	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tour/admin/update_tax.php.	7.2	More Details
CVE-2022-40091	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tour/admin/update_packages.php.	7.2	More Details
CVE-2022-40354	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_booking.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40352	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_traveller.php.	7.2	More Details
CVE-2022-40092	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tour/admin/update_payment.php.	7.2	More Details
CVE-2022-40026	SourceCodester Simple Task Managing System v1.0 was discovered to contain a SQL injection vulnerability via the bookId parameter at board.php.	7.2	More Details
CVE-2022-40403	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/feature_edit.php.	7.2	More Details
CVE-2022-40932	In Zoo Management System v1.0, there is an arbitrary file upload vulnerability in the picture upload point of the "gallery" file of the "Gallery" module in the background management system.	7.2	More Details
CVE-2022-37027	Ahsay AhsayCBS 9.1.4.0 allows an authenticated system user to inject arbitrary Java JVM options. Administrators that can modify the Runtime Options in the web interface can inject Java Runtime Options. These take effect after a restart. For example, an attacker can enable JMX services and consequently achieve remote code execution as the system user.	7.2	More Details
CVE-2022-40097	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_currency.php.	7.2	More Details
CVE-2022-40098	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_expense.php.	7.2	More Details
CVE-2022-40099	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_expense_category.php.	7.2	More Details
CVE-2022-40928	Online Leave Management System v1.0 is vulnerable to SQL Injection via /leave_system/classes/Master.php?f=delete_application.	7.2	More Details
CVE-2022-40861	Tenda AC18 router V15.03.05.19 contains a stack overflow vulnerability in the formSetQosBand->FUN_0007db78 function with the request /goform/SetNetControlList/	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40926	Online Leave Management System v1.0 is vulnerable to SQL Injection via /leave_system/classes/Master.php?f=delete_leave_type.	7.2	More Details
CVE-2022-40925	Zoo Management System v1.0 has an arbitrary file upload vulnerability in the picture upload point of the "save_event" file of the "Events" module in the background management system.	7.2	More Details
CVE-2022-40924	Zoo Management System v1.0 has an arbitrary file upload vulnerability in the picture upload point of the "save_animal" file of the "Animals" module in the background management system.	7.2	More Details
CVE-2022-40446	ZZCMS 2022 was discovered to contain a SQL injection vulnerability via the component /admin/sendmailto.php?tomail=&groupid=.	7.2	More Details
CVE-2022-40447	ZZCMS 2022 was discovered to contain a SQL injection vulnerability via the keyword parameter at /admin/baojia_list.php.	7.2	More Details
CVE-2022-40927	Online Leave Management System v1.0 is vulnerable to SQL Injection via /leave_system/classes/Master.php?f=delete_designation.	7.2	More Details
CVE-2022-3076	The CM Download Manager WordPress plugin before 2.8.6 allows high privilege users such as admin to upload arbitrary files by setting the any extension via the plugin's setting, which could be used by admins of multisite blog to upload PHP files for example.	7.2	More Details
CVE-2022-2903	The Ninja Forms Contact Form WordPress plugin before 3.6.13 unserialises the content of an imported file, which could lead to PHP object injections issues 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-2022-2352	The Post SMTP Mailer/Email Log WordPress plugin before 2.1.7 does not have proper authorisation in some AJAX actions, which could allow high privilege users such as admin to perform blind SSRF on multisite installations for example.	7.2	More Details
CVE-2022-40933	Online Pet Shop We App v1.0 by oretnom23 is vulnerable to SQL injection via /pet_shop/classes/Master.php?f=delete_order,id.	7.2	More Details
CVE-2022-40934	Online Pet Shop We App v1.0 is vulnerable to SQL injection via /pet_shop/classes/Master.php?f=delete_sub_category,id	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40935	Online Pet Shop We App v1.0 is vulnerable to SQL Injection via /pet_shop/classes/Master.php?f=delete_category,id.	7.2	More Details
CVE-2022-32807	This issue was addressed with improved file handling. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to overwrite arbitrary files.	7.1	More Details
CVE-2022-32797	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory.	7.1	More Details
CVE-2022-32853	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory.	7.1	More Details
CVE-2022-34348	IBM Sterling Partner Engagement Manager 6.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 230017.	7.1	More Details
CVE-2022-32852	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory.	7.1	More Details
CVE-2022-32851	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory.	7.1	More Details
CVE-2022-32843	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted Postscript file may result in unexpected app termination or disclosure of process memory.	7.1	More Details
CVE-2022-32831	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36521	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iCloud for Windows 11.4, iOS 14.0 and iPadOS 14.0, watchOS 7.0, tvOS 14.0, iCloud for Windows 7.21, iTunes for Windows 12.10.9. Processing a maliciously crafted tiff file may lead to a denial-of-service or potentially disclose memory contents.	7.1	More Details
CVE-2021-41803	HashiCorp Consul 1.8.1 up to 1.11.8, 1.12.4, and 1.13.1 do not properly validate the node or segment names prior to interpolation and usage in JWT claim assertions with the auto config RPC. Fixed in 1.11.9, 1.12.5, and 1.13.2."	7.1	More Details
CVE-2022-35951	Redis is an in-memory database that persists on disk. Versions 7.0.0 and above, prior to 7.0.5 are vulnerable to an Integer Overflow. Executing an `XAUTOCLAIM` command on a stream key in a specific state, with a specially crafted `COUNT` argument may cause an integer overflow, a subsequent heap overflow, and potentially lead to remote code execution. This has been patched in Redis version 7.0.5. No known workarounds exist.	7.0	More Details
CVE-2022-39224	Arr-pm is an RPM reader/writer library written in Ruby. Versions prior to 0.0.12 are subject to OS command injection resulting in shell execution if the RPM contains a malicious "payload compressor" field. This vulnerability impacts the `extract` and `files` methods of the `RPM::File` class of this library. Version 0.0.12 patches these issues. A workaround for this issue is to ensure any RPMs being processed contain valid/known payload compressor values such as gzip, bzip2, xz, zstd, and lzma. The payload compressor field in an rpm can be checked by using the rpm command line tool.	7.0	More Details
CVE-2022-41222	mm/mremap.c in the Linux kernel before 5.13.3 has a use-after-free via a stale TLB because an rmap lock is not held during a PUD move.	7.0	More Details
CVE-2022-3048	Inappropriate implementation in Chrome OS lockscreen in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a local attacker to bypass lockscreen navigation restrictions via physical access to the device.	6.8	More Details
CVE-2022-30124	An improper authentication vulnerability exists in Rocket.Chat Mobile App <4.14.1.22788 that allowed an attacker with physical access to a mobile device to bypass local authentication (PIN code).	6.8	More Details
