SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 April 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-2022-22570	A buffer overflow vulnerability found in the UniFi Door Access Reader Lite's (UA Lite) firmware (Version 3.8.28.24 and earlier) allows a malicious actor who has gained access to a network to control all connected UA devices. This vulnerability is fixed in Version 3.8.31.13 and later.	10.0	More Details
CVE-2022-24796	RaspberryMatic is a free and open-source operating system for running a cloud-free smart-home using the homematicIP / HomeMatic hardware line of IoT devices. A Remote Code Execution (RCE) vulnerability in the file upload facility of the WebUI interface of RaspberryMatic exists. Missing input validation/sanitization in the file upload mechanism allows remote, unauthenticated attackers with network access to the WebUI interface to achieve arbitrary operating system command execution via shell metacharacters in the HTTP query string. Injected commands are executed as root, thus leading to a full compromise of the underlying system and all its components. Versions after `2.31.25.20180428` and prior to `3.63.8.20220330` are affected. Users are advised to update to version `3.63.8.20220330` or newer. There are currently no known workarounds to mitigate the security impact and users are advised to update to the latest version available.	10.0	More Details
CVE-2021-32933	An attacker could leverage an API to pass along a malicious file that could then manipulate the process creation command line in MDT AutoSave versions prior to v6.02.06 and run a command line argument. This could then be leveraged to run a malicious process.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24803	Asciidoctor-include-ext is Asciidoctor's standard include processor reimplemented as an extension. Versions prior to 0.4.0, when used to render user-supplied input in AsciiDoc markup, may allow an attacker to execute arbitrary system commands on the host operating system. This attack is possible even when `allow-uri-read` is disabled! The problem has been patched in the referenced commits.	10.0	More Details
CVE-2022-0939	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18.	9.9	More Details
CVE-2020-24769	SQL injection vulnerability in takeconfirm.php in NexusPHP 1.5 allows remote attackers to execute arbitrary SQL commands via the classes parameter.	9.8	More Details
CVE-2022-25569	Bettini Srl GAMS Product Line v4.3.0 was discovered to re-use static SSH keys across installations, allowing unauthenticated attackers to login as root users via extracting a key from the software.	9.8	More Details
CVE-2021-32986	After Automation Direct CLICK PLC CPU Modules: C0-1x CPUs with firmware prior to v3.00 is unlocked by an authorized user, the unlocked state does not timeout. If the programming software is interrupted, the PLC remains unlocked. All subsequent programming connections are allowed without authorization. The PLC is only relocked by a power cycle, or when the programming software disconnects correctly.	9.8	More Details
CVE-2021-32984	All programming connections receive the same unlocked privileges, which can result in a privilege escalation. During the time Automation Direct CLICK PLC CPU Modules: C0-1x CPUs with firmware prior to v3.00 is unlocked by an authorized user, an attacker can connect to the PLC and read the project without authorization.	9.8	More Details
CVE-2021-32980	Automation Direct CLICK PLC CPU Modules: C0-1x CPUs with firmware prior to v3.00 does not protect against additional software programming connections. An attacker can connect to the PLC while an existing connection is already active.	9.8	More Details
CVE-2021-30064	On Schneider Electric ConneXium Tofino Firewall TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and Belden Tofino Xenon Security Appliance, an SSH login can succeed with hardcoded default credentials (if the device is in the uncommissioned state).	9.8	More Details
CVE-2022-24231	Simple Student Information System v1.0 was discovered to contain a SQL injection vulnerability via add/Student.	9.8	More Details
CVE-2022-28381	Mediaserver.exe in ALLMediaServer 1.6 has a stack-based buffer overflow that allows remote attackers to execute arbitrary code via a long string to TCP port 888, a related issue to CVE-2017-17932.	9.8	More Details
CVE-2022-28368	Dompdf 1.2.1 allows remote code execution via a .php file in the src:url field of an @font-face Cascading Style Sheets (CSS) statement (within an HTML input file).	9.8	More Details
CVE-2022-27534	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27177	A Python format string issue leading to information disclosure and potentially remote code execution in ConsoleMe for all versions prior to 1.2.2	9.8	More Details
CVE-2022-26585	Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.	9.8	More Details
CVE-2021-33207	The HTTP client in MashZone NextGen through 10.7 GA deserializes untrusted data when it gets an HTTP response with a 570 status code.	9.8	More Details
CVE-2022-22965	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.	9.8	More Details
CVE-2022-26628	Matrimony v1.0 was discovered to contain a SQL injection vulnerability via the Password parameter.	9.8	More Details
CVE-2022-28467	Online Student Admission v1.0 was discovered to contain a SQL injection vulnerability via the txtapplicationID parameter.	9.8	More Details
CVE-2022-28116	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter.	9.8	More Details
CVE-2022-28115	Online Sports Complex Booking v1.0 was discovered to contain a SQL injection vulnerability via the id parameter.	9.8	More Details
CVE-2022-27304	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via the user parameter.	9.8	More Details
CVE-2022-27124	Insurance Management System 1.0 was discovered to contain a SQL injection vulnerability via the username parameter.	9.8	More Details
CVE-2022-27123	Employee Performance Evaluation v1.0 was discovered to contain a SQL injection vulnerability via the email parameter.	9.8	More Details
CVE-2022-28219	Cewolf in Zoho ManageEngine ADAudit Plus before 7060 is vulnerable to an unauthenticated XXE attack that leads to Remote Code Execution.	9.8	More Details
CVE-2022-1212	Use-After-Free in str_escape in mruby/mruby in GitHub repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26635	PHP-Memcached v2.2.0 and below contains an improper NULL termination which allows attackers to execute CLRF injection. Note: Third parties have disputed this as not affecting PHP-Memcached directly.	9.8	More Details
CVE-2021-41752	Stack overflow vulnerability in Jerryscript before commit e1ce7dd7271288be8c0c8136eea9107df73a8ce2 on Oct 20, 2021 due to an unbounded recursive call to the new opt() function.	9.8	More Details
CVE-2021-41751	Buffer overflow vulnerability in file ecma-builtin-array-prototype.c:909 in function ecma_builtin_array_prototype_object_slice in Jerryscript before commit e1ce7dd7271288be8c0c8136eea9107df73a8ce2 on Oct 20, 2021.	9.8	More Details
CVE-2021-30080	An issue was discovered in the route lookup process in beego before 1.12.11 that allows attackers to bypass access control.	9.8	More Details
CVE-2021-28428	File upload vulnerability in HorizontCMS before 1.0.0-beta.3 via uploading a .htaccess and *.hello files using the Media Files upload functionality. The original file upload vulnerability (CVE-2020-27387) was remediated by restricting the PHP extensions; however, we confirmed that the filter was bypassed via uploading an arbitrary .htaccess and *.hello files in order to execute PHP code to gain RCE.	9.8	More Details
CVE-2020-19229	Jeesite 1.2.7 uses the apache shiro version 1.2.3 affected by CVE-2016-4437. Because of this version of the java deserialization vulnerability, an attacker could exploit the vulnerability to execute arbitrary commands via the rememberMe parameter.	9.8	More Details
CVE-2020-24770	SQL injection vulnerability in modrules.php in NexusPHP 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2022-28468	Payroll Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter.	9.8	More Details
CVE-2021-43479	A Remote Code Execution (RCE) vulnerability exists in The-Secretary 2.5 via install.php.	9.8	More Details
CVE-2022-23795	An issue was discovered in Joomla! 2.5.0 through 3.10.6 & 4.0.0 through 4.1.0. A user row was not bound to a specific authentication mechanism which could under very special circumstances allow an account takeover.	9.8	More Details
CVE-2022-23799	An issue was discovered in Joomla! 4.0.0 through 4.1.0. Under specific circumstances, JInput pollutes method-specific input bags with $_REQUEST data.	9.8	More Details
CVE-2021-46007	totolink a3100r V5.9c.4577 is vulnerable to os command injection. The backend of a page is executing the "ping" command, and the input field does not adequately filter special symbols. This can lead to command injection attacks.	9.8	More Details
CVE-2021-46009	In Totolink A3100R V5.9c.4577, multiple pages can be read by curl or Burp Suite without authentication. Additionally, admin configurations can be set without cookies.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26645	A remote code execution (RCE) vulnerability in Online Banking System Protect v1.0 allows attackers to execute arbitrary code via a crafted PHP file uploaded through the Upload Image function.	9.8	More Details
CVE-2022-26646	Online Banking System Protect v1.0 was discovered to contain a local file inclusion (LFI) vulnerability via the pages parameter.	9.8	More Details
CVE-2022-24136	Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then execute it.	9.8	More Details
CVE-2021-43506	An SQL Injection vulnerability exists in Sourcecodester Simple Client Management System 1.0 via the password parameter in Login.php.	9.8	More Details
CVE-2021-43484	A Remote Code Execution (RCE) vulnerability exists in Simple Client Management System 1.0 in create.php due to the failure to validate the extension of the file being sent in a request.	9.8	More Details
CVE-2022-22963	In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources.	9.8	More Details
CVE-2022-23797	An issue was discovered in Joomla! 3.0.0 through 3.10.6 & 4.0.0 through 4.1.0. Inadequate filtering on the selected Ids on an request could resulted into an possible SQL injection.	9.8	More Details
CVE-2021-43722	D-Link DIR-645 1.03 A1 is vulnerable to Buffer Overflow. The hnap_main function in the cgibin handler uses sprintf to format the soapaction header onto the stack and has no limit on the size.	9.8	More Details
