SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 August 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-2022-2310	An authentication bypass vulnerability in Skyhigh SWG in main releases 10.x prior to 10.2.12, 9.x prior to 9.2.23, 8.x prior to 8.2.28, and controlled release 11.x prior to 11.2.1 allows a remote attacker to bypass authentication into the administration User Interface. This is possible because of SWG incorrectly whitelisting authentication bypass methods and using a weak crypto password. This can lead to the attacker logging into the SWG admin interface, without valid credentials, as the super user with complete control over the SWG.	10.0	More Details
CVE-2021-41556	sqclass.cpp in Squirrel through 2.2.5 and 3.x through 3.1 allows an out-of-bounds read (in the core interpreter) that can lead to Code Execution. If a victim executes an attacker-controlled squirrel script, it is possible for the attacker to break out of the squirrel script sandbox even if all dangerous functionality such as File System functions has been disabled. An attacker might abuse this bug to target (for example) Cloud services that allow customization via SquirrelScripts, or distribute malware through video games that embed a Squirrel Engine.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2595	Improper Authorization in GitHub repository kromitgmbh/titra prior to 0.79.1.	10.0	More Details
CVE-2022-22683	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in cgi component in Synology Media Server before 1.8.1-2876 allows remote attackers to execute arbitrary code via unspecified vectors.	10.0	More Details
CVE-2022-36954	In Veritas NetBackup OpsCenter, under specific conditions, an authenticated remote attacker may be able to create or modify OpsCenter user accounts. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	9.9	More Details
CVE-2022-36992	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely execute arbitrary commands on a NetBackup Primary server (in specific notify conditions).	9.9	More Details
CVE-2022-31180	Shescape is a simple shell escape package for JavaScript. Affected versions were found to have insufficient escaping of white space when interpolating output. This issue only impacts users that use the `escape` or `escapeAll` functions with the `interpolation` option set to `true`. The result is that if an attacker is able to include whitespace in their input they can: 1. Invoke shell-specific behaviour through shell-specific special characters inserted directly after whitespace. 2. Invoke shell-specific behaviour through shell-specific special characters inserted or appearing after line terminating characters. 3. Invoke arbitrary commands by inserting a line feed character. 4. Invoke arbitrary commands by inserting a carriage return character. Behaviour number 1 has been patched in [v1.5.7] which you can upgrade to now. No further changes are required. Behaviour number 2, 3, and 4 have been patched in [v1.5.8] which you can upgrade to now. No further changes are required. The best workaround is to avoid having to use the `interpolation: true` option - in most cases using an alternative is possible, see [the recipes] (https://github.com/ericcornelissen/shescape#recipes) for recommendations. Alternatively, users may strip all whitespace from user input. Note that this is error prone, for example: for PowerShell this requires stripping `'\u0085'` which is not included in JavaScript's definition of `\s` for Regular Expressions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31181	PrestaShop is an Open Source e-commerce platform. In versions from 1.6.0.10 and before 1.7.8.7 PrestaShop is subject to an SQL injection vulnerability which can be chained to call PHP's Eval function on attacker input. The problem is fixed in version 1.7.8.7. Users are advised to upgrade. Users unable to upgrade may delete the MySQL Smarty cache feature.	9.8	More Details
CVE-2022-34945	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getproductreport.php.	9.8	More Details
CVE-2022-34946	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getexpproduct.php.	9.8	More Details
CVE-2022-34947	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editcategory.php.	9.8	More Details
CVE-2022-34948	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editbrand.php.	9.8	More Details
CVE-2022-34949	Pharmacy Management System v1.0 was discovered to contain multiple SQL injection vulnerabilities via the email or password parameter at login.php.	9.8	More Details
CVE-2022-34950	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editproduct.php.	9.8	More Details
CVE-2022-34951	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getsalereport.php.	9.8	More Details
CVE-2022-34953	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getOrderReport.php.	9.8	More Details
CVE-2022-34952	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at edituser.php.	9.8	More Details
CVE-2022-23100	OX App Suite through 7.10.6 allows OS Command Injection via Documentconverter (e.g., through an email attachment).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34954	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at invoiceprint.php.	9.8	More Details
CVE-2022-34955	Pligg CMS v2.0.2 was discovered to contain a time-based SQL injection vulnerability via the page_size parameter at load_data_for_topusers.php.	9.8	More Details
CVE-2022-34956	Pligg CMS v2.0.2 was discovered to contain a time-based SQL injection vulnerability via the page_size parameter at load_data_for_groups.php.	9.8	More Details
CVE-2022-35422	Web Based Quiz System v1.0 was discovered to contain a SQL injection vulnerability via the qid parameter at update.php.	9.8	More Details
CVE-2020-28423	This affects all versions of package monorepo-build.	9.8	More Details
CVE-2020-28451	This affects the package image-tiler before 2.0.2.	9.8	More Details
CVE-2022-34613	Mealie 1.0.0beta3 contains an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted file.	9.8	More Details
CVE-2022-35223	EasyUse MailHunter Ultimate's cookie deserialization function has an inadequate validation vulnerability. Deserializing a cookie containing malicious payload will trigger this insecure deserialization vulnerability, allowing an unauthenticated remote attacker to execute arbitrary code, manipulate system command or interrupt service.	9.8	More Details
CVE-2022-29807	A SQL injection vulnerability exists within Quest KACE Systems Management Appliance (SMA) through 12.0 that can allow for remote code execution via download_agent_installer.php.	9.8	More Details
CVE-2022-36301	BF-OS version 3.x up to and including 3.83 do not enforce strong passwords which may allow a remote attacker to brute-force the device password.	9.8	More Details
CVE-2022-26437	In httpclient, there is a possible out of bounds write due to uninitialized data. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WSAP00103831; Issue ID: WSAP00103831.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2317	The Simple Membership WordPress plugin before 4.1.3 allows user to change their membership at the registration stage due to insufficient checking of a user supplied parameter.	9.8	More Details
CVE-2022-34558	WMAgent v1.3.3rc2 and 1.3.3rc1, reqmgr 2 1.4.1rc5 and 1.4.0rc2, reqmon 1.4.1rc5, and global-workqueue 1.4.1rc5 allows attackers to execute arbitrary code via a crafted dbs-client package.	9.8	More Details
CVE-2022-24405	OX App Suite through 7.10.6 allows OS Command Injection via a serialized Java class to the Documentconverter API.	9.8	More Details
CVE-2022-36950	In Veritas NetBackup OpsCenter, an unauthenticated remote attacker may be able to perform remote command execution through a Java classloader manipulation. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	9.8	More Details
CVE-2022-36951	In Veritas NetBackup OpsCenter, an unauthenticated remote attacker may compromise the host by exploiting an incorrectly patched vulnerability. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30315	Honeywell Experion PKS Safety Manager (SM and FSC) through 2022-05-06 has Insufficient Verification of Data Authenticity. According to FSCT-2022-0053, there is a Honeywell Experion PKS Safety Manager insufficient logic security controls issue. The affected components are characterized as: Honeywell FSC runtime (FSC-CPU, QPP), Honeywell Safety Builder. The potential impact is: Remote Code Execution, Denial of Service. The Honeywell Experion PKS Safety Manager family of safety controllers utilize the unauthenticated Safety Builder protocol (FSCT-2022-0051) for engineering purposes, including downloading projects and control logic to the controller. Control logic is downloaded to the controller on a block-by-block basis. The logic that is downloaded consists of FLD code compiled to native machine code for the CPU module (which applies to both the Safety Manager and FSC families). Since this logic does not seem to be cryptographically authenticated, it allows an attacker capable of triggering a logic download to execute arbitrary machine code on the controller's CPU module in the context of the runtime. While the researchers could not verify this in detail, the researchers believe that the microprocessor underpinning the FSC and Safety Manager CPU modules is incapable of offering memory protection or privilege separation capabilities which would give an attacker full control of the CPU module. There is no authentication on control logic downloaded to the controller. Memory protection and privilege separation capabilities for the runtime are possibly lacking. The researchers confirmed the issues in question on Safety Manager R145.1 and R152.2 but suspect the issue affects all FSC and SM controllers and associated Safety Builder versions regardless of software or firmware revision. An attacker who can communicate with a Safety Manager controller via the Safety Builder protocol can execute arbitrary code without restrictions on the CPU module, allowing for covert manipulation of control operations and implanting capabilities similar to the TRITON malware (MITRE ATT&CK software ID S1009). A mitigating factor with regards to some, but not all, of the above functionality is that these require the Safety Manager physical keyswitch to be in the right position.	9.8	More Details
CVE-2022-1950	The Youzify WordPress plugin before 1.2.0 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to an unauthenticated SQL injection	9.8	More Details
CVE-2022-2564	Prototype Pollution in GitHub repository automattic/mongoose prior to 6.4.6.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34555	TP-LINK TL-R473G 2.0.1 Build 220529 Rel.65574n was discovered to contain a remote code execution vulnerability which is exploited via a crafted packet.	9.8	More Details
CVE-2016-4991	Input passed to the Pdf() function is shell escaped and passed to child_process.exec() during PDF rendering. However, the shell escape does not properly encode all special characters, namely, semicolon and curly braces. This can be abused to achieve command execution. This problem affects nodepdf 1.3.0.	9.8	More Details
CVE-2022-30285	In Quest KACE Systems Management Appliance (SMA) through 12.0, a hash collision is possible during authentication. This may allow authentication with invalid credentials.	9.8	More Details
CVE-2022-22280	Improper Neutralization of Special Elements used in an SQL Command leading to Unauthenticated SQL Injection vulnerability, impacting SonicWall GMS 9.3.1-SP2-Hotfix1, Analytics On-Prem 2.5.0.3-2520 and earlier versions.	9.8	More Details
CVE-2022-34496	Hiby R3 PRO firmware v1.5 to v1.7 was discovered to contain a file upload vulnerability via the file upload feature.	9.8	More Details
CVE-2022-34531	DedeCMS v5.7.95 was discovered to contain a remote code execution (RCE) vulnerability via the component mytag_ main.php.	9.8	More Details
CVE-2022-27255	In Realtek eCos RSDK 1.5.7p1 and MSDK 4.9.4p1, the SIP ALG function that rewrites SDP data has a stack-based buffer overflow. This allows an attacker to remotely execute code without authentication via a crafted SIP packet that contains malicious SDP data.	9.8	More Details
CVE-2022-30083	EllieGrid Android Application version 3.4.1 is vulnerable to Code Injection. The application appears to evaluate user input as code (remote).	9.8	More Details
CVE-2022-36990	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely write arbitrary files to arbitrary locations from any Client to any other Client via a Primary server.	9.6	More Details
CVE-2022-1853	Use after free in Indexed DB in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1277	Inavitas Solar Log product has an unauthenticated SQL Injection vulnerability.	9.4	More Details
CVE-2020-28434	This affects all versions of package gitblame. The injection point is located in line 15 in lib/gitblame.js.	9.4	More Details
CVE-2020-28437	This affects all versions of package heroku-env. The injection point is located in lib/get.js which is required by index.js.	9.4	More Details
CVE-2020-28453	This affects all versions of package npos-tesseract. The injection point is located in line 55 in lib/ocr.js.	9.4	More Details
CVE-2022-36949	In Veritas NetBackup OpsCenter, an attacker with local access to a NetBackup OpsCenter server could potentially escalate their privileges. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	9.3	More Details