CVE-2022-30121	The “LANDesk(R) Management Agent” service exposes a socket and once connected, it is possible to launch commands only for signed executables. This is a security bug that allows a limited user to get escalated admin privileges on their system.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2785	There exists an arbitrary memory read within the Linux Kernel BPF - Constants provided to fill pointers in structs passed in to bpf_sys_bpf are not verified and can point anywhere, including memory not owned by BPF. An attacker with CAP_BPF can arbitrarily read memory from anywhere on the system. We recommend upgrading past commit 86f44fcec22c	6.7	More Details
CVE-2022-32832	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2021-3782	An internal reference count is held on the buffer pool, incremented every time a new buffer is created from the pool. The reference count is maintained as an int; on LP64 systems this can cause the reference count to overflow if the client creates a large number of wl_shm buffer objects, or if it can coerce the server to create a large number of external references to the buffer storage. With the reference count overflowing, a use-after-free can be constructed on the wl_shm_pool tracking structure, where values may be incremented or decremented; it may also be possible to construct a limited oracle to leak 4 bytes of server-side memory to the attacking client at a time.	6.6	More Details
CVE-2022-38970	ieGeek IG20 hipcam RealServer V1.0 is vulnerable to Incorrect Access Control. The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	6.5	More Details
CVE-2022-35026	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fbc0b.	6.5	More Details
CVE-2022-35031	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x703969.	6.5	More Details
CVE-2022-35025	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x5266a8.	6.5	More Details
CVE-2022-35027	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fe9a7.	6.5	More Details
CVE-2022-35028	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fbbb6.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35029	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6babea.	6.5	More Details
CVE-2022-32220	An information disclosure vulnerability exists in Rocket.Chat <v5 due to the getUserMentionsByChannel meteor server method discloses messages from private channels and direct messages regardless of the users access permission to the room.	6.5	More Details
CVE-2022-35030	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fe954.	6.5	More Details
CVE-2022-35024	OTFCC commit 617837b was discovered to contain a segmentation violation via /multiarch/memmove-vec-unaligned-erms.S.	6.5	More Details
CVE-2022-32227	A cleartext transmission of sensitive information exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 relating to Oauth tokens by having the permission "view-full-other-user-info", this could cause an oauth token leak in the product.	6.5	More Details
CVE-2022-35036	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e1fc8.	6.5	More Details
CVE-2022-35032	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6b6a8f.	6.5	More Details
CVE-2022-35034	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e7e3d.	6.5	More Details
CVE-2022-35035	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b559f.	6.5	More Details
CVE-2022-35238	Unauthenticated Plugin Settings Change vulnerability in Awesome Filterable Portfolio plugin <= 1.9.7 at WordPress.	6.5	More Details
CVE-2022-35038	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b064d.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40630	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper session management in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to perform session fixation on the targeted device.	6.5	More Details
CVE-2022-35039	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e20a0.	6.5	More Details
CVE-2022-36340	Unauthenticated Optin Campaign Cache Deletion vulnerability in MailOptin plugin <= 1.2.49.0 at WordPress.	6.5	More Details
CVE-2022-41320	Veritas System Recovery (VSR) versions 18 and 21 store a network destination password in the Windows registry during configuration of the backup configuration. This vulnerability could provide a Windows user (who has sufficient privileges) to access a network file system that they were not authorized to access.	6.5	More Details
CVE-2022-39230	fhir-works-on-aws-authz-smart is an implementation of the authorization interface from the FHIR Works interface. Versions 3.1.1 and 3.1.2 are subject to Exposure of Sensitive Information to an Unauthorized Actor. This issue allows a client of the API to retrieve more information than the client's OAuth scope permits when making "search-type" requests. This issue would not allow a client to retrieve information about individuals other than those the client was already authorized to access. Users of fhir-works-on-aws-authz-smart 3.1.1 or 3.1.2 should upgrade to version 3.1.3 or higher immediately. Versions 3.1.0 and below are unaffected. There is no workaround for this issue.	6.5	More Details
CVE-2022-40716	HashiCorp Consul and Consul Enterprise up to 1.11.8, 1.12.4, and 1.13.1 do not check for multiple SAN URI values in a CSR on the internal RPC endpoint, enabling leverage of privileged access to bypass service mesh intentions. Fixed in 1.11.9, 1.12.5, and 1.13.2."	6.5	More Details
CVE-2022-32816	The issue was addressed with improved UI handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Visiting a website that frames malicious content may lead to UI spoofing.	6.5	More Details
CVE-2022-35037	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6adb1e.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35023	OTFCC commit 617837b was discovered to contain a segmentation violation via /lib/x86_64-linux-gnu/libc.so.6+0xbb384.	6.5	More Details
CVE-2022-24280	Improper Input Validation vulnerability in Proxy component of Apache Pulsar allows an attacker to make TCP/IP connection attempts that originate from the Pulsar Proxy's IP address. When the Apache Pulsar Proxy component is used, it is possible to attempt to open TCP/IP connections to any IP address and port that the Pulsar Proxy can connect to. An attacker could use this as a way for DoS attacks that originate from the Pulsar Proxy's IP address. It hasn't been detected that the Pulsar Proxy authentication can be bypassed. The attacker will have to have a valid token to a properly secured Pulsar Proxy. This issue affects Apache Pulsar Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.2; 2.9.0 to 2.9.1; 2.6.4 and earlier.	6.5	More Details
CVE-2022-3054	Insufficient policy enforcement in DevTools in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2022-3056	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to bypass content security policy via a crafted HTML page.	6.5	More Details
CVE-2022-3057	Inappropriate implementation in iframe Sandbox in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-41255	Jenkins CONS3RT Plugin 1.0.0 and earlier stores Cons3rt API token unencrypted in job config.xml files on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-3047	Insufficient policy enforcement in Extensions API in Google Chrome prior to 105.0.5195.52 allowed an attacker who convinced a user to install a malicious extension to bypass downloads policy via a crafted HTML page.	6.5	More Details
CVE-2022-35022	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6badae.	6.5	More Details