CVE-2022-28209	An issue was discovered in Mediawiki through 1.37.1. The check for the override-antispoof permission in the AntiSpoof extension is incorrect.	9.8	More Details
CVE-2022-28206	An issue was discovered in MediaWiki through 1.37.1. ImportPlanValidator.php in the FileImporter extension mishandles the check for edit rights.	9.8	More Details
CVE-2022-28205	An issue was discovered in MediaWiki through 1.37.1. The CentralAuth extension mishandles a ttl issue for groups expiring in the future.	9.8	More Details
CVE-2021-44135	pagekit all versions, as of 15-10-2021, is vulnerable to SQL Injection via Comment listing.	9.8	More Details
CVE-2022-24693	Baicells Nova436Q and Neutrino 430 devices with firmware through QRTB 2.7.8 have hardcoded credentials that are easily discovered, and can be used by remote attackers to authenticate via ssh. (The credentials are stored in the firmware, encrypted by the crypt function.)	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26562	An issue in provider/libserver/ECKrbAuth.cpp of Kopano Core <= v11.0.2.51 contains an issue which allows attackers to authenticate even if the user account or password is expired. It also exists in the predecessor Zarafa Collaboration Platform (ZCP) in provider/libserver/ECPamAuth.cpp of Zarafa >= 6.30 (introduced between 6.30.0 RC1e and 6.30.8 final).	9.8	More Details
CVE-2021-23247	A command injection vulerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine	9.8	More Details
CVE-2021-32953	An attacker could utilize SQL commands to create a new user MDT AutoSave versions prior to v6.02.06 and update the user's permissions, granting the attacker the ability to login.	9.8	More Details
CVE-2021-32974	Improper input validation in the built-in web server in Moxa NPort IAW5000A-I/O series firmware version 2.2 or earlier may allow a remote attacker to execute commands.	9.8	More Details
CVE-2021-32976	Five buffer overflows in the built-in web server in Moxa NPort IAW5000A-I/O series firmware version 2.2 or earlier may allow a remote attacker to initiate a denial-of-service attack and execute arbitrary code.	9.8	More Details
CVE-2021-43142	An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.	9.8	More Details
CVE-2022-0452	Use after free in Safe Browsing in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2022-0466	Inappropriate implementation in Extensions Platform in Google Chrome prior to 98.0.4758.80 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2022-0790	Use after free in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-1942	Improper handling of permissions of a shared memory region can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.3	More Details
CVE-2022-28223	Tekon KIO devices through 2022-03-30 allow an authenticated admin user to escalate privileges to root by uploading a malicious Lua plugin.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25157	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions, Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions, Mitsubishi Electric MELSEC iQ-R series R00/01/02CPU all versions, Mitsubishi Electric MELSEC iQ-R series R04/08/16/32/120(EN)CPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120SFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PSFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R16/32/64MTCPU all versions, Mitsubishi Electric MELSEC iQ-R series RJ71C24(-R2/R4) all versions, Mitsubishi Electric MELSEC iQ-R series RJ71EN71 all versions, Mitsubishi Electric MELSEC iQ-R series RJ71GF11-T2 all versions, Mitsubishi Electric MELSEC iQ-R series RJ71GP21(S)-SX all versions, Mitsubishi Electric MELSEC iQ-R series RJ72GF15-T2 all versions, Mitsubishi Electric MELSEC Q series Q03UDECPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/10/13/20/26/50/100UDEHCPU all versions, Mitsubishi Electric MELSEC Q series Q03/04/06/13/26UDVCPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/13/26UDPVCPU all versions, Mitsubishi Electric MELSEC Q series QJ71C24N(-R2/R4) all versions, Mitsubishi Electric MELSEC Q series QJ71E71-100 all versions, Mitsubishi Electric MELSEC L series L02/06/26CPU(-P) all versions, Mitsubishi Electric MELSEC L series L26CPU-(P)BT all versions, Mitsubishi Electric MELSEC L series LJ71C24(-R2) all versions, Mitsubishi Electric MELSEC L series LJ71E71-100 all versions and Mitsubishi Electric MELSEC L series LJ72GF15-T2 all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash.	9.1	More Details
CVE-2022-24790	Puma is a simple, fast, multi-threaded, parallel HTTP 1.1 server for Ruby/Rack applications. When using Puma behind a proxy that does not properly validate that the incoming HTTP request matches the RFC7230 standard, Puma and the frontend proxy may disagree on where a request starts and ends. This would allow requests to be smuggled via the front-end proxy to Puma. The vulnerability has been fixed in 5.6.4 and 4.3.12. Users are advised to upgrade as soon as possible. Workaround: when deploying a proxy in front of Puma, turning on any and all functionality to make sure that the request matches the RFC7230 standard.	9.1	More Details
CVE-2022-1162	A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts	9.1	More Details
CVE-2022-26546	Hospital Management System v1.0 was discovered to lack an authorization component, allowing attackers to access sensitive information and obtain the admin password.	9.1	More Details
CVE-2022-25017	Hitron CHITA 7.2.2.0.3b6-CD devices contain a command injection vulnerability via the Device/DDNS ddnsUsername field.	9.1	More Details
CVE-2022-0990	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1165	The Blackhole for Bad Bots WordPress plugin before 3.3.2 uses headers such as CF-CONNECTING-IP, CLIENT-IP etc to determine the IP address of requests hitting the blackhole URL, which allows them to be spoofed. This could result in blocking arbitrary IP addresses, such as legitimate/good search engine crawlers / bots. This could also be abused by competitors to cause damage related to visibility in search engines, can be used to bypass arbitrary blocks caused by this plugin, block any visitor or even the administrator and even more.	9.1	More Details
CVE-2022-26530	swaylock before 1.6 allows attackers to trigger a crash and achieve unlocked access to a Wayland compositor.	9.1	More Details
CVE-2022-25158	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions, Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions, Mitsubishi Electric MELSEC iQ-R series R00/01/02CPU all versions, Mitsubishi Electric MELSEC iQ-R series R04/08/16/32/120(EN)CPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120SFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PSFCPU all versions, Mitsubishi Electric MELSEC iQ-R series RJ71C24(-R2/R4) all versions, Mitsubishi Electric MELSEC iQ-R series RJ71EN71 all versions, Mitsubishi Electric MELSEC iQ-R series RJ71GF11-T2 all versions, Mitsubishi Electric MELSEC iQ-R series RJ71GP21(S)-SX all versions, Mitsubishi Electric MELSEC iQ-R series RJ72GF15-T2 all versions, Mitsubishi Electric MELSEC Q series Q03UDECPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/10/13/20/26/50/100UDEHCPU all versions, Mitsubishi Electric MELSEC Q series Q03/04/06/13/26UDVCPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/13/26UDPVCPU all versions, Mitsubishi Electric MELSEC Q series QJ71C24N(-R2/R4) all versions, Mitsubishi Electric MELSEC Q series QJ71E71-100 all versions, Mitsubishi Electric MELSEC L series L02/06/26CPU(-P) all versions, Mitsubishi Electric MELSEC L series L26CPU-(P)BT all versions, Mitsubishi Electric MELSEC L series LJ71C24(-R2) all versions, Mitsubishi Electric MELSEC L series LJ71E71-100 all versions and Mitsubishi Electric MELSEC L series LJ72GF15-T2 all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2015-3298	Yubico ykneo-openpgp before 1.0.10 has a typo in which an invalid PIN can be used. When first powered up, a signature will be issued even though the PIN has not been validated.	8.8	More Details
CVE-2021-43464	A Remiote Code Execution (RCE) vulnerability exiss in Subrion CMS 4.2.1 via modified code in a background field; when the information is modified, the data in it will be executed through eval().	8.8	More Details
CVE-2021-33008	AVEVA System Platform versions 2017 through 2020 R2 P01 does not perform any authentication for functionality that requires a provable user identity.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0603	Use after free in File Manager in Google Chrome on Chrome OS prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0604	Heap buffer overflow in Tab Groups in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0605	Use after free in Webstore API in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and convinced a user to enage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0606	Use after free in ANGLE in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0607	Use after free in GPU in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0608	Integer overflow in Mojo in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0609	Use after free in Animation in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0610	Inappropriate implementation in Gamepad API in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-23732	A path traversal vulnerability was identified in GitHub Enterprise Server management console that allowed the bypass of CSRF protections. This could potentially lead to privilege escalation. To exploit this vulnerability, an attacker would need to target a user that was actively logged into the management console. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.5 and was fixed in versions 3.1.19, 3.2.11, 3.3.6, 3.4.1. This vulnerability was reported via the GitHub Bug Bounty program.	8.8	More Details
CVE-2022-0453	Use after free in Reader Mode in Google Chrome prior to 98.0.4758.80 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-2022-0454	Heap buffer overflow in ANGLE in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-44312	An issue was discovered in Firmware Analysis and Comparison Tool v3.2. Logged in administrators could be targeted by a CSRF attack through visiting a crafted web page.	8.8	More Details
CVE-2022-0457	Type confusion in V8 in Google Chrome prior to 98.0.4758.80 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-2022-0458	Use after free in Thumbnail Tab Strip in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-24814	Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 9.7.0, unauthorized JavaScript (JS) can be executed by inserting an iframe into the rich text html interface that links to a file uploaded HTML file that loads another uploaded JS file in its script tag. This satisfies the regular content security policy header, which in turn allows the file to run any arbitrary JS. This issue was resolved in version 9.7.0. As a workaround, disable the live embed in the what-you-see-is-what-you-get by adding `{ "media_live_embeds": false }` to the _Options Overrides_ option of the Rich Text HTML interface.	8.8	More Details