CVE-2022-2010	Out of bounds read in compositing in Google Chrome prior to 102.0.5005.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35924	NextAuth.js is a complete open source authentication solution for Next.js applications. `next-auth` users who are using the `EmailProvider` either in versions before `4.10.3` or `3.29.10` are affected. If an attacker could forge a request that sent a comma-separated list of emails (eg.: `attacker@attacker.com,victim@victim.com`) to the sign-in endpoint, NextAuth.js would send emails to both the attacker and the victim's e-mail addresses. The attacker could then login as a newly created user with the email being `attacker@attacker.com,victim@victim.com`. This means that basic authorization like `email.endsWith("@victim.com")` in the `signIn` callback would fail to communicate a threat to the developer and would let the attacker bypass authorization, even with an `@attacker.com` address. This vulnerability has been patched in `v4.10.3` and `v3.29.10` by normalizing the email value that is sent to the sign-in endpoint before accessing it anywhere else. We also added a `normalizeIdentifier` callback on the `EmailProvider` configuration, where you can further tweak your requirements for what your system considers a valid e-mail address. (E.g.: strict RFC2821 compliance). Users are advised to upgrade. There are no known workarounds for this vulnerability. If for some reason you cannot upgrade, you can normalize the incoming request using Advanced Initialization.	9.1	More Details
CVE-2022-35643	IBM PowerVM VIOS 3.1 could allow a remote attacker to tamper with system configuration or cause a denial of service. IBM X-Force ID: 230956.	9.1	More Details
CVE-2022-31775	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228359.	9.1	More Details
CVE-2022-31183	fs2 is a compositional, streaming I/O library for Scala. When establishing a server-mode `TLSSocket` using `fs2-io` on Node.js, the parameter `requestCert = true` is ignored, peer certificate verification is skipped, and the connection proceeds. The vulnerability is limited to: 1. `fs2-io` running on Node.js. The JVM TLS implementation is completely independent. 2. `TLSSocket`s in server-mode. Client-mode `TLSSocket`s are implemented via a different API. 3. mTLS as enabled via `requestCert = true` in `TLSParameters`. The default setting is `false` for server-mode `TLSSocket`s. It was introduced with the initial Node.js implementation of fs2-io in 3.1.0. A patch is released in v3.2.11. The requestCert = true parameter is respected and the peer certificate is verified. If verification fails, a SSLException is raised. If using an unpatched version on Node.js, do not use a server-mode TLSSocket with requestCert = true to establish a mTLS connection.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31321	The foldername parameter in Bolt 5.1.7 was discovered to have incorrect input validation, allowing attackers to perform directory enumeration or cause a Denial of Service (DoS) via a crafted input.	9.1	More Details
CVE-2022-36956	In Veritas NetBackup, the NetBackup Client allows arbitrary command execution from any remote host that has access to a valid host-id NetBackup certificate/private key from the same domain. The affects 9.0.x through 9.0.0.1 and 9.1.x through 9.1.0.1.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-36364	Apache Calcite Avatica JDBC driver creates HTTP client instances based on class names provided via `httpclient_impl` connection property; however, the driver does not verify if the class implements the expected interface before instantiating it, which can lead to code execution loaded via arbitrary classes and in rare cases remote code execution. To exploit the vulnerability: 1) the attacker needs to have privileges to control JDBC connection parameters; 2) and there should be a vulnerable class (constructor with URL parameter and ability to execute code) in the classpath. From Apache Calcite Avatica 1.22.0 onwards, it will be verified that the class implements the expected interface before invoking its constructor.	8.8	More Details
CVE-2022-2415	Heap buffer overflow in WebGL in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2011	Use after free in ANGLE in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2156	Use after free in Core in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2157	Use after free in Interest groups in Google Chrome prior to 103.0.5060.53 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-2022-2158	Type confusion in V8 in Google Chrome prior to 103.0.5060.53 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-2022-2161	Use after free in WebApp Provider in Google Chrome prior to 103.0.5060.53 allowed a remote attacker who convinced the user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-2162	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 103.0.5060.53 allowed a remote attacker to bypass file system access via a crafted HTML page.	8.8	More Details
CVE-2022-36989	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely execute arbitrary commands on a NetBackup Primary server.	8.8	More Details
CVE-2022-2478	Use after free in PDF in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-36993	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely execute arbitrary commands on a NetBackup Primary server.	8.8	More Details
CVE-2022-2163	Use after free in Cast UI and Toolbar in Google Chrome prior to 103.0.5060.134 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via UI interaction.	8.8	More Details
CVE-2022-2294	Heap buffer overflow in WebRTC in Google Chrome prior to 103.0.5060.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2631	Improper Access Control in GitHub repository tooljet/tooljet prior to v1.19.0.	8.8	More Details
CVE-2022-2295	Type confusion in V8 in Google Chrome prior to 103.0.5060.114 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-2022-2296	Use after free in Chrome OS Shell in Google Chrome on Chrome OS prior to 103.0.5060.114 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via direct UI interactions.	8.8	More Details
CVE-2022-2008	Double free in WebGL in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2007	Use after free in WebGPU in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-36920	A cross-site request forgery (CSRF) vulnerability in Jenkins Coverity Plugin 1.11.4 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-2022-1919	Use after free in Codecs in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-1876	Heap buffer overflow in DevTools in Google Chrome prior to 102.0.5005.61 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-2022-1874	Insufficient policy enforcement in Safe Browsing in Google Chrome on Mac prior to 102.0.5005.61 allowed a remote attacker to bypass downloads protection policy via a crafted HTML page.	8.8	More Details
CVE-2022-1870	Use after free in App Service in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2022-1866	Use after free in Tablet Mode in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific user interactions.	8.8	More Details
CVE-2022-1865	Use after free in Bookmarks in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1864	Use after free in WebApp Installs in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.	8.8	More Details
CVE-2022-1863	Use after free in Tab Groups in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.	8.8	More Details
CVE-2022-1861	Use after free in Sharing in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to enage in specific user interactions to potentially exploit heap corruption via specific user interaction.	8.8	More Details
CVE-2022-1860	Use after free in UI Foundations in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific user interactions.	8.8	More Details
CVE-2022-1859	Use after free in Performance Manager in Google Chrome prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-1857	Insufficient policy enforcement in File System API in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to bypass file system restrictions via a crafted HTML page.	8.8	More Details
CVE-2022-1856	Use after free in User Education in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension or specific user interaction.	8.8	More Details
CVE-2022-1855	Use after free in Messaging in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2477	Use after free in Guest View in Google Chrome prior to 103.0.5060.134 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-2022-1854	Use after free in ANGLE in Google Chrome prior to 102.0.5005.61 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-2022-2480	Use after free in Service Worker API in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2481	Use after free in Views in Google Chrome prior to 103.0.5060.134 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via UI interaction.	8.8	More Details
CVE-2022-2550	OS Command Injection in GitHub repository hestiacp/hestiacp prior to 1.6.5.	8.8	More Details
CVE-2022-34557	Barangay Management System v1.0 was discovered to contain a SQL injection vulnerability via the hidden_id parameter at /pages/permit/permit.php.	8.8	More Details
CVE-2022-27864	A Double Free vulnerability allows remote attackers to execute arbitrary code through DesignReview.exe application on PDF files within affected installations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	8.8	More Details
CVE-2022-2323	Improper neutralization of special elements used in a user input allows an authenticated malicious user to perform remote code execution in the host system. This vulnerability impacts SonicWall Switch 1.1.1.0-2s and earlier versions	8.8	More Details
CVE-2022-34549	Sims v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /uploadServlet. This vulnerability allows attackers to escalate privileges and execute arbitrary commands via a crafted file.	8.8	More Details
CVE-2022-34527	D-Link DSL-3782 v1.03 and below was discovered to contain a command injection vulnerability via the function byte_4C0160.	8.8	More Details
CVE-2022-34528	D-Link DSL-3782 v1.03 and below was discovered to contain a stack overflow via the function getAttrValue.	8.8	More Details
CVE-2022-31776	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 228433.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34161	IBM CICS TX 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 229331.	8.8	More Details
CVE-2022-2184	The CAPTCHA 4WP WordPress plugin before 7.1.0 lets user input reach a sensitive require_once call in one of its admin-side templates. This can be abused by attackers, via a Cross-Site Request Forgery attack to run arbitrary code on the server.	8.8	More Details
CVE-2022-2245	The Counter Box WordPress plugin before 1.2.1 is lacking CSRF check when activating and deactivating counters, which could allow attackers to make a logged in admin perform such actions via CSRF attacks	8.8	More Details
CVE-2022-2273	The Simple Membership WordPress plugin before 4.1.3 does not properly validate the membership_level parameter when editing a profile, allowing members to escalate to a higher membership level by using a crafted POST request.	8.8	More Details
CVE-2022-36302	File path manipulation vulnerability in BF-OS version 3.00 up to and including 3.83 allows an attacker to modify the file path to access different resources, which may contain sensitive information.	8.8	More Details
CVE-2022-34971	An arbitrary file upload vulnerability in the Advertising Management module of Feehi CMS v2.1.1 allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-34567	An issue in \Roaming\Mango\Plugins of University of Texas Multi-image Analysis GUI (Mango) 4.1 allows attackers to escalate privileges via crafted plugins.	8.8	More Details
CVE-2022-2399	Use after free in WebGPU in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-36882	A cross-site request forgery (CSRF) vulnerability in Jenkins Git Plugin 4.11.3 and earlier allows attackers to trigger builds of jobs configured to use an attacker-specified Git repository and to cause them to check out an attacker-specified commit.	8.8	More Details
CVE-2022-29558	Realtek rtl819x-SDK before v3.6.1 allows command injection over the web interface.	8.8	More Details
CVE-2021-22648	Ovarro TBox proprietary Modbus file access functions allow attackers to read, alter, or delete the configuration file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22646	The “ipk” package containing the configuration created by TWinSoft can be uploaded, extracted, and executed in Ovarro TBox, allowing malicious code execution.	8.8	More Details
CVE-2022-36889	Jenkins Deployer Framework Plugin 85.v1d1888e8c021 and earlier does not restrict the application path of the applications when configuring a deployment, allowing attackers with Item/Configure permission to upload arbitrary files from the Jenkins controller file system to the selected service.	8.8	More Details
CVE-2022-1948	An issue has been discovered in GitLab affecting all versions starting from 15.0 before 15.0.1. Missing validation of input used in quick actions allowed an attacker to exploit XSS by injecting HTML in contact details.	8.7	More Details
CVE-2022-22685	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology WebDAV Server before 2.4.0-0062 allows remote authenticated users to delete arbitrary files via unspecified vectors.	8.7	More Details
CVE-2022-36986	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with unauthenticated access could remotely execute arbitrary commands on a NetBackup Primary server.	8.6	More Details
CVE-2022-31188	CVAT is an opensource interactive video and image annotation tool for computer vision. Versions prior to 2.0.0 were found to be subject to a Server-side request forgery (SSRF) vulnerability. Validation has been added to urls used in the affected code path in version 2.0.0. Users are advised to upgrade. There are no known workarounds for this issue.	8.6	More Details
CVE-2022-36987	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could arbitrarily write files to a NetBackup Primary server.	8.5	More Details
CVE-2022-36952	In Veritas NetBackup OpsCenter, a hard-coded credential exists that could be used to exploit the underlying VxSS subsystem. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	8.4	More Details