CVE-2022-3044	Inappropriate implementation in Site Isolation in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2022-2861	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.101 allowed an attacker who convinced a user to install a malicious extension to inject arbitrary scripts into WebUI via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2860	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to bypass cookie prefix restrictions via a crafted HTML page.	6.5	More Details
CVE-2022-2856	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 104.0.5112.101 allowed a remote attacker to arbitrarily browse to a malicious website via a crafted HTML page.	6.5	More Details
CVE-2022-40217	Authenticated (admin+) Arbitrary File Edit/Upload vulnerability in XplodedThemes WPide plugin <= 2.6 at WordPress.	6.5	More Details
CVE-2022-41254	Missing permission checks in Jenkins CONS3RT Plugin 1.0.0 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-41250	A missing permission check in Jenkins SCM HttpClient Plugin 1.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-41246	A missing permission check in Jenkins Worksoft Execution Manager Plugin 10.0.3.503 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2021-41437	An HTTP response splitting attack in web application in ASUS RT-AX88U before v3.0.0.4.388.20558 allows an attacker to craft a specific URL that if an authenticated victim visits it, the URL will give access to the cloud storage of the attacker.	6.5	More Details
CVE-2022-38512	The Translation module in Liferay Portal v7.4.3.12 through v7.4.3.36, and Liferay DXP 7.4 update 8 through 36 does not check permissions before allowing a user to export a web content for translation, allowing attackers to download a web content page's XLIFF translation file via crafted URL.	6.5	More Details
CVE-2022-40816	Zammad 5.2.1 is vulnerable to Incorrect Access Control. Zammad's asset handling mechanism has logic to ensure that customer users are not able to see personal information of other users. This logic was not effective when used through a web socket connection, so that a logged-in attacker would be able to fetch personal data of other users by querying the Zammad API. This issue is fixed in , 5.2.2.	6.5	More Details
CVE-2022-35021	OTFCC commit 617837b was discovered to contain a global buffer overflow via /release-x64/otfccdump+0x718693.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2937	The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Title & Description values that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.	6.4	More Details
CVE-2021-45035	Velneo vClient on its 28.1.3 version, does not correctly check the certificate of authenticity by default. This could allow an attacker that has access to the network to perform a MITM attack in order to obtain the user´s credentials.	6.3	More Details
CVE-2022-38061	Authenticated (author+) CSV Injection vulnerability in Export Post Info plugin <= 1.2.0 at WordPress.	6.2	More Details
CVE-2022-40754	In Apache Airflow 2.3.0 through 2.3.4, there was an open redirect in the webserver's `/confirm` endpoint.	6.1	More Details
CVE-2022-39239	netlify-ipx is an on-Demand image optimization for Netlify using ipx. In versions prior to 1.2.3, an attacker can bypass the source image domain allowlist by sending specially crafted headers, causing the handler to load and return arbitrary images. Because the response is cached globally, this image will then be served to visitors without requiring those headers to be set. XSS can be achieved by requesting a malicious SVG with embedded scripts, which would then be served from the site domain. Note that this does not apply to images loaded in `<img>` tags, as scripts do not execute in this context. The image URL can be set in the header independently of the request URL, meaning any site images that have not previously been cached can have their cache poisoned. This problem has been fixed in version 1.2.3. As a workaround, cached content can be cleared by re-deploying the site.	6.1	More Details
CVE-2022-41319	A Reflected Cross-Site Scripting (XSS) vulnerability affects the Veritas Desktop Laptop Option (DLO) application login page (aka the DLOServer/restore/login.jsp URI). This affects versions before 9.8 (e.g., 9.1 through 9.7).	6.1	More Details
CVE-2022-3062	The Simple File List WordPress plugin before 4.4.12 does not escape parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40088	Simple College Website v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /college_website/index.php?page=. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the page parameter.	6.1	More Details
CVE-2022-23458	Toast UI Grid is a component to display and edit data. Versions prior to 4.21.3 are vulnerable to cross-site scripting attacks when pasting specially crafted content into editable cells. This issue was fixed in version 4.21.3. There are no known workarounds.	6.1	More Details
CVE-2022-28979	Liferay Portal v7.1.0 through v7.4.2 and Liferay DXP 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 was discovered to contain a cross-site scripting (XSS) vulnerability in the Portal Search module's Custom Facet widget. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Parameter Name text field.	6.1	More Details
CVE-2022-28982	A cross-site scripting (XSS) vulnerability in Liferay Portal v7.3.3 through v7.4.2 and Liferay DXP v7.3 before service pack 3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name of a tag.	6.1	More Details
CVE-2022-28977	HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through 101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect.	6.1	More Details
CVE-2022-38553	Academy Learning Management System before v5.9.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Search parameter.	6.1	More Details
CVE-2022-28980	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal v7.4.3.4 and Liferay DXP v7.4 GA allows attackers to execute arbitrary web scripts or HTML via parameters with the filter_ prefix.	6.1	More Details
CVE-2022-39197	An XSS (Cross Site Scripting) vulnerability was found in HelpSystems Cobalt Strike through 4.7 that allowed a remote attacker to execute HTML on the Cobalt Strike teamserver. To exploit the vulnerability, one must first inspect a Cobalt Strike payload, and then modify the username field in the payload (or create a new payload with the extracted information and then modify that username field to be malformed).	6.1	More Details
CVE-2022-2266	University Library Automation System developed by Yordam Bilgi Teknolojileri before version 19.2 has an unauthenticated Reflected XSS vulnerability. This has been fixed in the version 19.2	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2404	The WP Popup Builder WordPress plugin before 1.2.9 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-40027	SourceCodester Simple Task Managing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component newTask.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the shortName parameter.	6.1	More Details
CVE-2022-40193	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability in Awesome Filterable Portfolio plugin <= 1.9.7 at WordPress.	6.1	More Details
CVE-2022-40359	Cross site scripting (XSS) vulnerability in kfm through 1.4.7 via crafted GET request to /kfm/index.php.	6.1	More Details
CVE-2022-36417	Multiple Stored Cross-Site Scripting (XSS) via Cross-Site Request Forgery (CSRF) vulnerability in 3D Tag Cloud plugin <= 3.8 at WordPress.	6.1	More Details