CVE-2022-28062	Car Rental System v1.0 contains an arbitrary file upload vulnerability via the Add Car component which allows attackers to upload a webshell and execute arbitrary code.	8.8	More Details
CVE-2022-0460	Use after free in Window Dialogue in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-27435	An unrestricted file upload at /public/admin/index.php?add_product of Ecommerce-Website v1.1.0 allows attackers to upload a webshell via the Product Image component.	8.8	More Details
CVE-2021-46008	In totolink a3100r V5.9c.4577, the hard-coded telnet password can be discovered from official released firmware. An attacker, who has connected to the Wi-Fi, can easily telnet into the target with root shell if the telnet is function turned on.	8.8	More Details
CVE-2021-46010	Totolink A3100R V5.9c.4577 suffers from Use of Insufficiently Random Values via the web configuration. The SESSION_ID is predictable. An attacker can hijack a valid session and conduct further malicious operations.	8.8	More Details
CVE-2022-25008	totolink EX300_v2 V4.0.3c.140_B20210429 and EX1200T V4.1.2cu.5230_B20210706 does not contain an authentication mechanism.	8.8	More Details
CVE-2022-22986	Netcommunity OG410X and OG810X series (Netcommunity OG410Xa, OG410Xi, OG810Xa, and OG810Xi firmware Ver.2.28 and earlier) allow an attacker on the adjacent network to execute an arbitrary OS command via a specially crafted config file.	8.8	More Details
CVE-2022-24299	Improper input validation vulnerability in pfSense CE and pfSense Plus (pfSense CE software versions prior to 2.6.0 and pfSense Plus software versions prior to 22.01) allows a remote attacker with the privilege to change OpenVPN client or server settings to execute an arbitrary command.	8.8	More Details
CVE-2022-26019	Improper access control vulnerability in pfSense CE and pfSense Plus (pfSense CE software versions prior to 2.6.0 and pfSense Plus software versions prior to 22.01) allows a remote attacker with the privilege to change NTP GPS settings to rewrite existing files on the file system, which may result in arbitrary command execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25915	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors.	8.8	More Details
CVE-2021-34257	Multiple Remote Code Execution (RCE) vulnerabilities exist in WPanel 4 4.3.1 and below via a malicious PHP file upload to (1) Dashboard's Avatar image, (2) Posts Folder image, (3) Pages Folder image and (4) Gallery Folder image.	8.8	More Details
CVE-2021-36625	An SQL Injection vulnerability exists in Dolibarr ERP/CRM 13.0.2 (fixed version is 14.0.0) via a POST request to the country_id parameter in an UPDATE statement.	8.8	More Details
CVE-2021-39772	In Bluetooth, there is a possible way to access the a2dp audio control switch 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.Product: AndroidVersions: Android-12LAndroid ID: A-181962322	8.8	More Details
CVE-2021-33657	There is a heap overflow problem in video/SDL_pixels.c in SDL (Simple DirectMedia Layer) 2.x to 2.0.18 versions. By crafting a malicious .BMP file, an attacker can cause the application using this library to crash, denial of service or Code execution.	8.8	More Details
CVE-2022-28391	BusyBox through 1.35.0 allows remote attackers to execute arbitrary code if netstat is used to print a DNS PTR record's value to a VT compatible terminal. Alternatively, the attacker could choose to change the terminal's colors.	8.8	More Details
CVE-2022-27249	An unrestricted file upload vulnerability in IdeaRE RefTree before 2021.09.17 allows remote authenticated users to execute arbitrary code by using UploadDwg to upload a crafted aspx file to the web root, and then visiting the URL for this aspx resource.	8.8	More Details
CVE-2021-36775	a Improper Access Control vulnerability in SUSE Rancher allows users to keep privileges that should have been revoked. This issue affects: SUSE Rancher Rancher versions prior to 2.4.18; Rancher versions prior to 2.5.12; Rancher versions prior to 2.6.3.	8.8	More Details
CVE-2021-36776	A Improper Access Control vulnerability in SUSE Rancher allows remote attackers impersonate arbitrary users. This issue affects: SUSE Rancher Rancher versions prior to 2.5.10.	8.8	More Details
CVE-2022-0459	Use after free in Screen Capture in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process and convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0456	Use after free in Web Search in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via profile destruction.	8.8	More Details
CVE-2022-0463	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0798	Use after free in MediaStream in Google Chrome prior to 99.0.4844.51 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-2022-27432	A Cross-Site Request Forgery (CSRF) in Pluck CMS v4.7.15 allows attackers to change the password of any given user by exploiting this feature leading to account takeover.	8.8	More Details
CVE-2022-24978	Zoho ManageEngine ADAudit Plus before 7055 allows authenticated Privilege Escalation on Integrated products. This occurs because a password field is present in a JSON response.	8.8	More Details
CVE-2022-24780	Combodo iTop is a web based IT Service Management tool. In versions prior to 2.7.6 and 3.0.0, users of the iTop user portal can send TWIG code to the server by forging specific http queries, and execute arbitrary code on the server using http server user privileges. This issue is fixed in versions 2.7.6 and 3.0.0. There are currently no known workarounds.	8.8	More Details
CVE-2022-26630	Jellycms v3.8.1 and below was discovered to contain an arbitrary file upload vulnerability via \app.\admin\Controllers\db.php.	8.8	More Details
CVE-2021-38834	easy-mock v1.5.0-v1.6.0 allows remote attackers to bypass the vm2 sandbox and execute arbitrary system commands through special js code.	8.8	More Details
CVE-2021-39114	Affected versions of Atlassian Confluence Server and Data Center allow users with a valid account on a Confluence Data Center instance to execute arbitrary Java code or run arbitrary system commands by injecting an OGNL payload. The affected versions are before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.	8.8	More Details
CVE-2021-45891	An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4., that allows attackers to escalate privileges within the application, since all permission checks are done client-side, not server-side.	8.8	More Details
CVE-2022-0464	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.	8.8	More Details
CVE-2022-0808	Use after free in Chrome OS Shell in Google Chrome on Chrome OS prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in a series of user interaction to potentially exploit heap corruption via user interactions.	8.8	More Details
CVE-2022-0805	Use after free in Browser Switcher in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.	8.8	More Details
CVE-2022-0800	Heap buffer overflow in Cast UI in Google Chrome prior to 99.0.4844.51 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-2022-0799	Insufficient policy enforcement in Installer in Google Chrome on Windows prior to 99.0.4844.51 allowed a remote attacker to perform local privilege escalation via a crafted offline installer file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0809	Out of bounds memory access in WebXR in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0467	Inappropriate implementation in Pointer Lock in Google Chrome on Windows prior to 98.0.4758.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	8.8	More Details
CVE-2022-0797	Out of bounds memory access in Mojo in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	8.8	More Details
CVE-2022-0796	Use after free in Media in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0795	Type confusion in Blink Layout in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0794	Use after free in WebShare in Google Chrome prior to 99.0.4844.51 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-2022-0793	Use after free in Cast in Google Chrome prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2022-0791	Use after free in Omnibox in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via user interactions.	8.8	More Details
CVE-2022-0789	Heap buffer overflow in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0470	Out of bounds memory access in V8 in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0469	Use after free in Cast in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0465	Use after free in Extensions in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via user interaction.	8.8	More Details
CVE-2022-0468	Use after free in Payments in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-1190	Improper handling of user input in GitLab CE/EE versions 8.3 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to exploit a stored XSS by abusing multi-word milestone references in issue descriptions, comments, etc.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1175	Improper neutralization of user input in GitLab CE/EE versions 14.4 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to exploit XSS by injecting HTML in notes.	8.7	More Details
CVE-2022-1026	Kyocera multifunction printers running vulnerable versions of Net View unintentionally expose sensitive user information, including usernames and passwords, through an insufficiently protected address book export function.	8.6	More Details
CVE-2021-32960	Rockwell Automation FactoryTalk Services Platform v6.11 and earlier, if FactoryTalk Security is enabled and deployed contains a vulnerability that may allow a remote, authenticated attacker to bypass FactoryTalk Security policies based on the computer name. If successfully exploited, this may allow an attacker to have the same privileges as if they were logged on to the client machine.	8.5	More Details
CVE-2022-22772	The cfsend, cfrecv, and CyberResp components of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for UNIX and TIBCO Managed File Transfer Platform Server for z/Linux contain a difficult to exploit Remote Code Execution (RCE) vulnerability that allows a low privileged attacker with network access to execute arbitrary code on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for UNIX: versions 8.1.0 and below and TIBCO Managed File Transfer Platform Server for z/Linux: versions 8.1.0 and below.	8.5	More Details