CVE-2022-35920	Sanic is an opensource python web server/framework. Affected versions of sanic allow access to lateral directories when using `app.static` if using encoded `%2F` URLs. Parent directory traversal is not impacted. Users are advised to upgrade. There is no known workaround for this issue.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27613	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in webapi component in Synology CardDAV Server before 6.0.10-0153 allows remote authenticated users to inject SQL commands via unspecified vectors.	8.3	More Details
CVE-2022-2313	A DLL hijacking vulnerability in the MA Smart Installer for Windows prior to 5.7.7, which allows local users to execute arbitrary code and obtain higher privileges via careful placement of a malicious DLL into the folder from where the Smart installer is being executed.	8.2	More Details
CVE-2022-31194	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI resumable upload implementations in SubmissionController and FileUploadRequest are vulnerable to multiple path traversal attacks, allowing an attacker to create files/directories anywhere on the server writable by the Tomcat/DSpace user, by modifying some request parameters during submission. This path traversal can only be executed by a user with special privileges (submitter rights). This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds. However, this vulnerability cannot be exploited by an anonymous user or a basic user. The user must first have submitter privileges to at least one Collection and be able to determine how to modify the request parameters to exploit the vulnerability.	8.2	More Details
CVE-2022-36900	Jenkins Compuware zAdviser API Plugin 1.0.3 and earlier does not restrict execution of a controller/agent message to agents, allowing attackers able to control agent processes to retrieve Java system properties.	8.2	More Details
CVE-2022-36899	Jenkins Compuware ISPW Operations Plugin 1.0.8 and earlier does not restrict execution of a controller/agent message to agents, allowing attackers able to control agent processes to retrieve Java system properties.	8.2	More Details
CVE-2022-31179	Shescape is a simple shell escape package for JavaScript. Versions prior to 1.5.8 were found to be subject to code injection on windows. This impacts users that use Shescape (any API function) to escape arguments for cmd.exe on Windows An attacker can omit all arguments following their input by including a line feed character (`'\n'`) in the payload. This bug has been patched in [v1.5.8] which you can upgrade to now. No further changes are required. Alternatively, line feed characters (`'\n'`) can be stripped out manually or the user input can be made the last argument (this only limits the impact).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30319	Saia Burgess Controls (SBC) PCD through 2022-05-06 allows Authentication bypass. According to FSCT-2022-0062, there is a Saia Burgess Controls (SBC) PCD S-Bus authentication bypass issue. The affected components are characterized as: S-Bus (5050/UDP) authentication. The potential impact is: Authentication bypass. The Saia Burgess Controls (SBC) PCD controllers utilize the S-Bus protocol (5050/UDP) for a variety of engineering purposes. It is possible to configure a password in order to restrict access to sensitive engineering functionality. Authentication functions on the basis of a MAC/IP whitelist with inactivity timeout to which an authenticated client's MAC/IP is stored. UDP traffic can be spoofed to bypass the whitelist-based access control. Since UDP is stateless, an attacker capable of passively observing traffic can spoof arbitrary messages using the MAC/IP of an authenticated client. This allows the attacker access to sensitive engineering functionality such as uploading/downloading control logic and manipulating controller configuration.	8.1	More Details
CVE-2022-36991	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could arbitrarily write content to a partially controlled path on a NetBackup Primary server.	8.1	More Details
CVE-2022-1805	When connecting to Amazon Workspaces, the SHA256 presented by AWS connection provisioner is not fully verified by Zero Clients. The issue could be exploited by an adversary that places a MITM (Man in the Middle) between a zero client and AWS session provisioner in the network. This issue is only applicable when connecting to an Amazon Workspace from a PCoIP Zero Client.	8.1	More Details
CVE-2022-37035	An issue was discovered in bgpd in FRRouting (FRR) 8.3. In bgp_notify_send_with_data() and bgp_process_packet() in bgp_packet.c, there is a possible use-after-free due to a race condition. This could lead to Remote Code Execution or Information Disclosure by sending crafted BGP packets. User interaction is not needed for exploitation.	8.1	More Details
CVE-2022-30571	The iWay Service Manager Console component of TIBCO Software Inc.'s TIBCO iWay Service Manager contains easily exploitable Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO iWay Service Manager: versions 8.0.6 and below.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35291	Due to misconfigured application endpoints, SAP SuccessFactors attachment APIs allow attackers with user privileges to perform activities with admin privileges over the network. These APIs were consumed in the SF Mobile application for Time Off, Time Sheet, EC Workflow, and Benefits. On successful exploitation, the attacker can read/write attachments. Thus, compromising the confidentiality and integrity of the application	8.1	More Details
CVE-2022-36881	Jenkins Git client Plugin 3.11.0 and earlier does not perform SSH host key verification when connecting to Git repositories via SSH, enabling man-in-the-middle attacks.	8.1	More Details
CVE-2022-36921	A missing permission check in Jenkins Coverity Plugin 1.11.4 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.	8.1	More Details
CVE-2022-30287	Horde Groupware Webmail Edition through 5.2.22 allows a reflection injection attack through which an attacker can instantiate a driver class. This then leads to arbitrary deserialization of PHP objects.	8.0	More Details
CVE-2022-36988	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup OpsCenter server, NetBackup Primary server, or NetBackup Media server could remotely execute arbitrary commands on a NetBackup Primary server or NetBackup Media server.	8.0	More Details
CVE-2022-36916	A cross-site request forgery (CSRF) vulnerability in Jenkins Google Cloud Backup Plugin 0.6 and earlier allows attackers to request a manual backup.	8.0	More Details
CVE-2022-36985	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with unprivileged local access to a Windows NetBackup Primary server could potentially escalate their privileges.	7.8	More Details
CVE-2022-2580	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0102.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27873	An attacker can force the victim's device to perform arbitrary HTTP requests in WAN through a malicious SVG file being parsed by Autodesk Fusion 360's document parser. The vulnerability exists in the application's 'Insert SVG' procedure. An attacker can also leverage this vulnerability to obtain victim's public IP and possibly other sensitive information.	7.8	More Details
CVE-2022-33881	Parsing a maliciously crafted PRT file can force Autodesk AutoCAD 2023 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-36123	The Linux kernel before 5.18.13 lacks a certain clear operation for the block starting symbol (.bss). This allows Xen PV guest OS users to cause a denial of service or gain privileges.	7.8	More Details
CVE-2022-2581	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.0104.	7.8	More Details
CVE-2022-35217	The NHI card's web service component has a stack-based buffer overflow vulnerability due to insufficient validation for network packet header length. A local area network attacker with general user privilege can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service.	7.8	More Details
CVE-2022-27865	A maliciously crafted TGA or PCX file may be used to write beyond the allocated buffer through DesignReview.exe application while parsing TGA and PCX files. This vulnerability may be exploited to execute arbitrary code.	7.8	More Details
CVE-2022-27866	A maliciously crafted TIFF file when consumed through DesignReview.exe application can be forced to read beyond allocated boundaries when parsing the TIFF file. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-35672	Adobe Acrobat Reader version 22.001.20085 (and earlier), 20.005.30314 (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2571	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0101.	7.8	More Details
CVE-2022-33158	Trend Micro VPN Proxy Pro version 5.2.1026 and below contains a vulnerability involving some overly permissive folders in a key directory which could allow a local attacker to obtain privilege escalation on an affected system.	7.8	More Details
CVE-2022-26429	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	7.8	More Details
CVE-2022-36336	A link following vulnerability in the scanning function of Trend Micro Apex One and Worry-Free Business Security agents could allow a local attacker to escalate privileges on affected installations. The resolution for this issue has been deployed automatically via ActiveUpdate to customers in an updated Spyware pattern. Customers who are up-to-date on detection patterns are not required to take any additional steps to mitigate this issue.	7.8	More Details
CVE-2021-39088	IBM QRadar SIEM 7.3, 7.4, and 7.5 is vulnerable to local privilege escalation if this could be combined with other unknown vulnerabilities then privilege escalation could be performed. IBM X-Force ID: 216111.	7.8	More Details
CVE-2022-36955	In Veritas NetBackup, an attacker with unprivileged local access to a NetBackup Client may send specific commands to escalate their privileges. This affects 8.0 through 8.1.2, 8.2, 8.3 through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1.	7.8	More Details
CVE-2022-31627	In PHP versions 8.1.x below 8.1.8, when fileinfo functions, such as finfo_buffer, due to incorrect patch applied to the third party code from libmagic, incorrect function may be used to free allocated memory, which may lead to heap corruption.	7.7	More Details
CVE-2022-27615	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in cgi component in Synology DNS Server before 2.2.2-5027 allows remote authenticated users to delete arbitrary files via unspecified vectors.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35220	Teamplus Pro community discussion function has an ‘allocation of resource without limits or throttling’ vulnerability. A remote attacker with general user privilege posting a thread with large content can cause the receiving client device to allocate too much memory, leading to abnormal termination of this client’s Teamplus Pro application.	7.7	More Details
CVE-2022-36984	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely trigger a denial of service attack against a NetBackup Primary server.	7.7	More Details
CVE-2022-36883	A missing permission check in Jenkins Git Plugin 4.11.3 and earlier allows unauthenticated attackers to trigger builds of jobs configured to use an attacker-specified Git repository and to cause them to check out an attacker-specified commit.	7.5	More Details
CVE-2022-34593	DPTech VPN v8.1.28.0 was discovered to contain an arbitrary file read vulnerability.	7.5	More Details
CVE-2022-34568	SDL v1.2 was discovered to contain a use-after-free via the XFree function at /src/video/x11/SDL_x11yuv.c.	7.5	More Details
CVE-2016-4427	In zulip before 1.3.12, deactivated users could access messages if SSO was enabled.	7.5	More Details
CVE-2022-37315	graphql-go (aka GraphQL for Go) through 0.8.0 has infinite recursion in the type definition parser.	7.5	More Details
CVE-2022-34924	Lanling OA Landray Office Automation (OA) internal patch number #133383/#137780 contains an arbitrary file read vulnerability via the component /sys/ui/extend/varkind/custom.jsp.	7.5	More Details
CVE-2022-35923	v8n is a javascript validation library. Versions of v8n prior to 1.5.1 were found to have an inefficient regular expression complexity in the `lowercase()` and `uppercase()` regex which could lead to a denial of service attack. In testing of the `lowercase()` function a payload of 'a' + 'a'.repeat(i) + 'A' with 32 leading characters took 29443 ms to execute. The same issue happens with uppercase(). Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2509	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification of pkcs7 signatures in gnutls_pkcs7_verify function.	7.5	More Details
CVE-2016-0796	WordPress Plugin mb.miniAudioPlayer-an HTML5 audio player for your mp3 files is prone to multiple vulnerabilities, including open proxy and security bypass vulnerabilities because it fails to properly verify user-supplied input. An attacker may leverage these issues to hide attacks directed at a target site from behind vulnerable website or to perform otherwise restricted actions and subsequently download files with the extension mp3, mp4a, wav and ogg from anywhere the web server application has read access to the system. WordPress Plugin mb.miniAudioPlayer-an HTML5 audio player for your mp3 files version 1.7.6 is vulnerable; prior versions may also be affected.	7.5	More Details
CVE-2021-22640	An attacker can decrypt the Ovarro TBox login password by communication capture and brute force attacks.	7.5	More Details
CVE-2021-22642	An attacker could use specially crafted invalid Modbus frames to crash the Ovarro TBox system.	7.5	More Details
CVE-2021-22644	Ovarro TBox TWinSoft uses the custom hardcoded user “TWinSoft” with a hardcoded key.	7.5	More Details
CVE-2022-22505	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 contains a vulnerability that could allow IBM tenant credentials to be exposed. IBM X-Force ID: 227288.	7.5	More Details
CVE-2022-29808	In Quest KACE Systems Management Appliance (SMA) through 12.0, predictable token generation occurs when appliance linking is enabled.	7.5	More Details