CVE-2022-35894	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an attacker-specified buffer, leading to information disclosure.	6.0	More Details
CVE-2022-35896	An issue SMM memory leak vulnerability in SMM driver (SMRAM was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An attacker can dump SMRAM contents via the software SMI provided by the FvbServicesRuntimeDxe driver to read the contents of SMRAM, leading to information disclosure.	6.0	More Details
CVE-2022-33683	Apache Pulsar Brokers and Proxies create an internal Pulsar Admin Client that does not verify peer TLS certificates, even when tlsAllowInsecureConnection is disabled via configuration. The Pulsar Admin Client's intra-cluster and geo-replication HTTPS connections are vulnerable to man in the middle attacks, which could leak authentication data, configuration data, and any other data sent by these clients. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. This issue affects Apache Pulsar Broker and Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33682	TLS hostname verification cannot be enabled in the Pulsar Broker's Java Client, the Pulsar Broker's Java Admin Client, the Pulsar WebSocket Proxy's Java Client, and the Pulsar Proxy's Admin Client leaving intra-cluster connections and geo-replication connections vulnerable to man in the middle attacks, which could leak credentials, configuration data, message data, and any other data sent by these clients. The vulnerability is for both the pulsar+ssl protocol and HTTPS. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. This issue affects Apache Pulsar Broker, Proxy, and WebSocket Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier.	5.9	More Details
CVE-2022-33681	Delayed TLS hostname verification in the Pulsar Java Client and the Pulsar Proxy make each client vulnerable to a man in the middle attack. Connections from the Pulsar Java Client to the Pulsar Broker/Proxy and connections from the Pulsar Proxy to the Pulsar Broker are vulnerable. Authentication data is sent before verifying the server’s TLS certificate matches the hostname, which means authentication data could be exposed to an attacker. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. Because the client sends authentication data before performing hostname verification, an attacker could gain access to the client’s authentication data. The client eventually closes the connection when it verifies the hostname and identifies the targeted hostname does not match a hostname on the certificate. Because the client eventually closes the connection, the value of the intercepted authentication data depends on the authentication method used by the client. Token based authentication and username/password authentication methods are vulnerable because the authentication data can be used to impersonate the client in a separate session. This issue affects Apache Pulsar Java Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier.	5.9	More Details
CVE-2022-32799	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. A user in a privileged network position may be able to leak sensitive information.	5.9	More Details
CVE-2022-41231	Jenkins Build-Publisher Plugin 1.22 and earlier allows attackers with Item/Configure permission to create or replace any config.xml file on the Jenkins controller file system by providing a crafted file name to an API endpoint.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35086	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via /multiarch/memmove-vec-unaligned-erms.S.	5.5	More Details
CVE-2022-26707	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in macOS Monterey 12.4. A user may be able to view sensitive user information.	5.5	More Details
CVE-2022-3278	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0552.	5.5	More Details
CVE-2022-35099	SWFTools commit 772e55a2 was discovered to contain a stack overflow via ImageStream::getPixel(unsigned char*) at /xpdf/Stream.cc.	5.5	More Details
CVE-2022-35098	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via GfxICCBasedColorSpace::getDefaultColor(GfxColor*) at /xpdf/GfxState.cc.	5.5	More Details
CVE-2022-32783	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4. An app may gain unauthorized access to Bluetooth.	5.5	More Details
CVE-2022-35097	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via FoFiTrueType::writeTTF at /xpdf/FoFiTrueType.cc.	5.5	More Details
CVE-2022-32785	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing an image may lead to a denial-of-service.	5.5	More Details
CVE-2022-35096	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via draw_stroke at /gfxpoly/stroke.c.	5.5	More Details
CVE-2022-35093	SWFTools commit 772e55a2 was discovered to contain a global buffer overflow via DCTStream::transformDataUnit at /xpdf/Stream.cc.	5.5	More Details
CVE-2022-35095	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via InfoOutputDev::type3D1 at /pdf/InfoOutputDev.cc.	5.5	More Details
CVE-2022-35094	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via DCTStream::readHuffSym(DCTHuffTable*) at /xpdf/Stream.cc.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35092	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via convert_gfxline at /gfxpoly/convert.c.	5.5	More Details
CVE-2022-35091	SWFTools commit 772e55a2 was discovered to contain a floating point exception (FPE) via DCTStream::readMCURow() at /xpdf/Stream.cc.ow()	5.5	More Details
CVE-2022-29799	A vulnerability was found in networkd-dispatcher. This flaw exists because no functions are sanitized by the OperationalState or the AdministrativeState of networkd-dispatcher. This attack leads to a directory traversal to escape from the “/etc/networkd-dispatcher” base directory.	5.5	More Details
CVE-2022-23951	In Keylime before 6.3.0, quote responses from the agent can contain possibly untrusted ZIP data which can lead to zip bombs.	5.5	More Details
CVE-2022-22423	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596.	5.5	More Details
CVE-2022-2881	The underlying bug might cause read past end of the buffer and either read memory it should not read, or crash the process.	5.5	More Details
CVE-2022-41218	In drivers/media/dvb-core/dmxdev.c in the Linux kernel through 5.19.10, there is a use-after-free caused by refcount races, affecting dvb_demux_open and dvb_dmxdev_release.	5.5	More Details
CVE-2022-35090	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via __asan_memcpy at /asan/asan_interceptors_memintrinsics.cpp:.	5.5	More Details
CVE-2022-35089	SWFTools commit 772e55a2 was discovered to contain a heap-buffer-overflow via getTransparentColor at /home/bupt/Desktop/swftools/src/gif2swf.	5.5	More Details
CVE-2022-35088	SWFTools commit 772e55a2 was discovered to contain a heap buffer-overflow via getGifDelayTime at /home/bupt/Desktop/swftools/src/src/gif2swf.c.	5.5	More Details
CVE-2022-35087	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via MovieAddFrame at /src/gif2swf.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32786	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2022-35085	SWFTools commit 772e55a2 was discovered to contain a memory leak via /lib/mem.c.	5.5	More Details
CVE-2022-32848	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to capture a user's screen.	5.5	More Details
CVE-2022-32805	The issue was addressed with improved handling of caches. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to access sensitive user information.	5.5	More Details