CVE-2021-35115	Improper handling of multiple session supported by PVM backend can lead to use after free in Snapdragon Auto, Snapdragon Mobile	8.4	More Details
CVE-2021-35105	Possible out of bounds access due to improper input validation during graphics profiling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-35089	Possible buffer overflow due to lack of input IB amount validation while processing the user command in Snapdragon Auto	8.4	More Details
CVE-2022-28651	In JetBrains IntelliJ IDEA before 2021.3.3 it was possible to get passwords from protected fields	8.4	More Details
CVE-2022-21947	A Exposure of Resource to Wrong Sphere vulnerability in Rancher Desktop of SUSE allows attackers in the local network to connect to the Dashboard API (steve) to carry out arbitrary actions. This issue affects: SUSE Rancher Desktop versions prior to V.	8.3	More Details
CVE-2022-24475	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26891	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26894	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26895	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26900	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26908	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26909	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26912	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2021-35088	Possible out of bound read due to improper validation of IE length during SSID IE parse when channel is DFS in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.2	More Details
CVE-2021-35117	An Out of Bounds read may potentially occur while processing an IBSS beacon, in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	8.2	More Details
CVE-2021-33020	Philips Vue PACS versions 12.2.x.x and prior uses a cryptographic key or password past its expiration date, which diminishes its safety significantly by increasing the timing window for cracking attacks against that key.	8.2	More Details
CVE-2022-1235	Weak secrethash can be brute-forced in GitHub repository livehelperchat/livehelperchat prior to 3.96.	8.2	More Details
CVE-2022-0403	The Library File Manager WordPress plugin before 5.2.3 is using an outdated version of the elFinder library, which is know to be affected by security issues (CVE-2021-32682), and does not have any authorisation as well as CSRF checks in its connector AJAX action, allowing any authenticated users, such as subscriber to call it. Furthermore, as the options passed to the elFinder library does not restrict any file type, users with a role as low as subscriber can Create/Upload/Delete Arbitrary files and folders.	8.1	More Details
CVE-2021-43664	totolink EX300_v2 V4.0.3c.140_B20210429 was discovered to contain a command injection vulnerability via the component process forceugpo.	8.1	More Details
CVE-2021-35110	Possible buffer overflow to improper validation of hash segment of file while allocating memory in Snapdragon Connectivity, Snapdragon Mobile	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24802	deepmerge-ts is a typescript library providing functionality to deep merging of javascript objects. deepmerge-ts is vulnerable to Prototype Pollution via file deepmerge.ts, function defaultMergeRecords(). This issue has been patched in version 4.0.2. There are no known workarounds for this issue.	8.1	More Details
CVE-2022-21235	The package github.com/masterminds/vcs before 1.13.3 are vulnerable to Command Injection via argument injection. When hg is executed, argument strings are passed to hg in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-21223	The package cocoapods-downloader before 1.6.2 are vulnerable to Command Injection via hg argument injection. When calling the download function (when using hg), the url (and/or revision, tag, branch) is passed to the hg clone command in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-24440	The package cocoapods-downloader before 1.6.0, from 1.6.2 and before 1.6.3 are vulnerable to Command Injection via git argument injection. When calling the Pod::Downloader.preprocess_options function and using git, both the git and branch parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-24066	The package simple-git before 3.5.0 are vulnerable to Command Injection due to an incomplete fix of [CVE-2022-24433](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2421199) which only patches against the git fetch attack vector. A similar use of the --upload-pack feature of git is also supported for git clone, which the prior fix didn't cover.	8.1	More Details
CVE-2022-24801	Twisted is an event-based framework for internet applications, supporting Python 3.6+. Prior to version 22.4.0rc1, the Twisted Web HTTP 1.1 server, located in the `twisted.web.http` module, parsed several HTTP request constructs more leniently than permitted by RFC 7230. This non-conformant parsing can lead to desync if requests pass through multiple HTTP parsers, potentially resulting in HTTP request smuggling. Users who may be affected use Twisted Web's HTTP 1.1 server and/or proxy and also pass requests through a different HTTP server and/or proxy. The Twisted Web client is not affected. The HTTP 2.0 server uses a different parser, so it is not affected. The issue has been addressed in Twisted 22.4.0rc1. Two workarounds are available: Ensure any vulnerabilities in upstream proxies have been addressed, such as by upgrading them; or filter malformed requests by other means, such as configuration of an upstream proxy.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24791	Wasmtime is a standalone JIT-style runtime for WebAssembly, using Cranelift. There is a use after free vulnerability in Wasmtime when both running Wasm that uses externrefs and enabling epoch interruption in Wasmtime. If you are not explicitly enabling epoch interruption (it is disabled by default) then you are not affected. If you are explicitly disabling the Wasm reference types proposal (it is enabled by default) then you are also not affected. The use after free is caused by Cranelift failing to emit stack maps when there are safepoints inside cold blocks. Cold blocks occur when epoch interruption is enabled. Cold blocks are emitted at the end of compiled functions, and change the order blocks are emitted versus defined. This reordering accidentally caused Cranelift to skip emitting some stack maps because it expected to emit the stack maps in block definition order, rather than block emission order. When Wasmtime would eventually collect garbage, it would fail to find live references on the stack because of the missing stack maps, think that they were unreferenced garbage, and therefore reclaim them. Then after the collection ended, the Wasm code could use the reclaimed-too-early references, which is a use after free. Patches have been released in versions 0.34.2 and 0.35.2, which fix the vulnerability. All Wasmtime users are recommended to upgrade to these patched versions. If upgrading is not an option for you at this time, you can avoid the vulnerability by either: disabling the Wasm reference types proposal, config.wasm_reference_types(false); or by disabling epoch interruption if you were previously enabling it. config.epoch_interruption(false).	8.1	More Details
CVE-2022-28376	Verizon 5G Home LVSKIHP outside devices through 2022-02-15 allow anyone (knowing the device's serial number) to access a CPE admin website, e.g., at the 10.0.0.1 IP address. The password (for the verizon username) is calculated by concatenating the serial number and the model (i.e., the LVSKIHP string), running the sha256sum program, and extracting the first seven characters concatenated with the last seven characters of that SHA-256 value.	8.1	More Details
CVE-2022-25159	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions, Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions, Mitsubishi Electric MELSEC iQ-R series R00/01/02CPU all versions, Mitsubishi Electric MELSEC iQ-R series R04/08/16/32/120(EN)CPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120SFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PSFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R16/32/64MTCPU all versions, Mitsubishi Electric MELSEC iQ-R series RJ71C24(-R2/R4) all versions, Mitsubishi Electric MELSEC iQ-R series RJ71EN71 all versions, Mitsubishi Electric MELSEC iQ-R series RJ72GF15-T2 all versions, Mitsubishi Electric MELSEC Q series Q03/04/06/13/26UDVCPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/13/26UDPVCPU all versions, Mitsubishi Electric MELSEC Q series QJ71C24N(-R2/R4) all versions and Mitsubishi Electric MELSEC Q series QJ71E71-100 all versions allows a remote unauthenticated attacker to login to the product by replay attack.	8.1	More Details
CVE-2022-1191	SSRF on index.php/cobrowse/proxycss/ in GitHub repository livehelperchat/livehelperchat prior to 3.96.	8.1	More Details
CVE-2022-1213	SSRF filter bypass port 80, 433 in GitHub repository livehelperchat/livehelperchat prior to 3.67v. An attacker could make the application perform arbitrary requests, bypass CVE-2022-1191	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25155	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions, Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions, Mitsubishi Electric MELSEC iQ-R series R00/01/02CPU all versions, Mitsubishi Electric MELSEC iQ-R series R04/08/16/32/120(EN)CPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120SFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PSFCPU all versions, Mitsubishi Electric MELSEC iQ-R series RJ71GN11-T2 all versions, Mitsubishi Electric MELSEC iQ-R series RJ71GN11-EIP all versions, Mitsubishi Electric MELSEC iQ-R series RJ71C24(-R2/R4) all versions, Mitsubishi Electric MELSEC iQ-R series RJ71EN71 all versions, Mitsubishi Electric MELSEC iQ-R series RJ72GF15-T2 all versions, Mitsubishi Electric MELSEC Q series Q03UDECPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/10/13/20/26/50/100UDEHCPU all versions, Mitsubishi Electric MELSEC Q series Q03/04/06/13/26UDVCPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/13/26UDPVCPU all versions, Mitsubishi Electric MELSEC Q series QJ71C24N(-R2/R4) all versions, Mitsubishi Electric MELSEC Q series QJ71E71-100 all versions, Mitsubishi Electric MELSEC Q series QJ72BR15 all versions, Mitsubishi Electric MELSEC Q series QJ72LP25(-25/G/GE) all versions, Mitsubishi Electric MELSEC L series L02/06/26CPU(-P) all versions, Mitsubishi Electric MELSEC L series L26CPU-(P)BT all versions, Mitsubishi Electric MELSEC L series LJ71C24(-R2) all versions, Mitsubishi Electric MELSEC L series LJ71E71-100 all versions and Mitsubishi Electric MELSEC L series LJ72GF15-T2 all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash.	8.1	More Details