CVE-2021-22650	An attacker may use TWinSoft and a malicious source project file (TPG) to extract files on machine executing Ovarro TWinSoft, which could lead to code execution.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35922	Rust-WebSocket is a WebSocket (RFC6455) library written in Rust. In versions prior to 0.26.5 untrusted websocket connections can cause an out-of-memory (OOM) process abort in a client or a server. The root cause of the issue is during dataframe parsing. Affected versions would allocate a buffer based on the declared dataframe size, which may come from an untrusted source. When `Vec::with_capacity` fails to allocate, the default Rust allocator will abort the current process, killing all threads. This affects only sync (non-Tokio) implementation. Async version also does not limit memory, but does not use `with_capacity`, so DoS can happen only when bytes for oversized dataframe or message actually got delivered by the attacker. The crashes are fixed in version 0.26.5 by imposing default dataframe size limits. Affected users are advised to update to this version. Users unable to upgrade are advised to filter websocket traffic externally or to only accept trusted traffic.	7.5	More Details
CVE-2022-31198	OpenZeppelin Contracts is a library for secure smart contract development. This issue concerns instances of Governor that use the module `GovernorVotesQuorumFraction`, a mechanism that determines quorum requirements as a percentage of the voting token's total supply. In affected instances, when a proposal is passed to lower the quorum requirements, past proposals may become executable if they had been defeated only due to lack of quorum, and the number of votes it received meets the new quorum requirement. Analysis of instances on chain found only one proposal that met this condition, and we are actively monitoring for new occurrences of this particular issue. This issue has been patched in v4.7.2. Users are advised to upgrade. Users unable to upgrade should consider avoiding lowering quorum requirements if a past proposal was defeated for lack of quorum.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30313	Honeywell Experion PKS Safety Manager through 2022-05-06 has Missing Authentication for a Critical Function. According to FSCT-2022-0051, there is a Honeywell Experion PKS Safety Manager multiple proprietary protocols with unauthenticated functionality issue. The affected components are characterized as: Honeywell Experion TCP (51000/TCP), Safety Builder (51010/TCP). The potential impact is: Manipulate controller state, Manipulate controller configuration, Manipulate controller logic, Manipulate controller files, Manipulate IO. The Honeywell Experion PKS Distributed Control System (DCS) Safety Manager utilizes several proprietary protocols for a wide variety of functionality, including process data acquisition, controller steering and configuration management. These protocols include: Experion TCP (51000/TCP) and Safety Builder (51010/TCP). None of these protocols have any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality. There is no authentication functionality on the protocols in question. An attacker capable of invoking the protocols' functionalities could achieve a wide range of adverse impacts, including (but not limited to), the following: for Experion TCP (51000/TCP): Issue IO manipulation commands, Issue file read/write commands; and for Safety Builder (51010/TCP): Issue controller start/stop commands, Issue logic download/upload commands, Issue file read commands, Issue system time change commands. A mitigating factor with regards to some, but not all, of the above functionality is that these require the Safety Manager physical keyswitch to be in the right position.	7.5	More Details
CVE-2022-31173	Juniper is a GraphQL server library for Rust. Affected versions of Juniper are vulnerable to uncontrolled recursion resulting in a program crash. This issue has been addressed in version 0.15.10. Users are advised to upgrade. Users unable to upgrade should limit the recursion depth manually.	7.5	More Details
CVE-2022-2414	Access to external entities when parsing XML documents can lead to XML external entity (XXE) attacks. This flaw allows a remote attacker to potentially retrieve the content of arbitrary files by sending specially crafted HTTP requests.	7.5	More Details
CVE-2022-25867	The package io.socket:socket.io-client before 2.0.1 are vulnerable to NULL Pointer Dereference when parsing a packet with with invalid payload format.	7.5	More Details
CVE-2022-2324	Improperly Implemented Security Check vulnerability in the SonicWall Hosted Email Security leads to bypass of Capture ATP security service in the appliance. This vulnerability impacts 10.0.17.7319 and earlier versions	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1585	The Project Source Code Download WordPress plugin through 1.0.0 does not protect its backup generation and download functionalities, which may allow any visitors on the site to download the entire site, including sensitive files like wp-config.php.	7.5	More Details
CVE-2022-36447	An inflation issue was discovered in Chia Network CAT1 Standard 1.0.0. Previously minted tokens minted on the Chia blockchain using the CAT1 standard can be inflated to an arbitrary extent by any holder of any amount of the token. The total amount of the token can be increased as high as the malicious actor pleases. This is true for every CAT1 on the Chia blockchain regardless of issuance rules. This attack is auditable on chain, so maliciously altered coins can potentially be marked by off-chain observers as malicious.	7.5	More Details
CVE-2022-34121	Cuppa CMS v1.0 was discovered to contain a local file inclusion (LFI) vulnerability via the component /templates/default/html/windows/right.php.	7.5	More Details
CVE-2022-36946	nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.	7.5	More Details
CVE-2022-36234	SimpleNetwork TCP Server commit 29bc615f0d9910eb2f59aa8dff1f54f0e3af4496 was discovered to contain a double free vulnerability which is exploited via crafted TCP packets.	7.5	More Details
CVE-2022-35911	On Patlite NH-FB series devices through 1.46, remote attackers can cause a denial of service by omitting the query string. NOTE: the vendor's perspective is that "omitting the query string does not cause a denial of service and the indicated event can not be reproduced.	7.5	More Details
CVE-2022-2591	A vulnerability classified as critical has been found in TEM FLEX-1085 1.6.0. Affected is an unknown function of the file /sistema/flash/reboot. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.5	More Details
CVE-2022-2576	In Eclipse Californium version 2.0.0 to 2.7.2 and 3.0.0-3.5.0 a DTLS resumption handshake falls back to a DTLS full handshake on a parameter mismatch without using a HelloVerifyRequest. Especially, if used with certificate based cipher suites, that results in message amplification (DDoS other peers) and high CPU load (DoS own peer). The misbehavior occurs only with DTLS_VERIFY_PEERS_ON_RESUMPTION_THRESHOLD values larger than 0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24912	The package github.com/runatlantis/atlantis/server/controllers/events before 0.19.7 are vulnerable to Timing Attack in the webhook event validator code, which does not use a constant-time comparison function to validate the webhook secret. It can allow an attacker to recover this secret as an attacker and then forge webhook events.	7.5	More Details
CVE-2022-35919	MinIO is a High Performance Object Storage released under GNU Affero General Public License v3.0. In affected versions all 'admin' users authorized for `admin:ServerUpdate` can selectively trigger an error that in response, returns the content of the path requested. Any normal OS system would allow access to contents at any arbitrary paths that are readable by MinIO process. Users are advised to upgrade. Users unable to upgrade may disable ServerUpdate API by denying the `admin:ServerUpdate` action for your admin users via IAM policies.	7.4	More Details
CVE-2021-38417	VISAM VBASE version 11.6.0.6 is vulnerable to improper access control via the web-remote endpoint, which may allow an unauthenticated user viewing access to folders and files in the directory listing.	7.4	More Details
CVE-2022-29154	An issue was discovered in rsync before 3.2.5 that allows malicious remote servers to write arbitrary files inside the directories of connecting peers. The server chooses which files/directories are sent to the client. However, the rsync client performs insufficient validation of file names. A malicious rsync server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the rsync client target directory and subdirectories (for example, overwrite the .ssh/authorized_keys file).	7.4	More Details
CVE-2021-38410	AVEVA Software Platform Common Services (PCS) Portal versions 4.5.2, 4.5.1, 4.5.0, and 4.4.6 are vulnerable to DLL hijacking through an uncontrolled search path element, which may allow an attacker control to one or more locations in the search path.	7.3	More Details
CVE-2022-27612	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in cgi component in Synology Audio Station before 6.5.4-3367 allows remote attackers to execute arbitrary commands via unspecified vectors.	7.3	More Details
CVE-2022-26310	Pandora FMS v7.0NG.760 and below allows an improper authorization in User Management where any authenticated user with access to the User Management module could create, modify or delete any user with full admin privilege. The impact could lead to a vertical privilege escalation to access the privileges of a higher-level user or typically an admin user.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7795	The package get-npm-package-version before 1.0.7 are vulnerable to Command Injection via main function in index.js.	7.3	More Details
CVE-2020-28433	This affects all versions of package node-latex-pdf.	7.3	More Details
CVE-2020-28425	This affects all versions of package curljs.	7.3	More Details
CVE-2022-36799	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1.	7.2	More Details
CVE-2020-28424	This affects all versions of package s3-kilatstorage.	7.2	More Details
CVE-2022-34625	Mealie1.0.0beta3 was discovered to contain a Server-Side Template Injection vulnerability, which allows attackers to execute arbitrary code via a crafted Jinja2 template.	7.2	More Details
CVE-2022-34578	Open Source Point of Sale v3.3.7 was discovered to contain an arbitrary file upload vulnerability via the Update Branding Settings page.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31109	laminas-diactoros is a PHP package containing implementations of the PSR-7 HTTP message interfaces and PSR-17 HTTP message factory interfaces. Applications that use Diactoros, and are either not behind a proxy, or can be accessed via untrusted proxies, can potentially have the host, protocol, and/or port of a `Laminas\Diactoros\Uri` instance associated with the incoming server request modified to reflect values from `X-Forwarded-*` headers. Such changes can potentially lead to XSS attacks (if a fully-qualified URL is used in links) and/or URL poisoning. Since the `X-Forwarded-*` headers do have valid use cases, particularly in clustered environments using a load balancer, the library offers mitigation measures only in the v2 releases, as doing otherwise would break these use cases immediately. Users of v2 releases from 2.11.1 can provide an additional argument to `Laminas\Diactoros\ServerRequestFactory::fromGlobals()` in the form of a `Laminas\Diactoros\RequestFilter\RequestFilterInterface` instance, including the shipped `Laminas\Diactoros\RequestFilter\NoOpRequestFilter` implementation which ignores the `X-Forwarded-*` headers. Starting in version 3.0, the library will reverse behavior to use the `NoOpRequestFilter` by default, and require users to opt-in to `X-Forwarded-*` header usage via a configured `Laminas\Diactoros\RequestFilter\LegacyXForwardedHeaderFilter` instance. Users are advised to upgrade to version 2.11.1 or later to resolve this issue. Users unable to upgrade may configure web servers to reject `X-Forwarded-*` headers at the web server level.	7.2	More Details
CVE-2022-33970	Authenticated WordPress Options Change vulnerability in Biplob018 Shortcode Addons plugin <= 3.1.2 at WordPress.	7.2	More Details
CVE-2022-35421	Online Tours And Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the pname parameter at /admin/operations/packages.php.	7.2	More Details
CVE-2022-34120	Barangay Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the module editing function at /pages/activity/activity.php.	7.2	More Details
CVE-2022-30616	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to elevate their privilege to platform administrator through manipulation of APIs. IBM X-Force ID: 227978.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22684	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in task management component in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows remote authenticated users to execute arbitrary commands via unspecified vectors.	7.2	More Details
CVE-2022-31195	DSpace open source software is a repository application which provides durable access to digital resources. In affected versions the ItemImportServiceImpl is vulnerable to a path traversal vulnerability. This means a malicious SAF (simple archive format) package could cause a file/directory to be created anywhere the Tomcat/DSpace user can write to on the server. However, this path traversal vulnerability is only possible by a user with special privileges (either Administrators or someone with command-line access to the server). This vulnerability impacts the XMLUI, JSPUI and command-line. Users are advised to upgrade. As a basic workaround, users may block all access to the following URL paths: If you are using the XMLUI, block all access to /admin/batchimport path (this is the URL of the Admin Batch Import tool). Keep in mind, if your site uses the path "/xmlui", then you'd need to block access to /xmlui/admin/batchimport. If you are using the JSPUI, block all access to /dspace-admin/batchimport path (this is the URL of the Admin Batch Import tool). Keep in mind, if your site uses the path "/jspui", then you'd need to block access to /jspui/dspace-admin/batchimport. Keep in mind, only an Administrative user or a user with command-line access to the server is able to import/upload SAF packages. Therefore, assuming those users do not blindly upload untrusted SAF packages, then it is unlikely your site could be impacted by this vulnerability.	7.2	More Details