CVE-2022-32841	The issue was addressed with improved memory handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2022-32817	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-32800	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2022-32818	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.5. An app may be able to leak sensitive kernel state.	5.5	More Details
CVE-2022-32828	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-32825	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-32789	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.5. An app may be able to bypass Privacy preferences.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32849	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information.	5.5	More Details
CVE-2022-32823	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information.	5.5	More Details
CVE-2022-40103	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formSetAutoPing function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	5.5	More Details
CVE-2022-3025	The Bitcoin / Altcoin Faucet WordPress plugin through 1.6.0 does not have any CSRF check when saving its settings, allowing attacker to make a logged in admin change them via a CSRF attack. Furthermore, due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site Scripting issues	5.4	More Details
CVE-2022-40748	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236586.	5.4	More Details
CVE-2022-36791	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Awesome UG Torro Forms plugin <= 1.0.16 at WordPress.	5.4	More Details
CVE-2022-3024	The Simple Bitcoin Faucets WordPress plugin through 1.7.0 does not have any authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscribers to call it and add/delete/edit Bonds. Furthermore, due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site Scripting issues	5.4	More Details
CVE-2022-36388	Cross-Site Request Forgery (CSRF) vulnerability in YDS Support Ticket System plugin <= 1.0 at WordPress.	5.4	More Details
CVE-2022-38460	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in NOTICE BOARD plugin <= 1.1 at WordPress.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38438	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM.	5.4	More Details
CVE-2022-38079	Cross-Site Request Forgery (CSRF) vulnerability Backup Scheduler plugin <= 1.5.13 at WordPress.	5.4	More Details
CVE-2022-40358	An issue was discovered in AjaXplorer 4.2.3, allows attackers to cause cross site scripting vulnerabilities via a crafted svg file upload.	5.4	More Details
CVE-2022-37028	ISAMS 22.2.3.2 is prone to stored Cross-site Scripting (XSS) attack on the title field for groups, allowing an attacker to store a JavaScript payload that will be executed when another user uses the application.	5.4	More Details
CVE-2022-35721	IBM Jazz for Service Management 1.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 231380.	5.4	More Details
CVE-2022-38085	Cross-Site Request Forgery (CSRF) vulnerability in Read more By Adam plugin <= 1.1.8 at WordPress.	5.4	More Details
CVE-2022-35251	A cross-site scripting vulnerability exists in Rocket.chat <v5 due to style injection in the complete chat window, an adversary is able to manipulate not only the style of it, but will also be able to block functionality as well as hijacking the content of targeted users. Hence the payloads are stored in messages, it is a persistent attack vector, which will trigger as soon as the message gets viewed.	5.4	More Details
CVE-2022-28978	Stored cross-site scripting (XSS) vulnerability in the Site module's user membership administration page in Liferay Portal 7.0.1 through 7.4.1, and Liferay DXP 7.0 before fix pack 102, 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the a user's name.	5.4	More Details
CVE-2022-41240	Jenkins Walti Plugin 1.0.1 and earlier does not escape the information provided by the Walti API, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide malicious API responses from Walti.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38073	Multiple Authenticated (custom specific plugin role) Persistent Cross-Site Scripting (XSS) vulnerability in Awesome Support plugin <= 6.0.7 at WordPress.	5.4	More Details
CVE-2022-38335	Vtiger CRM v7.4.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the e-mail template modules.	5.4	More Details
CVE-2022-36383	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in WHA Word Search Puzzles game plugin <= 2.0.1 at WordPress.	5.4	More Details
CVE-2022-36365	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in WHA Crossword plugin <= 1.1.10 at WordPress.	5.4	More Details
CVE-2022-2872	Unrestricted Upload of File with Dangerous Type in GitHub repository octoprint/octoprint prior to 1.8.3.	5.4	More Details
CVE-2022-40219	Cross-Site Request Forgery (CSRF) vulnerability in SedLex FavIcon Switcher plugin <= 1.2.11 at WordPress allows plugin settings change.	5.4	More Details
CVE-2022-41242	A missing permission check in Jenkins extreme-feedback Plugin 1.7 and earlier allows attackers with Overall/Read permission to discover information about job names attached to lamps, discover MAC and IP addresses of existing lamps, and rename lamps.	5.4	More Details
CVE-2022-38975	DOM-based cross-site scripting vulnerability in EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.1.2) allows a remote attacker to inject an arbitrary script by having an administrative user of the product to visit a specially crafted page.	5.4	More Details
CVE-2022-41239	Jenkins DotCi Plugin 2.40.00 and earlier does not escape the GitHub user name parameter provided to commit notifications when displaying them in a build cause, resulting in a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-40044	Centreon v20.10.18 was discovered to contain a cross-site scripting (XSS) vulnerability via the esc_name (Escalation Name) parameter at Configuration/Notifications/Escalations. This vulnerability allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	5.4	More Details
CVE-2022-40132	Cross-Site Request Forgery (CSRF) vulnerability in Seriously Simple Podcasting plugin <= 2.16.0 at WordPress, leading to plugin settings change.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37330	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WHA Crossword plugin <= 1.1.10 at WordPress.	5.4	More Details
CVE-2022-36798	Cross-Site Request Forgery (CSRF) vulnerability in Topdigitaltrends Mega Addons For WPBakery Page Builder plugin <= 4.2.7 at WordPress.	5.4	More Details
CVE-2022-38704	Cross-Site Request Forgery (CSRF) vulnerability in SEO Redirection plugin <= 8.9 at WordPress, leading to deletion of 404 errors and redirection history.	5.4	More Details
CVE-2022-39240	MyGraph is a permission management system. Versions prior to 1.0.4 are vulnerable to a storage XSS vulnerability leading to Remote Code Execution. This issue is patched in version 1.0.4. There is no known workaround.	5.4	More Details
CVE-2022-23461	Jodit Editor is a WYSIWYG editor written in pure TypeScript without the use of additional libraries. Jodit Editor is vulnerable to XSS attacks when pasting specially constructed input. This issue has not been fully patched. There are no known workarounds.	5.4	More Details
CVE-2022-37246	Craft CMS 4.2.0.1 is affected by Cross Site Scripting (XSS) in the file src/web/assets/cp/src/js/BaseElementSelectInput.js and in specific on the line label: elementInfo.label.	5.4	More Details
CVE-2022-41224	Jenkins 2.367 through 2.369 (both inclusive) does not escape tooltips of the l:helpIcon UI component used for some help icons on the Jenkins web UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control tooltips for this component.	5.4	More Details