CVE-2022-25156	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions, Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions, Mitsubishi Electric MELSEC iQ-R series R00/01/02CPU all versions, Mitsubishi Electric MELSEC iQ-R series R04/08/16/32/120(EN)CPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120SFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PSFCPU all versions, Mitsubishi Electric MELSEC iQ-R series RJ71C24(-R2/R4) all versions, Mitsubishi Electric MELSEC iQ-R series RJ71EN71 all versions, Mitsubishi Electric MELSEC iQ-R series RJ72GF15-T2 all versions, Mitsubishi Electric MELSEC Q series Q03UDECPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/10/13/20/26/50/100UDEHCPU all versions, Mitsubishi Electric MELSEC Q series Q03/04/06/13/26UDVCPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/13/26UDPVCPU all versions, Mitsubishi Electric MELSEC Q series QJ71C24N(-R2/R4) all versions, Mitsubishi Electric MELSEC Q series QJ71E71-100 all versions, Mitsubishi Electric MELSEC Q series QJ72BR15 all versions, Mitsubishi Electric MELSEC Q series QJ72LP25(-25/G/GE) all versions, Mitsubishi Electric MELSEC L series L02/06/26CPU(-P) all versions, Mitsubishi Electric MELSEC L series L26CPU-(P)BT all versions, Mitsubishi Electric MELSEC L series LJ71C24(-R2) all versions, Mitsubishi Electric MELSEC L series LJ71E71-100 all versions and Mitsubishi Electric MELSEC L series LJ72GF15-T2 all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash.	8.1	More Details
CVE-2021-43456	An Unquoted Service Path vulnerablility exists in Rumble Mail Server 0.51.3135 via via a specially crafted file in the RumbleService executable service path.	7.8	More Details
CVE-2021-30333	Improper validation of buffer size input to the EFS file can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43458	An Unquoted Service Path vulnerability exits in Vembu BDR 4.2.0.1 via a specially crafted file in the (1) hsflowd, (2) VembuBDR360Agent, or (3) VembuOffice365Agent service paths.	7.8	More Details
CVE-2021-43457	An Unquoted Service Path vulnerability exists in bVPN 2.5.1 via a specially crafted file in the waselvpnserv service path.	7.8	More Details
CVE-2021-1950	Improper cleaning of secure memory between authenticated users can lead to face authentication bypass in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-27117	An issue was discovered in file profile.go in function GetCPUProfile in beego through 2.0.2, allows attackers to launch symlink attacks locally.	7.8	More Details
CVE-2021-43454	An Unquoted Service Path vulnerability exists in AnyTXT Searcher 1.2.394 via a specially crafted file in the ATService path. .	7.8	More Details
CVE-2022-1154	Use after free in utf_ptr2char in GitHub repository vim/vim prior to 8.2.4646.	7.8	More Details
CVE-2021-43455	An Unquoted Service Path vulnerability exists in FreeLAN 2.2 via a specially crafted file in the FreeLAN Service path.	7.8	More Details
CVE-2021-39767	In miniadb, there is a possible way to get read/write access to recovery system properties due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-201308542	7.8	More Details
CVE-2022-27052	FreeFtpd version 1.0.13 and below contains an unquoted service path vulnerability which allows local users to launch processes with elevated privileges.	7.8	More Details
CVE-2022-27050	BitComet Service for Windows before version 1.8.6 contains an unquoted service path vulnerability which allows attackers to escalate privileges to the system level.	7.8	More Details
CVE-2021-27116	An issue was discovered in file profile.go in function MemProf in beego through 2.0.2, allows attackers to launch symlink attacks locally.	7.8	More Details
CVE-2021-39790	In Dialer, there is a possible way to manipulate visual voicemail settings due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-186405146	7.8	More Details
CVE-2022-28390	ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the Linux kernel through 5.17.1 has a double free.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35103	Possible out of bound write due to improper validation of number of timer values received from firmware while syncing timers in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-39776	In NFC, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-192614125	7.8	More Details
CVE-2022-23909	There is an unquoted service path in Sherpa Connector Service (SherpaConnectorService.exe) 2020.2.20328.2050. This might allow a local user to escalate privileges by creating a "C:\Program Files\Sherpa Software\Sherpa.exe" file.	7.8	More Details
CVE-2021-3847	An unauthorized access to the execution of the setuid file with capabilities flaw in the Linux kernel OverlayFS subsystem was found in the way user copying a capable file from a nosuid mount into another mount. A local user could use this flaw to escalate their privileges on the system.	7.8	More Details
CVE-2021-39771	In Settings, there is a possible way to misrepresent which app wants to add a wifi network due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-198661951	7.8	More Details
CVE-2022-25959	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to memory corruption while processing a specific project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-26022	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to an out-of-bounds write while processing a specific project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-26417	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to a use after free memory condition while processing a specific project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-26624	An local privilege escalation vulnerability due to a "runasroot" command in eScan Anti-Virus. This vulnerability is due to invalid arguments and insufficient execution conditions related to "runasroot" command. This vulnerability can induce remote attackers to exploit root privileges by manipulating parameter values.	7.8	More Details
CVE-2021-26623	A remote code execution vulnerability due to incomplete check for 'xheader_decode_path_record' function's parameter length value in the ark library. Remote attackers can induce exploit malicious code using this function.	7.8	More Details
CVE-2022-26419	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to multiple stack-based buffer overflow conditions while parsing a specific project file, which may allow an attacker to locally execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26358	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption.	7.8	More Details
CVE-2022-26359	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption.	7.8	More Details
CVE-2022-26360	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption.	7.8	More Details
CVE-2022-24426	Dell Command | Update, Dell Update, and Alienware Update version 4.4.0 contains a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation.	7.8	More Details
CVE-2022-26361	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption.	7.8	More Details
CVE-2021-1000	In createBluetoothDeviceSlice of ConnectedDevicesSliceProvider.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-185190688	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23868	RuoYi v4.7.2 contains a CSV injection vulnerability through ruoyi-admin when a victim opens .xlsx log file.	7.8	More Details
CVE-2021-35106	Possible out of bound read due to improper length calculation of WMI message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2021-39764	In Settings, there is a possible way to display an incorrect app name due to improper input validation. This could lead to local escalation of privilege via app spoofing with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-170642995	7.8	More Details
CVE-2021-39768	In Settings, there is a possible way to add an auto-connect WiFi network without the user's consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-202017876	7.8	More Details
CVE-2021-43460	An Unquoted Service Path vulnerability exists in System Explorer 7.0.0 via via a specially crafted file in the SystemExplorerHelpService service executable path.	7.8	More Details
CVE-2021-39763	In Settings, there is a possible way to make the user enable WiFi due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-199176115	7.8	More Details
CVE-2021-39787	In SystemUI, there is a possible arbitrary Activity launch due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-202506934	7.8	More Details
CVE-2021-39743	In PackageManager, there is a possible way to update the last usage time of another package 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.Product: AndroidVersions: Android-12LAndroid ID: A-201534884	7.8	More Details
CVE-2022-1160	heap buffer overflow in get_one_sourceline in GitHub repository vim/vim prior to 8.2.4647.	7.8	More Details
CVE-2022-27772	spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer	7.8	More Details
CVE-2021-39749	In WindowManager, there is a possible way to start non-exported and protected activities 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.Product: AndroidVersions: Android-12LAndroid ID: A-205996115	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39789	In Telecom, there is a possible leak of TTY mode change 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.Product: AndroidVersions: Android-12LAndroid ID: A-203880906	7.8	More Details
CVE-2022-27815	SWHKD 1.1.5 unsafely uses the /tmp/swhkd.pid pathname. There can be an information leak or denial of service.	7.8	More Details
CVE-2021-39750	In PackageManager, there is a possible way to change the splash screen theme of other apps 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.Product: AndroidVersions: Android-12LAndroid ID: A-206474016	7.8	More Details
CVE-2021-39752	In Bubbles, there is a possible way to interfere with Bubbles due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-202756848	7.8	More Details
CVE-2021-39759	In libstagefright, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-180200830	7.8	More Details
CVE-2022-23699	A local authentication restriction bypass vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView.	7.8	More Details