CVE-2022-34154	Authenticated (author or higher user role) Arbitrary File Upload vulnerability in ideasToCode Enable SVG, WebP & ICO Upload plugin <= 1.0.1 at WordPress.	7.2	More Details
CVE-2022-31191	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI spellcheck "Did you mean" HTML escapes the data-spell attribute in the link, but not the actual displayed text. Similarly, the JSPUI autocomplete HTML does not properly escape text passed to it. Both are vulnerable to XSS. This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds for this issue.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31192	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI "Request a Copy" feature does not properly escape values submitted and stored from the "Request a Copy" form. This means that item requests could be vulnerable to XSS attacks. This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2022-36997	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely trigger impacts that include arbitrary file read, Server-Side Request Forgery (SSRF), and denial of service.	7.1	More Details
CVE-2022-31193	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI controlled vocabulary servlet is vulnerable to an open redirect attack, where an attacker can craft a malicious URL that looks like a legitimate DSpace/repository URL. When that URL is clicked by the target, it redirects them to a site of the attacker's choice. This issue has been patched in versions 5.11 and 6.4. Users are advised to upgrade. There are no known workaround for this vulnerability.	7.1	More Details
CVE-2022-35234	Trend Micro Security 2021 and 2022 (Consumer) is vulnerable to an Out-Of-Bounds Read Information Disclosure Vulnerability that could allow an attacker to read sensitive information from other memory locations and cause a crash on an affected machine.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30316	Honeywell Experion PKS Safety Manager 5.02 has Insufficient Verification of Data Authenticity. According to FSCT-2022-0054, there is a Honeywell Experion PKS Safety Manager unauthenticated firmware update issue. The affected components are characterized as: Firmware update functionality. The potential impact is: Firmware manipulation. The Honeywell Experion PKS Safety Manager utilizes the DCOM-232/485 communication FTA serial interface and Enea POLO bootloader for firmware management purposes. An engineering workstation running the Safety Builder software communicates via serial or serial-over-ethernet link with the DCOM-232/485 interface. Firmware images were found to have no authentication (in the form of firmware signing) and only relied on insecure checksums for regular integrity checks. Firmware images are unsigned. An attacker with access to the serial interface (either through physical access, a compromised EWS or an exposed serial-to-ethernet gateway) can utilize hardcoded credentials (see FSCT-2022-0052) for the POLO bootloader to control the boot process and push malicious firmware images to the controller allowing for firmware manipulation, remote code execution and denial of service impacts. A mitigating factor is that in order for a firmware update to be initiated, the Safety Manager has to be rebooted which is typically done by means of physical controls on the Safety Manager itself. As such, an attacker would have to either lay dormant until a legitimate reboot occurs or possibly attempt to force a reboot through a secondary vulnerability.	6.8	More Details
CVE-2022-35222	HiCOS Citizen verification component has a stack-based buffer overflow vulnerability due to insufficient parameter length validation. An unauthenticated physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service.	6.8	More Details
CVE-2022-33955	IBM CICS TX 11.1 could allow allow an attacker with physical access to the system to execute code due using a back and refresh attack. IBM X-Force ID: 229312.	6.8	More Details
CVE-2022-21788	In scp, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06988728; Issue ID: ALPS06988728.	6.7	More Details
CVE-2022-26443	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26430	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521.	6.7	More Details
CVE-2022-26440	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037.	6.7	More Details
CVE-2022-26431	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553.	6.7	More Details
CVE-2022-26432	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542.	6.7	More Details
CVE-2022-26433	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400.	6.7	More Details
CVE-2022-26434	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450.	6.7	More Details
CVE-2022-26435	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435.	6.7	More Details
CVE-2022-26445	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088.	6.7	More Details
CVE-2022-26438	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26426	In camera isp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07085486; Issue ID: ALPS07085486.	6.7	More Details
CVE-2022-26439	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020.	6.7	More Details
CVE-2022-26427	In camera isp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07085540; Issue ID: ALPS07085540.	6.7	More Details
CVE-2022-21792	In camera isp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07085410; Issue ID: ALPS07085410.	6.7	More Details
CVE-2022-26442	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051.	6.7	More Details
CVE-2022-26441	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	6.7	More Details
CVE-2022-26444	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075.	6.7	More Details
CVE-2022-24406	OX App Suite through 7.10.6 allows SSRF because multipart/form-data boundaries are predictable, and this can lead to injection into internal Documentconverter API calls.	6.5	More Details
CVE-2021-46830	A path traversal vulnerability exists within GoAnywhere MFT before 6.8.3 that utilize self-registration for the GoAnywhere Web Client. This vulnerability could potentially allow an external user who self-registers with a specific username and/or profile information to gain access to files at a higher directory level than intended.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36888	A missing permission check in Jenkins HashiCorp Vault Plugin 354.vdb_858fd6b_f48 and earlier allows attackers with Overall/Read permission to obtain credentials stored in Vault with attacker-specified path and keys.	6.5	More Details
CVE-2022-30698	NLnet Labs Unbound, up to and including version 1.16.1 is vulnerable to a novel type of the "ghost domain names" attack. The vulnerability works by targeting an Unbound instance. Unbound is queried for a subdomain of a rogue domain name. The rogue nameserver returns delegation information for the subdomain that updates Unbound's delegation cache. This action can be repeated before expiry of the delegation information by querying Unbound for a second level subdomain which the rogue nameserver provides new delegation information. Since Unbound is a child-centric resolver, the ever-updating child delegation information can keep a rogue domain name resolvable long after revocation. From version 1.16.2 on, Unbound checks the validity of parent delegation records before using cached delegation information.	6.5	More Details
CVE-2022-2160	Insufficient policy enforcement in DevTools in Google Chrome on Windows prior to 103.0.5060.53 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from a user's local files via a crafted HTML page.	6.5	More Details
CVE-2022-1858	Out of bounds read in DevTools in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to perform an out of bounds memory read via specific user interaction.	6.5	More Details
CVE-2022-1862	Inappropriate implementation in Extensions in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass profile restrictions via a crafted HTML page.	6.5	More Details
CVE-2022-1867	Insufficient validation of untrusted input in Data Transfer in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to bypass same origin policy via a crafted clipboard content.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30699	NLnet Labs Unbound, up to and including version 1.16.1, is vulnerable to a novel type of the "ghost domain names" attack. The vulnerability works by targeting an Unbound instance. Unbound is queried for a rogue domain name when the cached delegation information is about to expire. The rogue nameserver delays the response so that the cached delegation information is expired. Upon receiving the delayed answer containing the delegation information, Unbound overwrites the now expired entries. This action can be repeated when the delegation information is about to expire making the rogue delegation information ever-updating. From version 1.16.2 on, Unbound stores the start time for a query and uses that to decide if the cached delegation information can be overwritten.	6.5	More Details
CVE-2022-1869	Type Confusion in V8 in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2022-34526	A stack overflow was discovered in the _TIFFVGetField function of Tiffsplit v4.4.0. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted TIFF file parsed by the "tiffsplit" or "tiffcrop" utilities.	6.5	More Details
CVE-2022-35716	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.16, 7.0.0.0 through 7.0.5.11, 7.1.0.0 through 7.1.2.7, and 7.2.0.0 through 7.2.3.0 could allow an authenticated user to obtain sensitive information in some instances due to improper security checking. IBM X-Force ID: 231360.	6.5	More Details
CVE-2022-34338	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could disclose sensitive information due to improper privilege management for storage provider types. IBM X-Force ID: 229962.	6.5	More Details
CVE-2022-1873	Insufficient policy enforcement in COOP in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-33169	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to insufficiently protected credentials for users created via a bulk upload. IBM X-Force ID: 228888.	6.5	More Details
CVE-2022-36911	A cross-site request forgery (CSRF) vulnerability in Jenkins Openstack Heat Plugin 1.5 and earlier allows attackers to connect to an attacker-specified URL.	6.5	More Details
CVE-2022-1868	Inappropriate implementation in Extensions API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34551	Sims v1.0 was discovered to allow path traversal when downloading attachments.	6.5	More Details
CVE-2022-2598	Out-of-bounds Write to API in GitHub repository vim/vim prior to 9.0.0100.	6.5	More Details
CVE-2022-2553	The authfile directive in the booth config file is ignored, preventing use of authentication in communications from node to node. As a result, nodes that do not have the correct authentication key are not prevented from communicating with other nodes in the cluster.	6.5	More Details
CVE-2022-30572	The iWay Service Manager Console component of TIBCO Software Inc.'s TIBCO iWay Service Manager contains an easily exploitable Directory Traversal vulnerability that allows a low privileged attacker with network access to read arbitrary resources on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO iWay Service Manager: versions 8.0.6 and below.	6.5	More Details
CVE-2022-27610	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25423 allows remote authenticated users to delete arbitrary files via unspecified vectors.	6.5	More Details
CVE-2022-36901	Jenkins HTTP Request Plugin 1.15 and earlier stores HTTP Request passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-36909	A missing permission check in Jenkins OpenShift Deployer Plugin 1.2.0 and earlier allows attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system and to upload a SSH key file from the Jenkins controller file system to an attacker-specified URL.	6.5	More Details
CVE-2022-36908	A cross-site request forgery (CSRF) vulnerability in Jenkins OpenShift Deployer Plugin 1.2.0 and earlier allows attackers to check for the existence of an attacker-specified file path on the Jenkins controller file system and to upload a SSH key file from the Jenkins controller file system to an attacker-specified URL.	6.5	More Details
CVE-2022-36907	A missing permission check in Jenkins OpenShift Deployer Plugin 1.2.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified username and password.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37000	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). Under certain conditions, an attacker with authenticated access to a NetBackup Client could remotely read files on a NetBackup Primary server.	6.5	More Details
CVE-2022-36999	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). Under certain conditions, an attacker with authenticated access to a NetBackup Client could remotely read files on a NetBackup Primary server.	6.5	More Details
CVE-2022-36906	A cross-site request forgery (CSRF) vulnerability in Jenkins OpenShift Deployer Plugin 1.2.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified username and password.	6.5	More Details
CVE-2022-36894	An arbitrary file write vulnerability in Jenkins CLIF Performance Testing Plugin 64.vc0d66de1dfb_f and earlier allows attackers with Overall/Read permission to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content.	6.5	More Details