CVE-2022-41225	Jenkins Anchore Container Image Scanner Plugin 1.0.24 and earlier does not escape content provided by the Anchore engine API, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control API responses by Anchore engine.	5.4	More Details
CVE-2022-38095	Cross-Site Request Forgery (CSRF) vulnerability in AlgolPlus Advanced Dynamic Pricing for WooCommerce plugin <= 4.1.3 at WordPress.	5.4	More Details
CVE-2022-30003	Sourcecodester Online Market Place Site 1.0 is vulnerable to Cross Site Scripting (XSS), allowing attackers to register as a Seller then create new products containing XSS payloads in the 'Product Title' and 'Short Description' fields.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41229	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.134 and earlier does not escape configuration options of the Execute NetStorm/NetCloud Test build step, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-38439	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM.	5.4	More Details
CVE-2022-1755	The SVG Support WordPress plugin before 2.5 does not properly handle SVG added via an URL, which could allow users with a role as low as author to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2022-3201	Insufficient validation of untrusted input in DevTools in Google Chrome on Chrome OS prior to 105.0.5195.125 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: High)	5.4	More Details
CVE-2022-38454	Cross-Site Request Forgery (CSRF) vulnerability in Kraken.io Image Optimizer plugin <= 2.6.5 at WordPress.	5.4	More Details
CVE-2022-3250	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository ikus060/rdiffweb prior to 2.4.6.	5.3	More Details
CVE-2022-35621	Access control vulnerability in Evoh NFT EvohClaimable contract with sha256 hash code fa2084d5abca91a62ed1d2f1cad3ec318e6a9a2d7f1510a00d898737b05f48ae allows remote attackers to execute fraudulent NFT transfers.	5.3	More Details
CVE-2022-39835	An issue was discovered in Gajim through 1.4.7. The vulnerability allows attackers, via crafted XML stanzas, to correct messages that were not sent by them. The attacker needs to be part of the group chat or single chat. The fixed version is 1.5.0.	5.3	More Details
CVE-2022-1613	The Restricted Site Access WordPress plugin before 7.3.2 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based limitations in certain situations.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39242	Frontier is an Ethereum compatibility layer for Substrate. Prior to commit d3beddc6911a559a3ecc9b3f08e153dbe37a8658, the worst case weight was always accounted as the block weight for all cases. In case of large EVM gas refunds, this can lead to block spamming attacks -- the adversary can construct blocks with transactions that have large amount of refunds or unused gases with reverts, and as a result inflate up the chain gas prices. The impact of this issue is limited in that the spamming attack would still be costly for any adversary, and it has no ability to alter any chain state. This issue has been patched in commit d3beddc6911a559a3ecc9b3f08e153dbe37a8658. There are no known workarounds.	5.3	More Details
CVE-2022-2795	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.	5.3	More Details
CVE-2022-40194	Unauthenticated Sensitive Information Disclosure vulnerability in Customer Reviews for WooCommerce plugin <= 5.3.5 at WordPress	5.3	More Details
CVE-2022-41235	Jenkins WildFly Deployer Plugin 1.0.2 and earlier implements functionality that allows agent processes to read arbitrary files on the Jenkins controller file system.	5.3	More Details
CVE-2021-39190	The SCCM plugin for GLPI is a plugin to synchronize computers from SCCM (version 1802) to GLPI. In versions prior to 2.3.0, the Configuration page is publicly accessible in read-only mode. This issue is patched in version 2.3.0. No known workarounds exist.	5.3	More Details
CVE-2022-3251	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository ikus060/minarca prior to 4.2.2.	5.3	More Details
CVE-2022-40443	An absolute path traversal vulnerability in ZZCMS 2022 allows attackers to obtain sensitive information via a crafted GET request sent to /one/siteinfo.php.	5.3	More Details
CVE-2022-38648	Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to fetch external resources. This issue affects Apache XML Graphics Batik 1.14.	5.3	More Details
CVE-2022-41248	Jenkins BigPanda Notifier Plugin 1.4.0 and earlier does not mask the BigPanda API key on the global configuration form, increasing the potential for attackers to observe and capture it.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38398	Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to load a url thru the jar protocol. This issue affects Apache XML Graphics Batik 1.14.	5.3	More Details
CVE-2022-40444	ZZCMS 2022 was discovered to contain a full path disclosure vulnerability via the page /admin/index.PHP? _server.	5.3	More Details
CVE-2022-32217	A cleartext storage of sensitive information exists in Rocket.Chat <v4.6.4 due to Oauth token being leaked in plaintext in Rocket.chat logs.	5.3	More Details
CVE-2022-2926	The Download Manager WordPress plugin before 3.2.55 does not validate one of its settings, which could allow high privilege users such as admin to list and read arbitrary files and folders outside of the blog directory	4.9	More Details
CVE-2022-40028	SourceCodester Simple Task Managing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component newProjectValidation.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the fullName parameter.	4.8	More Details
CVE-2022-3255	If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can: Perform any action within the application that the user can perform. View any information that the user is able to view. Modify any information that the user is able to modify. Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user.	4.8	More Details
CVE-2022-37342	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability Add Shortcodes Actions And Filters plugin <= 2.0.9 at WordPress.	4.8	More Details
CVE-2022-3070	The Generate PDF WordPress plugin before 3.6 does not sanitise 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-2022-3069	The WordLift WordPress plugin before 3.37.2 does not sanitise 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-2022-3135	The SEO Smart Links WordPress plugin through 3.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40195	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PCA Predict plugin <= 1.0.3 at WordPress.	4.8	More Details
CVE-2022-3074	The Slider Hero WordPress plugin before 8.4.4 does not escape the slider Name, which could allow high-privileged users to perform Cross-Site Scripting attacks.	4.8	More Details
CVE-2022-40672	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CPO Shortcodes plugin <= 1.5.0 at WordPress.	4.8	More Details
CVE-2022-40029	SourceCodester Simple Task Managing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component newProjectValidation.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the shortName parameter.	4.8	More Details
CVE-2021-27853	Layer 2 network filtering capabilities such as IPv6 RA guard or ARP inspection can be bypassed using combinations of VLAN 0 headers and LLC/SNAP headers.	4.7	More Details
CVE-2021-27862	Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length and Ethernet to Wifi frame conversion (and optionally VLAN0 headers).	4.7	More Details
CVE-2021-27854	Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using combinations of VLAN 0 headers, LLC/SNAP headers, and converting frames from Ethernet to Wifi and its reverse.	4.7	More Details