CVE-2021-39758	In WindowManager, there is a possible way to start a foreground activity from the background 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.Product: AndroidVersions: Android-12LAndroid ID: A-205130886	7.8	More Details
CVE-2022-22996	The G-RAID 4/8 Software Utility setups for Windows were affected by a DLL hijacking vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the system user.	7.8	More Details
CVE-2022-20002	In incfs, there is a possible way of mounting on arbitrary paths due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-198657657	7.8	More Details
CVE-2022-0998	An integer overflow flaw was found in the Linux kernel's virtio device driver code in the way a user triggers the vhost_vdpa_config_validate function. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2021-39784	In CellBroadcastReceiver, there is a possible path to enable specific cellular features 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.Product: AndroidVersions: Android-12LAndroid ID: A-200163477	7.8	More Details
CVE-2021-39746	In PermissionController, there is a possible way to delete some local files due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-194696395	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1098	Delta Electronics DIAEnergie (all versions prior to 1.8.02.004) are vulnerable to a DLL hijacking condition. When combined with the Incorrect Default Permissions vulnerability of 4.2.2 above, this makes it possible for an attacker to escalate privileges	7.8	More Details
CVE-2021-43463	An Unquoted Service Path vulnerability exists in Ext2Fsd v0.68 via a specially crafted file in the Ext2Srv Service executable service path.	7.8	More Details
CVE-2022-25348	Untrusted search path vulnerability in AttacheCase ver.4.0.2.7 and earlier allows an attacker to gain privileges and execute arbitrary code via a Trojan horse DLL in an unspecified directory.	7.8	More Details
CVE-2021-39781	In SmsController, there is a possible information disclosure due to a permissions bypass. This could lead to local escalation of privilege and sending sms with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-195311502	7.8	More Details
CVE-2022-28128	Untrusted search path vulnerability in AttacheCase ver.3.6.1.0 and earlier allows an attacker to gain privileges and execute arbitrary code via a Trojan horse DLL in an unspecified directory.	7.8	More Details
CVE-2021-39780	In Traceur, there is a possible bypass of developer settings requirements for capturing system traces due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-204992293	7.8	More Details
CVE-2021-39783	In rcsservice, there is a possible way to modify TTY mode 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.Product: AndroidVersions: Android-12LAndroid ID: A-197960597	7.8	More Details
CVE-2021-39782	In Telephony, there is a possible unauthorized modification of the PLMN SIM file 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.Product: AndroidVersions: Android-12LAndroid ID: A-202760015	7.8	More Details
CVE-2021-1033	In createGeneralSlice of ConnectedDevicesSliceProvider.java.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-185247656	7.8	More Details
CVE-2021-39741	In Keymaster, 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.Product: AndroidVersions: Android-12LAndroid ID: A-173567719	7.8	More Details
CVE-2022-1159	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user.	7.7	More Details
CVE-2021-45031	A vulnerability in MEPSAN's USC+ before version 3.0 has a weakness in login function which lets attackers to generate high privileged accounts passwords.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12266	Stack-based Buffer Overflow vulnerability in Wyze Cam Pan v2, Cam v2, Cam v3 allows an attacker to run arbitrary code on the affected device. This issue affects: Wyze Cam Pan v2 versions prior to 4.49.1.47. Wyze Cam v2 versions prior to 4.9.8.1002. Wyze Cam v3 versions prior to 4.36.8.32.	7.6	More Details
CVE-2020-24771	Incorrect access control in NexusPHP 1.5.beta5.20120707 allows unauthorized attackers to access published content.	7.5	More Details
CVE-2021-22277	Improper Input Validation vulnerability in ABB 800xA, Control Software for AC 800M, Control Builder Safe, Compact Product Suite - Control and I/O, ABB Base Software for SoftControl allows an attacker to cause the denial of service.	7.5	More Details
CVE-2022-28355	randomUUID in Scala.js before 1.10.0 generates predictable values.	7.5	More Details
CVE-2022-23974	In 0.9.3 or older versions of Apache Pinot segment upload path allowed segment directories to be imported into pinot tables. In pinot installations that allow open access to the controller a specially crafted request can potentially be exploited to cause disruption in pinot service. Pinot release 0.10.0 fixes this. See https://docs.pinot.apache.org/basics/releases/0.10.0	7.5	More Details
CVE-2022-24758	The Jupyter notebook is a web-based notebook environment for interactive computing. Prior to version 6.4.9, unauthorized actors can access sensitive information from server logs. Anytime a 5xx error is triggered, the auth cookie and other header values are recorded in Jupyter server logs by default. Considering these logs do not require root access, an attacker can monitor these logs, steal sensitive auth/cookie information, and gain access to the Jupyter server. Jupyter notebook version 6.4.x contains a patch for this issue. There are currently no known workarounds.	7.5	More Details
CVE-2022-26281	BigAnt Server v5.6.06 was discovered to contain an incorrect access control issue.	7.5	More Details
CVE-2022-25598	Apache DolphinScheduler user registration is vulnerable to Regular express Denial of Service (ReDoS) attacks, Apache DolphinScheduler users should upgrade to version 2.0.5 or higher.	7.5	More Details
CVE-2021-27501	Philips Vue PACS versions 12.2.x.x and prior does not follow certain coding rules for development, which can lead to resultant weaknesses or increase the severity of the associated vulnerabilities.	7.5	More Details
CVE-2021-28504	On Arista Strata family products which have “TCAM profile” feature enabled when Port IPv4 access-list has a rule which matches on “vxlan” as protocol then that rule and subsequent rules (rules declared after it in ACL) do not match on IP protocol field as expected.	7.5	More Details
CVE-2022-23698	A remote unauthenticated disclosure of information vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView.	7.5	More Details
CVE-2021-32937	An attacker can gain knowledge of a session temporary working folder where the getfile and putfile commands are used in MDT AutoSave versions prior to v6.02.06. An attacker can leverage this knowledge to provide a malicious command to the working directory where the read and write activity can be initiated.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32945	An attacker could decipher the encryption and gain access to MDT AutoSave versions prior to v6.02.06.	7.5	More Details
CVE-2021-32949	An attacker could utilize a function in MDT AutoSave versions prior to v6.02.06 that permits changing a designated path to another path and traversing the directory, allowing the replacement of an existing file with a malicious file.	7.5	More Details
CVE-2021-32957	A function in MDT AutoSave versions prior to v6.02.06 is used to retrieve system information for a specific process, and this information collection executes multiple commands and summarizes the information into an XML. This function and subsequent process gives full path to the executable and is therefore vulnerable to binary hijacking.	7.5	More Details
CVE-2021-37517	An Access Control vulnerability exists in Dolibarr ERP/CRM 13.0.2, fixed version is 14.0.0,in the forgot-password function becuase the application allows email addresses as usernames, which can cause a Denial of Service.	7.5	More Details
CVE-2022-24132	phpshe V1.8 is affected by a denial of service (DoS) attack in the registry's verification code, which can paralyze the target service.	7.5	More Details
CVE-2021-32961	A getfile function in MDT AutoSave versions prior to v6.02.06 enables a user to supply an optional parameter, resulting in the processing of a request in a special manner. This can result in the execution of an unzip command and place a malicious .exe file in one of the locations the function looks for and get execution capabilities.	7.5	More Details
CVE-2021-32968	Two buffer overflows in the built-in web server in Moxa NPort IAW5000A-I/O Series firmware version 2.2 or earlier may allow a remote attacker to cause a denial-of-service condition.	7.5	More Details
CVE-2021-32970	Data can be copied without validation in the built-in web server in Moxa NPort IAW5000A-I/O series firmware version 2.2 or earlier, which may allow a remote attacker to cause denial-of-service conditions.	7.5	More Details
CVE-2021-33018	The use of a broken or risky cryptographic algorithm in Philips Vue PACS versions 12.2.x.x and prior is an unnecessary risk that may result in the exposure of sensitive information.	7.5	More Details
CVE-2022-1176	Loose comparison causes IDOR on multiple endpoints in GitHub repository livehelperchat/livehelperchat prior to 3.96.	7.5	More Details
CVE-2021-33022	Philips Vue PACS versions 12.2.x.x and prior transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.	7.5	More Details
CVE-2022-27442	TPCMS v3.2 allows attackers to access the ThinkPHP log directory and obtain sensitive information such as the administrator's user name and password.	7.5	More Details
CVE-2022-23793	An issue was discovered in Joomla! 3.0.0 through 3.10.6 & 4.0.0 through 4.1.0. Extracting an specifilcy crafted tar package could write files outside of the intended path.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27649	A flaw was found in Podman, where containers were started incorrectly with non-empty default permissions. A vulnerability was found in Moby (Docker Engine), where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs.	7.5	More Details
CVE-2022-27650	A flaw was found in crun where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs.	7.5	More Details
CVE-2021-44109	A buffer overflow in lib/sbi/message.c in Open5GS 2.3.6 and earlier allows remote attackers to Denial of Service via a crafted sbi request.	7.5	More Details
CVE-2021-45893	An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4. There is Improper Handling of Case Sensitivity, which makes password guessing easier.	7.5	More Details