CVE-2022-2370	The YaySMTP WordPress plugin before 2.2.1 does not have capability check before displaying the Mailer Credentials in JS code for the settings, allowing any authenticated users, such as subscriber to retrieve them	6.5	More Details
CVE-2022-31184	Discourse is the an open source discussion platform. In affected versions an email activation route can be abused to send mass spam emails. A fix has been included in the latest stable, beta and tests-passed versions of Discourse which rate limits emails. Users are advised to upgrade. Users unable to upgrade should manually rate limit email.	6.5	More Details
CVE-2022-35918	Streamlit is a data oriented application development framework for python. Users hosting Streamlit app(s) that use custom components are vulnerable to a directory traversal attack that could leak data from their web server file-system such as: server logs, world readable files, and potentially other sensitive information. An attacker can craft a malicious URL with file paths and the streamlit server would process that URL and return the contents of that file. This issue has been resolved in version 1.11.1. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2260	The GiveWP WordPress plugin before 2.21.3 does not have CSRF in place when exporting data, and does not validate the exporting parameters such as dates, which could allow attackers to make a logged in admin DoS the web server via a CSRF attack as the plugin will try to retrieve data from the database many times which leads to overwhelm the target's CPU.	6.5	More Details
CVE-2022-36896	A missing permission check in Jenkins Compuware Source Code Download for Endevor, PDS, and ISPW Plugin 2.0.12 and earlier allows attackers with Overall/Read permission to enumerate hosts and ports of Compuware configurations and credentials IDs of credentials stored in Jenkins.	6.5	More Details
CVE-2016-2138	In kippo-graph before version 1.5.1, there is a cross-site scripting vulnerability in xss_clean() in class/KippoInput.class.php.	6.4	More Details
CVE-2022-31154	Sourcegraph is an opensource code search and navigation engine. It is possible for an authenticated Sourcegraph user to edit the Code Monitors owned by any other Sourcegraph user. This includes being able to edit both the trigger and the action of the monitor in question. An attacker is not able to read contents of existing code monitors, only override the data. The issue is fixed in Sourcegraph 3.42. There are no workaround for the issue and patching is highly recommended.	6.4	More Details
CVE-2016-2139	In kippo-graph before version 1.5.1, there is a cross-site scripting vulnerability in $file_link in class/KippoInput.class.php.	6.4	More Details
CVE-2022-21789	In audio ipi, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478101; Issue ID: ALPS06478101.	6.4	More Details
CVE-2022-26428	In video codec, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521260; Issue ID: ALPS06521260.	6.4	More Details
CVE-2022-2578	A vulnerability, which was classified as critical, has been found in SourceCodester Garage Management System 1.0. This issue affects some unknown processing of the file /php_action/createUser.php. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2577	A vulnerability classified as critical was found in SourceCodester Garage Management System 1.0. This vulnerability affects unknown code of the file /edituser.php. The manipulation of the argument id with the input -2'%20UNION%20select%2011,user(),333,444--+ leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-2164	Inappropriate implementation in Extensions API in Google Chrome prior to 103.0.5060.53 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted HTML page.	6.3	More Details
CVE-2022-36994	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could arbitrarily read files from a NetBackup Primary server.	6.3	More Details
CVE-2022-36998	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could remotely trigger a stack-based buffer overflow on the NetBackup Primary server, resulting in a denial of service.	6.3	More Details
CVE-2022-36967	In Progress WS_FTP Server prior to version 8.7.3, multiple reflected cross-site scripting (XSS) vulnerabilities exist in the administrative web interface. It is possible for a remote attacker to inject arbitrary JavaScript into a WS_FTP administrator's web session. This would allow the attacker to execute code within the context of the victim's browser.	6.1	More Details
CVE-2022-27509	Unauthenticated redirection to a malicious website	6.1	More Details
CVE-2022-34163	IBM CICS TX 11.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 229333.	6.1	More Details
CVE-2022-34162	IBM CICS TX 11.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 229332.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-3709	Possible cross-site scripting vulnerability in libxml after commit 960f0e2.	6.1	More Details
CVE-2022-36880	The Read Mail module in Webmin 1.995 and Usermin through 1.850 allows XSS via a crafted HTML e-mail message.	6.1	More Details
CVE-2022-35118	PyroCMS v3.9 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities.	6.1	More Details
CVE-2022-23101	OX App Suite through 7.10.6 allows XSS via appHandler in a deep link in an e-mail message.	6.1	More Details
CVE-2022-36922	Jenkins Lucene-Search Plugin 370.v62a5f618cd3a and earlier does not escape the search query parameter displayed on the 'search' result page, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-35630	A cross-site scripting (XSS) issue in generating a collection report made it possible for malicious clients to inject JavaScript code into the static HTML file. This issue was resolved in Velociraptor 0.6.5-2.	6.1	More Details
CVE-2022-2241	The Featured Image from URL (FIFU) WordPress plugin before 4.0.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. Furthermore, due to the lack of validation, sanitisation and escaping in some of them, it could also lead to Stored XSS issues	6.1	More Details
CVE-2022-2589	Cross-site Scripting (XSS) - Reflected in GitHub repository beancount/fava prior to 1.22.3.	6.1	More Details
CVE-2022-2181	The Advanced WordPress Reset WordPress plugin before 1.6 does not escape some generated URLs before outputting them back in href attributes of admin dashboard pages, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1906	The Copyright Proof WordPress plugin through 4.16 does not sanitise and escape a parameter before outputting it back via an AJAX action available to both unauthenticated and authenticated users, leading to a Reflected Cross-Site Scripting when a specific setting is enabled.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42537	VISAM VBASE version 11.6.0.6 processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.	5.9	More Details
CVE-2022-2596	Inefficient Regular Expression Complexity in GitHub repository node-fetch/node-fetch prior to 3.2.10.	5.9	More Details
CVE-2020-6998	The connection establishment algorithm found in Rockwell Automation CompactLogix 5370 and ControlLogix 5570 versions 33 and prior does not sufficiently manage its control flow during execution, creating an infinite loop. This may allow an attacker to send specially crafted CIP packet requests to a controller, which may cause denial-of-service conditions in communications with other products.	5.8	More Details
CVE-2022-1293	The embedded neutralization of Script-Related HTML Tag, was by-passed in the case of some extra conditions.	5.7	More Details
CVE-2022-1799	Incorrect signature trust exists within Google Play services SDK play-services-basement. A debug version of Google Play services is trusted by the SDK for devices that are non-GMS. We recommend upgrading the SDK past the 2022-05-03 release.	5.7	More Details
CVE-2022-34164	IBM CICS TX 11.1 could allow a local user to impersonate another legitimate user due to improper input validation. IBM X-Force ID: 229338.	5.5	More Details
CVE-2022-36879	An issue was discovered in the Linux kernel through 5.18.14. xfrm_expand_policies in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice.	5.5	More Details
CVE-2022-35218	The NHI card’s web service component has a heap-based buffer overflow vulnerability due to insufficient validation for packet origin parameter length. A LAN attacker with general user privilege can exploit this vulnerability to disrupt service.	5.5	More Details
CVE-2022-34556	PicoC v3.2.2 was discovered to contain a NULL pointer dereference at variable.c.	5.5	More Details
CVE-2022-2549	NULL Pointer Dereference in GitHub repository gpac/gpac prior to v2.1.0-DEV.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36752	png2webp v1.0.4 was discovered to contain an out-of-bounds write via the function w2p. This vulnerability is exploitable via a crafted png file.	5.5	More Details
CVE-2022-34529	WASM3 v0.5.0 was discovered to contain a segmentation fault via the component Compile_Memory_CopyFill.	5.5	More Details
CVE-2022-35219	The NHI card's web service component has a stack-based buffer overflow vulnerability due to insufficient validation for network packet key parameter. A LAN attacker with general user privilege can exploit this vulnerability to disrupt service.	5.5	More Details
CVE-2022-35631	On MacOS and Linux, it may be possible to perform a symlink attack by replacing this predictable file name with a symlink to another file and have the Velociraptor client overwrite the other file. This issue was resolved in Velociraptor 0.6.5-2.	5.5	More Details
CVE-2022-35669	Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 20.005.30334 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-34612	Rizin v0.4.0 and below was discovered to contain an integer overflow via the function get_long_object(). This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted binary.	5.5	More Details
CVE-2022-33917	An issue was discovered in the Arm Mali GPU Kernel Driver (Valhall r29p0 through r38p0). A non-privileged user can make improper GPU processing operations to gain access to already freed memory.	5.5	More Details
CVE-2022-34009	Fossil 2.18 on Windows allows attackers to cause a denial of service (daemon crash) via an XSS payload in a ticket. This occurs because the ticket data is stored in a temporary file, and the product does not properly handle the absence of this file after Windows Defender has flagged it as malware.	5.5	More Details
CVE-2022-35221	Teamplus Pro community discussion has an 'allocation of resource without limits or throttling' vulnerability on thread subject field. A remote attacker with general user privilege posting a thread subject with large content can cause the server to allocate too much memory, leading to missing partial post content and disrupt partial service.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34611	A cross-site scripting (XSS) vulnerability in /index.php/?p=report of Online Fire Reporting System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the "Contac #" text field.	5.4	More Details
CVE-2021-23385	This affects all versions of package Flask-Security. When using the get_post_logout_redirect and get_post_login_redirect functions, it is possible to bypass URL validation and redirect a user to an arbitrary URL by providing multiple back slashes such as \\\evil.com/path. This vulnerability is only exploitable if an alternative WSGI server other than Werkzeug is used, or the default behaviour of Werkzeug is modified using 'autocorrect_location_header=False. **Note:** Flask-Security is not maintained anymore.	5.4	More Details
CVE-2022-34619	A stored cross-site scripting (XSS) vulnerability in Mealie v0.5.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Shopping Lists item names text field.	5.4	More Details
CVE-2022-36910	Jenkins Lucene-Search Plugin 370.v62a5f618cd3a and earlier does not perform a permission check in several HTTP endpoints, allowing attackers with Overall/Read permission to reindex the database and to obtain information about jobs otherwise inaccessible to them.	5.4	More Details
CVE-2022-27611	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Audio Station before 6.5.4-3367 allows remote authenticated users to delete arbitrary files via unspecified vectors.	5.4	More Details
CVE-2022-23733	A stored XSS vulnerability was identified in GitHub Enterprise Server that allowed the injection of arbitrary attributes. This injection was blocked by Github's Content Security Policy (CSP). This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.3.11, 3.4.6 and 3.5.3. This vulnerability was reported via the GitHub Bug Bounty program.	5.4	More Details
CVE-2022-34140	A stored cross-site scripting (XSS) vulnerability in /index.php?r=site%2Fsignup of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username field.	5.4	More Details
CVE-2022-2171	The Progressive License WordPress plugin through 1.1.0 is lacking any CSRF check when saving its settings, which could allow attackers to make a logged in admin change them. Furthermore, as the plugin allows arbitrary HTML to be inserted in one of the settings, this could lead to Stored XSS issue which will be triggered in the frontend as well.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23099	OX App Suite through 7.10.6 allows XSS by forcing block-wise read.	5.4	More Details
CVE-2022-29360	The Email Viewer in RainLoop through 1.6.0 allows XSS via a crafted email message.	5.4	More Details
CVE-2022-36902	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier does not escape several fields of Moded Extended Choice parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2021-33371	A stored cross-site scripting (XSS) vulnerability in /nav_bar_action.php of Student Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Chat box.	5.4	More Details
CVE-2022-33943	Authenticated (contributor or higher user role) Cross-Site Scripting (XSS) vulnerability in Nico Amarilla's BxSlider WP plugin <= 2.0.0 at WordPress.	5.4	More Details