CVE-2022-29800	A time-of-check-time-of-use (TOCTOU) race condition vulnerability was found in networkd-dispatcher. This flaw exists because there is a certain time between the scripts being discovered and them being run. An attacker can abuse this vulnerability to replace scripts that networkd-dispatcher believes to be owned by root with ones that are not.	4.7	More Details
CVE-2021-27861	Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length (and optionally VLAN0 headers)	4.7	More Details
CVE-2022-3303	A race condition flaw was found in the Linux kernel sound subsystem due to improper locking. It could lead to a NULL pointer dereference while handling the SNDCTL_DSP_SYNC ioctl. A privileged local user (root or member of the audio group) could use this flaw to crash the system, resulting in a denial of service condition	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32782	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4. An app with root privileges may be able to access private information.	4.4	More Details
CVE-2022-32781	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An app with root privileges may be able to access private information.	4.4	More Details
CVE-2022-3144	The Wordfence Security – Firewall & Malware Scan plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 7.6.0 via a setting on the options page due to insufficient escaping on the stored value. This makes it possible for authenticated users, with administrative privileges, to inject malicious web scripts into the setting that executes whenever a user accesses a page displaying the affected setting on sites running a vulnerable version.	4.4	More Details
CVE-2022-2888	If an attacker comes into the possession of a victim's OctoPrint session cookie through whatever means, the attacker can use this cookie to authenticate as long as the victim's account exists.	4.4	More Details
CVE-2022-40979	In JetBrains TeamCity before 2022.04.4 environmental variables of "password" type could be logged when using custom Perforce executable	4.4	More Details
CVE-2022-40671	Cross-Site Request Forgery (CSRF) vulnerability in Rate my Post – WP Rating System plugin <= 3.3.4 at WordPress.	4.3	More Details
CVE-2022-40817	Zammad 5.2.1 has a fine-grained permission model that allows to configure read-only access to tickets. However, agents were still wrongly able to perform some operations on such tickets, like adding and removing links, tags. and related answers. This issue has been fixed in 5.2.2.	4.3	More Details
CVE-2022-40310	Authenticated (subscriber+) Race Condition vulnerability in Rate my Post – WP Rating System plugin <= 3.3.4 at WordPress allows attackers to increase/decrease votes.	4.3	More Details
CVE-2022-23464	Nepxion Discovery is a solution for Spring Cloud. Discovery is vulnerable to a potential Server-Side Request Forgery (SSRF). RouterResourceImpl uses RestTemplate’s getForEntity to retrieve the contents of a URL containing user-controlled input, potentially resulting in Information Disclosure. There is no patch available for this issue at time of publication. There are no known workarounds.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3233	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.6.	4.3	More Details
CVE-2022-35246	A NoSQL-Injection information disclosure vulnerability vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 in the getS3FileUrl Meteor server method that can disclose arbitrary file upload URLs to users that should not be able to access.	4.3	More Details
CVE-2022-32229	A information disclosure vulnerability exists in Rockert.Chat <v5 due to /api/v1/chat.getThreadsList lack of sanitization of user inputs and can therefore leak private thread messages to unauthorized users via Mongo DB injection.	4.3	More Details
CVE-2022-32228	An information disclosure vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 since the getReadReceipts Meteor server method does not properly filter user inputs that are passed to MongoDB queries, allowing $regex queries to enumerate arbitrary Message IDs.	4.3	More Details
CVE-2022-32226	An improper access control vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 due to input data in the getUsersOfRoom Meteor server method is not type validated, so that MongoDB query operator objects are accepted by the server, so that instead of a matching rid String a$regex query can be executed, bypassing the room access permission check for every but the first matching room.	4.3	More Details
CVE-2022-41230	Jenkins Build-Publisher Plugin 1.22 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to obtain names and URLs of Jenkins servers that the plugin is configured to publish builds to, as well as builds pending for publication to those Jenkins servers.	4.3	More Details
CVE-2022-32219	An information disclosure vulnerability exists in Rocket.Chat <v4.7.5 which allowed the "users.list" REST endpoint gets a query parameter from JSON and runs Users.find(queryFromClientSide). This means virtually any authenticated user can access any data (except password hashes) of any user authenticated.	4.3	More Details
CVE-2022-41233	Jenkins Rundeck Plugin 3.6.11 and earlier does not perform Run/Artifacts permission checks in multiple HTTP endpoints, allowing attackers with Item/Read permission to obtain information about build artifacts of a given job, if the optional Run/Artifacts permission is enabled.	4.3	More Details
CVE-2022-32218	An information disclosure vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 due to the actionLinkHandler method was found to allow Message ID Enumeration with Regex MongoDB queries.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28886	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.so/aerdl.dll may go into an infinite loop when unpacking PE files. It is possible that this can crash the scanning engine	4.3	More Details
CVE-2022-35250	A privilege escalation vulnerability exists in Rocket.chat <v5 which made it possible to elevate privileges for any authenticated user to view Direct messages without appropriate permissions.	4.3	More Details
CVE-2022-39975	The Layout module in Liferay Portal v7.3.3 through v7.4.3.34, and Liferay DXP 7.3 before update 10, and 7.4 before update 35 does not check user permission before showing the preview of a "Content Page" type page, allowing attackers to view unpublished "Content Page" pages via URL manipulation.	4.3	More Details
CVE-2022-2405	The WP Popup Builder WordPress plugin before 1.2.9 does not have authorisation and CSRF check in an AJAX action, allowing any authenticated users, such as subscribers to delete arbitrary Popup	4.3	More Details
CVE-2022-35247	A information disclosure vulnerability exists in Rocket.chat <v5, <v4.8.2 and <v4.7.5 where the lack of ACL checks in the getRoomRoles Meteor method leak channel members with special roles to unauthorized clients.	4.3	More Details
CVE-2022-39225	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.15, or 5.0.0 and above prior to 5.2.6, a user can write to the session object of another user if the session object ID is known. For example, an attacker can assign the session object to their own user by writing to the `user` field and then read any custom fields of that session object. Note that assigning a session to another user does not usually change the privileges of either of the two users, and a user cannot assign their own session to another user. This issue is patched in version 4.10.15 and above, and 5.2.6 and above. To mitigate this issue in unpatched versions add a `beforeSave` trigger to the `_Session` class and prevent writing if the requesting user is different from the user in the session object.	4.3	More Details