CVE-2020-25691	A flaw was found in darkhttpd. Invalid error handling allows remote attackers to cause denial-of-service by accessing a file with a large modification date. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2021-30065	On Schneider Electric ConneXium Tofino Firewall TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and Belden Tofino Xenon Security Appliance, crafted ModBus packets can bypass the ModBus enforcer. NOTE: this issue exists because of an incomplete fix of CVE-2017-11401.	7.5	More Details
CVE-2021-32982	Automation Direct CLICK PLC CPU Modules: C0-1x CPUs with firmware prior to v3.00 passwords are sent as plaintext during unlocking and project transfers. An attacker who has network visibility can observe the password exchange.	7.5	More Details
CVE-2021-30063	On Schneider Electric ConneXium Tofino OPCLSM TCSEFM0000 before 03.23 and Belden Tofino Xenon Security Appliance, crafted OPC packets can cause an OPC enforcer denial of service.	7.5	More Details
CVE-2021-32978	The programming protocol allows for a previously entered password and lock state to be read by an attacker. If the previously entered password was successful, the attacker can then use the password to unlock Automation Direct CLICK PLC CPU Modules: C0-1x CPUs with firmware prior to v3.00.	7.5	More Details
CVE-2022-26572	Xerox ColorQube 8580 was discovered to contain an access control issue which allows attackers to print, view the status, and obtain sensitive information.	7.5	More Details
CVE-2021-39762	In tremolo, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-210625816	7.5	More Details
CVE-2022-0709	The Booking Package WordPress plugin before 1.5.29 requires a token for exporting the ical representation of it's booking calendar, but this token is returned in the json response to unauthenticated users performing a booking, leading to a sensitive data disclosure vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24787	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. In version 0.3.1 and prior, bytestrings can have dirty bytes in them, resulting in the word-for-word comparisons giving incorrect results. Even without dirty nonzero bytes, two bytestrings can compare to equal if one ends with `"\x00"` because there is no comparison of the length. A patch is available and expected to be part of the 0.3.2 release. There are currently no known workarounds.	7.5	More Details
CVE-2021-32994	Softing OPC UA C++ SDK (Software Development Kit) versions from 5.59 to 5.64 exported library functions don't properly validate received extension objects, which may allow an attacker to crash the software by sending a variety of specially crafted packets to access several unexpected memory locations.	7.5	More Details
CVE-2021-30332	Possible assertion due to improper validation of OTA configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2020-23349	An intent redirection issue was doscovered in Sina Weibo Android SDK 4.2.7 (com.sina.weibo.sdk.share.WbShareTransActivity), any unexported Activities could be started by the com.sina.weibo.sdk.share.WbShareTransActivity.	7.5	More Details
CVE-2021-30329	Possible assertion due to improper validation of TCI configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-30328	Possible assertion due to improper validation of invalid NR CSI-IM resource configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2022-24785	Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.	7.5	More Details
CVE-2022-26233	Barco Control Room Management through Suite 2.9 Build 0275 was discovered to be vulnerable to directory traversal, allowing attackers to access sensitive information and components. Requests must begin with the "GET /..\.." substring.	7.5	More Details
CVE-2021-30062	On Schneider Electric ConneXium Tofino OPCLSM TCSEFM0000 before 03.23 and Belden Tofino Xenon Security Appliance, crafted OPC packets can bypass the OPC enforcer.	7.5	More Details
CVE-2022-24763	PJSIP is a free and open source multimedia communication library written in the C language. Versions 2.12 and prior contain a denial-of-service vulnerability that affects PJSIP users that consume PJSIP's XML parsing in their apps. Users are advised to update. There are no known workarounds.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24794	Express OpenID Connect is an Express JS middleware implementing sign on for Express web apps using OpenID Connect. Users of the `requiresAuth` middleware, either directly or through the default `authRequired` option, are vulnerable to an Open Redirect when the middleware is applied to a catch all route. If all routes under `example.com` are protected with the `requiresAuth` middleware, a visit to `http://example.com//google.com` will be redirected to `google.com` after login because the original url reported by the Express framework is not properly sanitized. This vulnerability affects versions prior to 2.7.2. Users are advised to upgrade. There are no known workarounds.	7.5	More Details
CVE-2022-22327	IBM UrbanCode Deploy (UCD) 7.0.5, 7.1.0, 7.1.1, and 7.1.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 218859.	7.5	More Details
CVE-2021-43663	totolink EX300_v2 V4.0.3c.140_B20210429 was discovered to contain a command injection vulnerability via the component cloudupdate_check.	7.5	More Details
CVE-2021-44138	There is a Directory traversal vulnerability in Caucho Resin, as distributed in Resin 4.0.52 - 4.0.56, which allows remote attackers to read files in arbitrary directories via a ; in a pathname within an HTTP request.	7.5	More Details
CVE-2022-24798	Internet Routing Registry daemon version 4 is an IRR database server, processing IRR objects in the RPSL format. IRRd did not always filter password hashes in query responses relating to `mntner` objects and database exports. This may have allowed adversaries to retrieve some of these hashes, perform a brute-force search for the clear-text passphrase, and use these to make unauthorised changes to affected IRR objects. This issue only affected instances that process password hashes, which means it is limited to IRRd instances that serve authoritative databases. IRRd instances operating solely as mirrors of other IRR databases are not affected. This has been fixed in IRRd 4.2.3 and the main branch. Versions in the 4.1.x series never were affected. Users of the 4.2.x series are strongly recommended to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2019-9564	A vulnerability in the authentication logic of Wyze Cam Pan v2, Cam v2, Cam v3 allows an attacker to bypass login and control the devices. This issue affects: Wyze Cam Pan v2 versions prior to 4.49.1.47. Wyze Cam v2 versions prior to 4.9.8.1002. Wyze Cam v3 versions prior to 4.36.8.32.	7.5	More Details
CVE-2021-44108	A null pointer dereference in src/amf/namf-handler.c in Open5GS 2.3.6 and earlier allows remote attackers to Denial of Service via a crafted sbi request to amf.	7.5	More Details
CVE-2022-28380	The rc-httpd component through 2022-03-31 for 9front (Plan 9 fork) allows ..%2f directory traversal if serve-static is used.	7.5	More Details
CVE-2021-43008	Improper Access Control in Adminer versions 1.12.0 to 4.6.2 (fixed in version 4.6.3) allows an attacker to achieve Arbitrary File Read on the remote server by requesting the Adminer to connect to a remote MySQL database.	7.5	More Details
CVE-2021-33010	An exception is thrown from a function in AVEVA System Platform versions 2017 through 2020 R2 P01, but it is not caught, which may cause a denial-of-service condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22332	IBM Sterling Partner Engagement Manager 6.2.0 could allow an attacker to impersonate another user due to missing revocation mechanism for the JWT token. IBM X-Force ID: 219131.	7.5	More Details
CVE-2022-26619	Halo Blog CMS v1.4.17 was discovered to allow attackers to upload arbitrary files via the Attachment Upload function.	7.5	More Details
CVE-2022-25584	Seyeon Tech Co., Ltd FlexWATCH FW3170-PS-E Network Video System 4.23-3000_GY allows attackers to access sensitive information.	7.5	More Details
CVE-2019-14839	It was observed that while login into Business-central console, HTTP request discloses sensitive information like username and password when intercepted using some tool like burp suite etc.	7.5	More Details
CVE-2022-1155	Old sessions are not blocked by the login enable function. in GitHub repository snipe/snipe-it prior to 5.3.10.	7.4	More Details
CVE-2022-0088	Cross-Site Request Forgery (CSRF) in GitHub repository yourls/yourls prior to 1.8.3.	7.4	More Details
CVE-2021-42324	An issue was discovered on DCN (Digital China Networks) S4600-10P-SI devices before R0241.0470. Due to improper parameter validation in the console interface, it is possible for a low-privileged authenticated attacker to escape the sandbox environment and execute system commands as root via shell metacharacters in the capture command parameters. Command output will be shown on the Serial interface of the device. Exploitation requires both credentials and physical access.	7.4	More Details
CVE-2022-25154	A DLL hijacking vulnerability in Samsung portable SSD T5 PC software before 1.6.9 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on Windows 7, 10, or 11 to exploit this vulnerability.)	7.3	More Details
CVE-2022-28650	In JetBrains YouTrack before 2022.1.43700 it was possible to inject JavaScript into Markdown in the YouTrack Classic UI	7.3	More Details
CVE-2022-0887	The Easy Social Icons WordPress plugin before 3.1.4 does not sanitize the selected_icons attribute to the cnss_widget before using it in an SQL statement, leading to a SQL injection vulnerability.	7.2	More Details
CVE-2022-0537	The MapPress Maps for WordPress plugin before 2.73.13 allows a high privileged user to bypass the DISALLOW_FILE_EDIT and DISALLOW_FILE_MODS settings and upload arbitrary files to the site through the "ajax_save" function. The file is written relative to the current 's stylesheet directory, and a .php file extension is added. No validation is performed on the content of the file, triggering an RCE vulnerability by uploading a web shell. Further the name parameter is not sanitized, allowing the payload to be uploaded to any directory to which the server has write access.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26982	SimpleMachinesForum 2.1.1 and earlier allows remote authenticated administrators to execute arbitrary code by inserting a vulnerable php code because the themes can be modified by an administrator. NOTE: the vendor's position is that administrators are intended to have the ability to modify themes, and can thus choose any PHP code that they wish to have executed on the server.	7.2	More Details