CVE-2022-35629	Due to a bug in the handling of the communication between the client and server, it was possible for one client, already registered with their own client ID, to send messages to the server claiming to come from another client ID. This issue was resolved in Velociraptor 0.6.5-2.	5.4	More Details
CVE-2022-31148	Shopware is an open source e-commerce software. In versions from 5.7.0 a persistent cross site scripting (XSS) vulnerability exists in the customer module. Users are recommend to update to the current version 5.7.14. You can get the update to 5.7.14 regularly via the Auto-Updater or directly via the download overview. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-34618	A stored cross-site scripting (XSS) vulnerability in Mealie 1.0.0beta3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the recipe description text field.	5.4	More Details
CVE-2022-36948	In Veritas NetBackup OpsCenter, a DOM XSS attack can occur. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31128	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions Tuleap does not properly verify permissions when creating branches with the REST API in Git repositories using the fine grained permissions. Users can create branches via the REST endpoint `POST git/:id/branches` regardless of the permissions set on the repository. This issue has been fixed in version 13.10.99.82 Tuleap Community Edition as well as in version 13.10-3 of Tuleap Enterprise Edition. Users are advised to upgrade. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-32750	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228435.	5.4	More Details
CVE-2022-34550	Sims v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /addNotifyServlet. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the notifyInfo parameter.	5.4	More Details
CVE-2022-31774	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228358.	5.4	More Details
CVE-2022-36905	Jenkins Maven Metadata Plugin for Jenkins CI server Plugin 2.2 and earlier does not perform URL validation for the Repository Base URL of List maven artifact versions parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2021-42535	VISAM VBASE version 11.6.0.6 does not neutralize or incorrectly neutralizes user-controllable input before the data is placed in output used as a public-facing webpage.	5.3	More Details
CVE-2022-36885	Jenkins GitHub Plugin 1.34.4 and earlier uses a non-constant time comparison function when checking whether the provided and computed webhook signatures are equal, allowing attackers to use statistical methods to obtain a valid webhook signature.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27614	Exposure of sensitive information to an unauthorized actor vulnerability in web server in Synology Media Server before 1.8.1-2876 allows remote attackers to obtain sensitive information via unspecified vectors.	5.3	More Details
CVE-2022-35925	BookWyrm is a social network for tracking reading. Versions prior to 0.4.5 were found to lack rate limiting on authentication views which allows brute-force attacks. This issue has been patched in version 0.4.5. Admins with existing instances will need to update their `nginx.conf` file that was created when the instance was set up. Users are advised advised to upgrade. Users unable to upgrade may update their nginx.conf files with the changes manually.	5.3	More Details
CVE-2022-35917	Solana Pay is a protocol and set of reference implementations that enable developers to incorporate decentralized payments into their apps and services. When a Solana Pay transaction is located using a reference key, it may be checked to represent a transfer of the desired amount to the recipient, using the supplied `validateTransfer` function. An edge case regarding this mechanism could cause the validation logic to validate multiple transfers. This issue has been patched as of version `0.2.1`. Users of the Solana Pay SDK should upgrade to it. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-35916	OpenZeppelin Contracts is a library for secure smart contract development. Contracts using the cross chain utilities for Arbitrum L2, `CrossChainEnabledArbitrumL2` or `LibArbitrumL2`, will classify direct interactions of externally owned accounts (EOAs) as cross chain calls, even though they are not started on L1. This issue has been patched in v4.7.2. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-35915	OpenZeppelin Contracts is a library for secure smart contract development. The target contract of an EIP-165 `supportsInterface` query can cause unbounded gas consumption by returning a lot of data, while it is generally assumed that this operation has a bounded cost. The issue has been fixed in v4.7.2. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31189	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. When an "Internal System Error" occurs in the JSPUI, then entire exception (including stack trace) is available. Information in this stacktrace may be useful to an attacker in launching a more sophisticated attack. This vulnerability only impacts the JSPUI. This issue has been fixed in version 6.4. users are advised to upgrade. Users unable to upgrade should disable the display of error messages in their internal.jsp file.	5.3	More Details
CVE-2022-31190	DSpace open source software is a repository application which provides durable access to digital resources. dspace-xmlui is a UI component for DSpace. In affected versions metadata on a withdrawn Item is exposed via the XMLUI "mets.xml" object, as long as you know the handle/URL of the withdrawn Item. This vulnerability only impacts the XMLUI. Users are advised to upgrade to version 6.4 or newer.	5.3	More Details
CVE-2022-36884	The webhook endpoint in Jenkins Git Plugin 4.11.3 and earlier provide unauthenticated attackers information about the existence of jobs configured to use an attacker-specified Git repository.	5.3	More Details
CVE-2022-31185	mprweb is a hosting platform for the makedeb Package Repository. Email addresses were found to not have been hidden, even if a user had clicked the `Hide Email Address` checkbox on their account page, or during signup. This could lead to an account's email being leaked, which may be problematic if your email needs to remain private for any reason. Users hosting their own mprweb instance will need to upgrade to the latest commit to get this fixed. Users on the official instance will already have this issue fixed.	5.3	More Details
CVE-2022-31182	Discourse is the an open source discussion platform. In affected versions a maliciously crafted request for static assets could cause error responses to be cached by Discourse's default NGINX proxy configuration. A corrected NGINX configuration is included in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2022-1600	The YOP Poll WordPress plugin before 6.4.3 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based limitations to vote in certain situations.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23001	When compressing or decompressing elliptic curve points using the Sweet B library, an incorrect choice of sign bit is used. An attacker with user level privileges and no other user's assistance can exploit this vulnerability with only knowledge of the public key and the library. The resulting output may cause an error when used in other operations; for instance, verification of a valid signature under a decompressed public key may fail. This may be leveraged by an attacker to cause an error scenario in applications which use the library, resulting in a limited denial of service for an individual user. The scope of impact cannot extend to other components.	5.3	More Details
CVE-2022-23002	When compressing or decompressing a point on the NIST P-256 elliptic curve with an X coordinate of zero, the resulting output is not properly reduced modulo the P-256 field prime and is invalid. The resulting output will cause an error when used in other operations. This may be leveraged by an attacker to cause an error scenario in applications which use the library, resulting in a limited denial of service for an individual user. The scope of impact cannot extend to other components.	5.3	More Details
CVE-2022-23003	When computing a shared secret or point multiplication on the NIST P-256 curve that results in an X coordinate of zero, the resulting output is not properly reduced modulo the P-256 field prime and is invalid. The resulting output may cause an error when used in other operations. This may be leveraged by an attacker to cause an error scenario or incorrect choice of session key in applications which use the library, resulting in a limited denial of service for an individual user. The scope of impact cannot extend to other components.	5.3	More Details
CVE-2022-23004	When computing a shared secret or point multiplication on the NIST P-256 curve using a public key with an X coordinate of zero, an error is returned from the library, and an invalid unreduced value is written to the output buffer. This may be leveraged by an attacker to cause an error scenario, resulting in a limited denial of service for an individual user. The scope of impact cannot extend to other components.	5.3	More Details
CVE-2022-34530	An issue in the login and reset password functionality of Backdrop CMS v1.22.0 allows attackers to enumerate usernames via password reset requests and distinct responses returned based on usernames.	5.3	More Details
CVE-2022-34594	Advanced School Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component ip/school/moudel/update_subject.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Edit Subject text field.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35632	The Velociraptor GUI contains an editor suggestion feature that can display the description field of a VQL function, plugin or artifact. This field was not properly sanitized and can lead to cross-site scripting (XSS). This issue was resolved in Velociraptor 0.6.5-2.	4.8	More Details
CVE-2022-1324	The Event Timeline WordPress plugin through 1.1.5 does not sanitize and escape Timeline Text, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-35882	Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in GS Plugins GS Testimonial Slider plugin <= 1.9.5 at WordPress.	4.8	More Details
CVE-2022-34580	Advanced School Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the address parameter at ip/school/index.php.	4.8	More Details
CVE-2022-2328	The Flexi Quote Rotator WordPress plugin through 0.9.4 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-2022-36378	Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in PluginlySpeaking Floating Div plugin <= 3.0 at WordPress.	4.8	More Details
CVE-2022-2325	The Invitation Based Registrations WordPress plugin through 2.2.84 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2305	The WordPress Popup WordPress plugin through 1.9.3.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2278	The Featured Image from URL (FIFU) WordPress plugin before 4.0.1 does not validate, sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2215	The GiveWP WordPress plugin before 2.21.3 does not properly sanitise and escape the currency settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2170	The Microsoft Advertising Universal Event Tracking (UET) WordPress plugin before 1.0.4 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. Due to the nature of this plugin, well crafted XSS can also leak into the frontpage.	4.8	More Details
CVE-2022-0598	The Login with phone number WordPress plugin before 1.3.8 does not sanitise and escape plugin settings which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-30314	Honeywell Experion PKS Safety Manager 5.02 uses Hard-coded Credentials. According to FSCT-2022-0052, there is a Honeywell Experion PKS Safety Manager hardcoded credentials issue. The affected components are characterized as: POLO bootloader. The potential impact is: Manipulate firmware. The Honeywell Experion PKS Safety Manager utilizes the DCOM-232/485 serial interface for firmware management purposes. When booting, the Safety Manager exposes the Enea POLO bootloader via this interface. Access to the boot configuration is controlled by means of credentials hardcoded in the Safety Manager firmware. The credentials for the bootloader are hardcoded in the firmware. An attacker with access to the serial interface (either through physical access, a compromised EWS or an exposed serial-to-ethernet gateway) can utilize these credentials to control the boot process and manipulate the unauthenticated firmware image (see FSCT-2022-0054).	4.6	More Details
CVE-2022-26436	In emi mpu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07023666; Issue ID: ALPS07023666.	4.4	More Details
CVE-2022-21790	In camera isp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479306; Issue ID: ALPS06479306.	4.4	More Details
CVE-2022-21791	In camera isp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478059; Issue ID: ALPS06478059.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36886	A cross-site request forgery (CSRF) vulnerability in Jenkins External Monitor Job Type Plugin 191.v363d0d1efdf8 and earlier allows attackers to create runs of an external job.	4.3	More Details
CVE-2022-2479	Insufficient validation of untrusted input in File in Google Chrome on Android prior to 103.0.5060.134 allowed an attacker who convinced a user to install a malicious app to obtain potentially sensitive information from internal file directories via a crafted HTML page.	4.3	More Details
CVE-2022-36996	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with access to a NetBackup Client could remotely gather information about any host known to a NetBackup Primary server.	4.3	More Details
CVE-2022-36995	An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with authenticated access to a NetBackup Client could arbitrarily create directories on a NetBackup Primary server.	4.3	More Details