CVE-2022-41247	Jenkins BigPanda Notifier Plugin 1.4.0 and earlier stores the BigPanda API key unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2022-3098	The Login Block IPs WordPress plugin through 1.0.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3299	A vulnerability was found in Open5GS up to 2.4.10. It has been declared as problematic. Affected by this vulnerability is an unknown functionality in the library lib/sbi/client.c of the component AMF. The manipulation leads to denial of service. The attack can be launched remotely. The name of the patch is 724fa568435dae45ef0c3a48b2aabde052afae88. It is recommended to apply a patch to fix this issue. The identifier VDB-209545 was assigned to this vulnerability.	4.3	More Details
CVE-2022-41251	A missing permission check in Jenkins Apprenda Plugin 2.2.0 and earlier allows users with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-35249	A information disclosure vulnerability exists in Rocket.Chat <v5 where the getUserMentionsByChannel meteor server method discloses messages from private channels and direct messages regardless of the users access permission to the room.	4.3	More Details
CVE-2022-41252	Missing permission checks in Jenkins CONS3RT Plugin 1.0.0 and earlier allows users with Overall/Read permission to enumerate credentials ID of credentials stored in Jenkins.	4.3	More Details
CVE-2022-38134	Authenticated (subscriber+) Broken Access Control vulnerability in Customer Reviews for WooCommerce plugin <= 5.3.5 at WordPress.	4.3	More Details
CVE-2022-3053	Inappropriate implementation in Pointer Lock in Google Chrome on Mac prior to 105.0.5195.52 allowed a remote attacker to restrict user navigation via a crafted HTML page.	4.3	More Details
CVE-2022-38470	Cross-Site Request Forgery (CSRF) vulnerability in Customer Reviews for WooCommerce plugin <= 5.3.5 at WordPress.	4.3	More Details
CVE-2022-3267	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.6.	4.3	More Details
CVE-2022-39238	Arvados is an open source platform for managing and analyzing biomedical big data. In versions prior to 2.4.3, when using Portable Authentication Modules (PAM) for user authentication, if a user presented valid credentials but the account is disabled or otherwise not allowed to access the host (such as an expired password), it would still be accepted for access to Arvados. Other authentication methods (LDAP, OpenID Connect) supported by Arvados are not affected by this flaw. This issue is patched in version 2.4.3. Workaround for this issue is to migrate to a different authentication method supported by Arvados, such as LDAP.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36390	Authenticated (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Totalsoft Event Calendar – Calendar plugin <= 1.4.6 at WordPress.	4.1	More Details
CVE-2022-40213	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in GS Testimonial Slider plugin <= 1.9.6 at WordPress.	4.1	More Details
CVE-2022-37338	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in Blossom Recipe Maker plugin <= 1.0.7 at WordPress.	4.1	More Details
CVE-2022-37339	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Meet My Team plugin <= 2.0.5 at WordPress.	4.1	More Details
CVE-2022-31679	Applications that allow HTTP PATCH access to resources exposed by Spring Data REST in versions 3.6.0 - 3.5.5, 3.7.0 - 3.7.2, and older unsupported versions, if an attacker knows about the structure of the underlying domain model, they can craft HTTP requests that expose hidden entity attributes.	3.7	More Details
CVE-2022-39231	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.16, or from 5.0.0 to 5.2.6, validation of the authentication adapter app ID for _Facebook_ and _Spotify_ may be circumvented. Configurations which allow users to authenticate using the Parse Server authentication adapter where `appIds` is set as a string instead of an array of strings authenticate requests from an app with a different app ID than the one specified in the `appIds` configuration. For this vulnerability to be exploited, an attacker needs to be assigned an app ID by the authentication provider which is a sub-set of the server-side configured app ID. This issue is patched in versions 4.10.16 and 5.2.7. There are no known workarounds.	3.7	More Details
CVE-2022-35252	When curl is used to retrieve and parse cookies from a HTTP(S) server, itaccepts cookies using control codes that when later are sent back to a HTTPserver might make the server return 400 responses. Effectively allowing a"sister site" to deny service to all siblings.	3.7	More Details
CVE-2022-3274	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.7.	3.5	More Details
CVE-2022-38703	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Max Foundry Button Plugin MaxButtons plugin <= 9.2 at WordPress	3.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40215	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities in Tabs plugin <= 3.7.1 at WordPress.	3.4	More Details
CVE-2022-37328	Authenticated (author+) Stored Cross-Site Scripting (XSS) vulnerability in Themes Awesome History Timeline plugin <= 1.0.5 at WordPress.	3.4	More Details
CVE-2019-5641	Rapid7 InsightVM suffers from an information exposure issue whereby, when the user's session has ended due to inactivity, an attacker can use the Inspect Element browser feature to remove the login panel and view the details available in the last webpage visited by previous user	3.3	More Details
CVE-2022-3257	Mattermost version 7.1.x and earlier fails to sufficiently process a specifically crafted GIF file when it is uploaded while drafting a post, which allows authenticated users to cause resource exhaustion while processing the file, resulting in server-side Denial of Service.	3.1	More Details
CVE-2021-27774	User input included in error response, which could be used in a phishing attack.	3.1	More Details
CVE-2022-40199	Directory traversal vulnerability in EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p4) and EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.1.2) allows a remote authenticated attacker with an administrative privilege to obtain the product's directory structure information.	2.7	More Details
CVE-2022-3301	Improper Cleanup on Thrown Exception in GitHub repository ikus060/rdiffweb prior to 2.4.8.	2.4	More Details
CVE-2022-23006	A stack-based buffer overflow vulnerability was found on Western Digital My Cloud Home, My Cloud Home Duo, and SanDisk ibi that could allow an attacker accessing the system locally to read information from /etc/version file. This vulnerability can only be exploited by chaining it with another issue. If an attacker is able to carry out a remote code execution attack, they can gain access to the vulnerable file, due to the presence of insecure functions in code. User interaction is required for exploitation. Exploiting the vulnerability could result in exposure of information, ability to modify files, memory access errors, or system crashes.	1.8	More Details
CVE-2022-35253	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40669	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-40668	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-40667	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-40666	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-40665	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details