CVE-2022-2165	Insufficient data validation in URL formatting in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	4.3	More Details
CVE-2022-1875	Inappropriate implementation in PDF in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2022-1872	Insufficient policy enforcement in Extensions API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass downloads policy via a crafted HTML page.	4.3	More Details
CVE-2022-1871	Insufficient policy enforcement in File System API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass file system policy via a crafted HTML page.	4.3	More Details
CVE-2022-36953	In Veritas NetBackup OpsCenter, certain endpoints could allow an unauthenticated remote attacker to gain sensitive information. This affects 8.x through 8.3.0.2, 9.x through 9.0.0.1, 9.1.x through 9.1.0.1, and 10.	4.3	More Details
CVE-2022-36919	A missing permission check in Jenkins Coverity Plugin 1.11.4 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36918	Jenkins Buckminster Plugin 1.1.1 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2022-36917	A missing permission check in Jenkins Google Cloud Backup Plugin 0.6 and earlier allows attackers with Overall/Read permission to request a manual backup.	4.3	More Details
CVE-2022-36891	A missing permission check in Jenkins Deployer Framework Plugin 85.v1d1888e8c021 and earlier allows attackers with Item/Read permission but without Deploy Now/Deploy permission to read deployment logs.	4.3	More Details
CVE-2022-36890	Jenkins Deployer Framework Plugin 85.v1d1888e8c021 and earlier does not restrict the name of files in methods implementing form validation, allowing attackers with Item/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2022-36914	Jenkins Files Found Trigger Plugin 1.5 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2022-36913	Jenkins Openstack Heat Plugin 1.5 and earlier does not perform permission checks in methods implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2022-36912	A missing permission check in Jenkins Openstack Heat Plugin 1.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2022-36904	Jenkins Repository Connector Plugin 2.2.0 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2022-36903	A missing permission check in Jenkins Repository Connector Plugin 2.2.0 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30320	Saia Burgess Controls (SBC) PCD through 2022-05-06 uses a Broken or Risky Cryptographic Algorithm. According to FSCT-2022-0063, there is a Saia Burgess Controls (SBC) PCD S-Bus weak credential hashing scheme issue. The affected components are characterized as: S-Bus (5050/UDP) authentication. The potential impact is: Authentication bypass. The Saia Burgess Controls (SBC) PCD controllers utilize the S-Bus protocol (5050/UDP) for a variety of engineering purposes. It is possible to configure a password in order to restrict access to sensitive engineering functionality. Authentication is done by using the S-Bus 'write byte' message to a specific address and supplying a hashed version of the password. The hashing algorithm used is based on CRC-16 and as such not cryptographically secure. An insecure hashing algorithm is used. An attacker capable of passively observing traffic can intercept the hashed credentials and trivially find collisions allowing for authentication without having to bruteforce a keyspace defined by the actual strength of the password. This allows the attacker access to sensitive engineering functionality such as uploading/downloading control logic and manipulating controller configuration.	4.3	More Details
CVE-2022-36968	In Progress WS_FTP Server prior to version 8.7.3, forms within the administrative interface did not include a nonce to mitigate the risk of cross-site request forgery (CSRF) attacks.	4.3	More Details
CVE-2022-36898	A missing permission check in Jenkins Compuware ISPW Operations Plugin 1.0.8 and earlier allows attackers with Overall/Read permission to enumerate hosts and ports of Compuware configurations and credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-36897	A missing permission check in Jenkins Compuware Xpediter Code Coverage Plugin 1.0.7 and earlier allows attackers with Overall/Read permission to enumerate hosts and ports of Compuware configurations and credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-36895	A missing permission check in Jenkins Compuware Topaz Utilities Plugin 1.0.8 and earlier allows attackers with Overall/Read permission to enumerate hosts and ports of Compuware configurations and credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-36893	Jenkins rpmsign-plugin Plugin 0.5.0 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Item/Read permission but without Item/Workspace or Item/Configure permission to check whether attacker-specified file patterns match workspace contents.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36892	Jenkins rhnpush-plugin Plugin 0.5.1 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Item/Read permission but without Item/Workspace or Item/Configure permission to check whether attacker-specified file patterns match workspace contents.	4.3	More Details
CVE-2022-36887	A cross-site request forgery (CSRF) vulnerability in Jenkins Job Configuration History Plugin 1155.v28a_46a_cc06a_5 and earlier allows attackers to delete entries from job, agent, and system configuration history, or restore older versions of job, agent, and system configurations.	4.3	More Details
CVE-2022-36915	Jenkins Android Signing Plugin 2.2.5 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Item/Read permission but without Item/Workspace or Item/Configure permission to check whether attacker-specified file patterns match workspace contents.	4.3	More Details
CVE-2016-4426	In zulip before 1.3.12, bot API keys were accessible to other users in the same realm.	4.3	More Details
CVE-2022-22334	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user to access information from a tenant of which they should not have access. IBM X-Force ID: 219391.	4.3	More Details
CVE-2022-34307	IBM CICS TX 11.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 229436.	4.3	More Details
CVE-2022-31155	Sourcegraph is an opensource code search and navigation engine. In Sourcegraph versions before 3.41.0, it is possible for an attacker to delete other users' saved searches due to a bug in the authorization check. The vulnerability does not allow the reading of other users' saved searches, only overwriting them with attacker-controlled searches. The issue is patched in Sourcegraph version 3.41.0. There is no workaround for this issue and updating to a secure version is highly recommended.	4.3	More Details
CVE-2022-31178	eLabFTW is an electronic lab notebook manager for research teams. A vulnerability was discovered which allows a logged in user to read a template without being authorized to do so. This vulnerability has been patched in 4.3.4. Users are advised to upgrade. There are no known workarounds for this issue.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2369	The YaySMTP WordPress plugin before 2.2.1 does not have capability check in an AJAX action, allowing any logged in users, such as subscriber to view the Logs of the plugin	4.3	More Details
CVE-2022-1561	Lura and KrakenD-CE versions older than v2.0.2 and KrakenD-EE versions older than v2.0.0 do not sanitize URL parameters correctly, allowing a malicious user to alter the backend URL defined for a pipe when remote users send crafty URL requests. The vulnerability does not affect KrakenD itself, but the consumed backend might be vulnerable.	4.0	More Details
CVE-2022-37009	In JetBrains IntelliJ IDEA before 2022.2 local code execution via a Vagrant executable was possible	3.9	More Details
CVE-2021-27785	HCL Commerce's Remote Store server could allow a local attacker to obtain sensitive personal information. The vulnerability requires the victim to first perform a particular operation on the website.	3.9	More Details
CVE-2022-26309	Pandora FMS v7.0NG.759 allows Cross-Site Request Forgery in Bulk operation (User operation) resulting in elevation of privilege to Administrator group.	3.7	More Details
CVE-2022-26308	Pandora FMS v7.0NG.760 and below allows an improper access control in Configuration (Credential store) where a user with the role of Operator (Write) could create, delete, view existing keys which are outside the intended role.	3.7	More Details
CVE-2022-37010	In JetBrains IntelliJ IDEA before 2022.2 email address validation in the "Git User Name Is Not Defined" dialog was missed	3.6	More Details
CVE-2022-35921	fof/byobu is a private discussions extension for Flarum forum. Affected versions were found to not respect private discussion disablement by users. Users of Byobu should update the extension to version 1.1.7, where this has been patched. Users of Byobu with Flarum 1.0 or 1.1 should upgrade to Flarum 1.2 or later, or evaluate the impact this issue has on your forum's users and choose to disable the extension if needed. There are no workarounds for this issue.	3.5	More Details
CVE-2022-2579	A vulnerability, which was classified as problematic, was found in SourceCodester Garage Management System 1.0. Affected is an unknown function of the file /php_action/createUser.php. The manipulation of the argument userName with the input lala<img src="" onerror=alert(1)> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36343	Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in ideasToCode Enable SVG, WebP & ICO Upload plugin <= 1.0.1 at WordPress.	3.4	More Details
CVE-2022-31186	NextAuth.js is a complete open source authentication solution for Next.js applications. An information disclosure vulnerability in `next-auth` before `v4.10.2` and `v3.29.9` allows an attacker with log access privilege to obtain excessive information such as an identity provider's secret in the log (which is thrown during OAuth error handling) and use it to leverage further attacks on the system, like impersonating the client to ask for extensive permissions. This issue has been patched in `v4.10.2` and `v3.29.9` by moving the log for `provider` information to the debug level. In addition, we added a warning for having the `debug: true` option turned on in production. If for some reason you cannot upgrade, you can user the `logger` configuration option by sanitizing the logs.	3.3	More Details
CVE-2022-22326	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856.	3.3	More Details
CVE-2022-33994	The Gutenberg plugin through 13.7.3 for WordPress allows stored XSS by the Contributor role via an SVG document to the "Insert from URL" feature. NOTE: the XSS payload does not execute in the context of the WordPress instance's domain; however, analogous attempts by low-privileged users to reference SVG documents are blocked by some similar products, and this behavioral difference might have security relevance to some WordPress site administrators.	3.0	More Details
CVE-2022-31177	Flask-AppBuilder is an application development framework built on top of Flask python framework. In versions prior to 4.1.3 an authenticated Admin user could query other users by their salted and hashed passwords strings. These filters could be made by using partial hashed password strings. The response would not include the hashed passwords, but an attacker could infer partial password hashes and their respective users. This issue has been fixed in version 4.1.3. Users are advised to upgrade. There are no known workarounds for this issue.	2.7	More Details
CVE-2016-4981	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-4982. Reason: This candidate is a duplicate of CVE-2016-4982. Notes: All CVE users should reference CVE-2016-4982 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3601	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. OpenSSL does not class this issue as a security vulnerability. The trusted CA store should not contain anything that the user does not trust to issue other certificates. Notes: https://github.com/openssl/openssl/issues/5236#issuecomment-119646061	N/A	More Details
CVE-2016-3692	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 2016. Notes: none	N/A	More Details
CVE-2016-6326	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 2016. Notes: none	N/A	More Details
CVE-2016-7029	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 2016. Notes: none	N/A	More Details
CVE-2016-2122	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 2016. Notes: none	N/A	More Details
CVE-2016-6324	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 2016. Notes: none	N/A	More Details
CVE-2016-6315	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 2016. Notes: none	N/A	More Details
CVE-2016-6314	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 2016. Notes: none	N/A	More Details
CVE-2016-5428	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 2016. Notes: none	N/A	More Details
CVE-2016-5415	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 2016. Notes: none	N/A	More Details
CVE-2016-5413	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 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-4458	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 2016. Notes: none	N/A	More Details
CVE-2016-4452	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 2016. Notes: none	N/A	More Details
CVE-2016-3730	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 2016. Notes: none	N/A	More Details
CVE-2016-3701	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 2016. Notes: none	N/A	More Details
CVE-2016-3700	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 2016. Notes: none	N/A	More Details
CVE-2016-0786	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 2016. Notes: none	N/A	More Details
CVE-2016-2101	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 2016. Notes: none	N/A	More Details
CVE-2016-7049	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 2016. Notes: none	N/A	More Details