CVE-2021-33208	The "Register an Ehcache Configuration File" admin feature in MashZone NextGen through 10.7 GA allows XXE attacks via a malicious XML configuration file.	7.2	More Details
CVE-2021-33581	MashZone NextGen through 10.7 GA has an SSRF vulnerability that allows an attacker to interact with arbitrary TCP services, by abusing the feature to check the availability of a PPM connection. This occurs in com.idsscheer.ppmmashup.web.webservice.impl.ZPrestoAdminWebService.	7.2	More Details
CVE-2022-26986	SQL Injection in ImpressCMS 1.4.3 and earlier allows remote attackers to inject into the code in unintended way, this allows an attacker to read and modify the sensitive information from the database used by the application. If misconfigured, an attacker can even upload a malicious web shell to compromise the entire system.	7.2	More Details
CVE-2021-32985	AVEVA System Platform versions 2017 through 2020 R2 P01 does not properly verify that the source of data or communication is valid.	7.2	More Details
CVE-2021-32981	AVEVA System Platform versions 2017 through 2020 R2 P01 uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.	7.2	More Details
CVE-2021-32977	AVEVA System Platform versions 2017 through 2020 R2 P01 does not verify, or incorrectly verifies, the cryptographic signature for data.	7.2	More Details
CVE-2021-33523	MashZone NextGen through 10.7 GA allows a remote authenticated user, with access to the admin console, to upload a new JDBC driver that can execute arbitrary commands on the underlying host. This occurs in com.idsscheer.ppmmashup.business.jdbc.DriverUploadController.	7.2	More Details
CVE-2020-28062	An Access Control vulnerability exists in HisiPHP 2.0.11 via special packets that are constructed in $files = Dir::getList($decompath. '/ Upload/Plugins /, which could let a remote malicious user execute arbitrary code.	7.2	More Details
CVE-2022-23155	Dell Wyse Management Suite versions 2.0 through 3.5.2 contain an unrestricted file upload vulnerability. A malicious user with admin privileges can exploit this vulnerability in order to execute arbitrary code on the system.	7.2	More Details
CVE-2022-27816	SWHKD 1.1.5 unsafely uses the /tmp/swhks.pid pathname. There can be data loss or a denial of service.	7.1	More Details
CVE-2021-3461	A flaw was found in keycloak where keycloak may fail to logout user session if the logout request comes from external SAML identity provider and Principal Type is set to Attribute [Name].	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3456	An improper authorization handling flaw was found in Foreman. The Salt plugin for the smart-proxy allows foreman clients to execute actions that should be limited to the Foreman Server. This flaw allows an authenticated local attacker to access and delete limited resources and also causes a denial of service on the Foreman server. The highest threat from this vulnerability is to integrity and system availability.	7.1	More Details
CVE-2022-22331	IBM SterlingPartner Engagement Manager 6.2.0 could allow a remote authenticated attacker to obtain sensitive information or modify user details caused by an insecure direct object vulnerability (IDOR). IBM X-Force ID: 219130.	7.1	More Details
CVE-2022-26357	race in VT-d domain ID cleanup Xen domain IDs are up to 15 bits wide. VT-d hardware may allow for only less than 15 bits to hold a domain ID associating a physical device with a particular domain. Therefore internally Xen domain IDs are mapped to the smaller value range. The cleaning up of the housekeeping structures has a race, allowing for VT-d domain IDs to be leaked and flushes to be bypassed.	7.0	More Details
CVE-2021-23850	A specially crafted TCP/IP packet may cause a camera recovery image telnet interface to crash. It may also cause a buffer overflow which could enable remote code execution. The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.	6.8	More Details
CVE-2021-23851	A specially crafted TCP/IP packet may cause the camera recovery image web interface to crash. It may also cause a buffer overflow which could enable remote code execution. The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.	6.8	More Details
CVE-2021-30066	On Schneider Electric ConneXium Tofino Firewall TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and Belden Tofino Xenon Security Appliance, an arbitrary firmware image can be loaded because firmware signature verification (for a USB stick) can be bypassed. NOTE: this issue exists because of an incomplete fix of CVE-2017-11400.	6.8	More Details
CVE-2021-30061	On Schneider Electric ConneXium Tofino Firewall TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and Belden Tofino Xenon Security Appliance, physically proximate attackers can execute code via a crafted file on a USB stick.	6.8	More Details
CVE-2022-27651	A flaw was found in buildah where containers were incorrectly started with non-empty default permissions. A bug was found in Moby (Docker Engine) where containers were incorrectly started with non-empty inheritable Linux process capabilities, enabling an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. This has the potential to impact confidentiality and integrity.	6.8	More Details
CVE-2022-28379	jc21.com Nginx Proxy Manager before 2.9.17 allows XSS during item deletion.	6.8	More Details
CVE-2021-39786	In NFC, 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.Product: AndroidVersions: Android-12LAndroid ID: A-192551247	6.7	More Details
CVE-2022-1207	Out-of-bounds read in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability allows attackers to read sensitive information from outside the allocated buffer boundary.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0461	Policy bypass in COOP in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to bypass iframe sandbox via a crafted HTML page.	6.5	More Details
CVE-2022-22356	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow an attacker to enumerate account credentials due to an observable discrepancy in valid and invalid login attempts. IBM X-Force ID: 220487.	6.5	More Details
CVE-2022-0792	Out of bounds read in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2022-0922	The software does not perform any authentication for critical system functionality.	6.5	More Details
CVE-2022-0404	The Material Design for Contact Form 7 WordPress plugin through 2.6.4 does not check authorization or that the option mentioned in the notice param belongs to the plugin when processing requests to the cf7md_dismiss_notice action, allowing any logged in user (with roles as low as Subscriber) to set arbitrary options to true, potentially leading to Denial of Service by breaking the site.	6.5	More Details
CVE-2022-1201	NULL Pointer Dereference in mrb_vm_exec with super in GitHub repository mruby/mruby prior to 3.2. This vulnerability is capable of making the mruby interpreter crash, thus affecting the availability of the system.	6.5	More Details
CVE-2022-23183	Missing authorization vulnerability in Advanced Custom Fields versions prior to 5.12.1 and Advanced Custom Fields Pro versions prior to 5.12.1 allows a remote authenticated attacker to view the information on the database without the access permission.	6.5	More Details
CVE-2022-0830	The FormBuilder WordPress plugin through 1.08 does not have CSRF checks in place when creating/updating and deleting forms, and does not sanitise as well as escape its form field values. As a result, attackers could make logged in admin update and delete arbitrary forms via a CSRF attack, and put Cross-Site Scripting payloads in them.	6.5	More Details
CVE-2022-0462	Inappropriate implementation in Scroll in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-43662	totolink EX300_v2, ver V4.0.3c.140_B20210429 and A720R ,ver V4.1.5cu.470_B20200911 have an issue which causes uncontrolled resource consumption.	6.5	More Details
CVE-2021-46006	In Totolink A3100R V5.9c.4577, "test.asp" contains an API-like function, which is not authenticated. Using this function, an attacker can configure multiple settings without authentication.	6.5	More Details
CVE-2022-0802	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2021-27497	Philips Vue PACS versions 12.2.x.x and prior does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45900	Vivoh Webinar Manager before 3.6.3.0 has improper API authentication. When a user logs in to the administration configuration web portlet, a VIVOH_AUTH cookie is assigned so that they can be uniquely identified. Certain APIs can be successfully executed without proper authentication. This can let an attacker impersonate as victim and make state changing requests on their behalf.	6.5	More Details
CVE-2022-1236	Weak Password Requirements in GitHub repository weseek/growi prior to v5.0.0.	6.5	More Details
CVE-2021-38362	In RSA Archer 6.x through 6.9 SP3 (6.9.3.0), an authenticated attacker can make a GET request to a REST API endpoint that is vulnerable to an Insecure Direct Object Reference (IDOR) issue and retrieve sensitive data.	6.5	More Details
CVE-2021-39908	In all versions of GitLab CE/EE starting from 0.8.0 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 certain Unicode characters can be abused to commit malicious code into projects without being noticed in merge request or source code viewer UI.	6.5	More Details
CVE-2022-22950	n Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.	6.5	More Details
CVE-2021-40645	An SQL Injection vulnerability exists in glorylion JFinalOA as of 9/7/2021 in the defkey parameter getHaveDoneTaskDataList method of the FlowTaskController.	6.5	More Details
CVE-2021-40644	An SQL Injection vulnerability exists in oasys oa_system as of 9/7/2021 in resources/mappers/notice-mapper.xml.	6.5	More Details
CVE-2022-0455	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 98.0.4758.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2022-26951	Archer 6.x through 6.10 (6.10.0.0) contains a reflected XSS vulnerability. A remote SAML-unauthenticated malicious Archer user could potentially exploit this vulnerability by tricking a victim application user into supplying malicious HTML or JavaScript code to the vulnerable web application; the malicious code is then reflected back to the victim and gets executed by the web browser in the context of the vulnerable web application.	6.5	More Details
CVE-2022-1185	A denial of service vulnerability when rendering RDoc files in GitLab CE/EE versions 10 to 14.7.7, 14.8.0 to 14.8.5, and 14.9.0 to 14.9.2 allows an attacker to crash the GitLab web application with a maliciously crafted RDoc file	6.5	More Details
CVE-2022-22311	IBM Security Verify Access could allow a user, using man in the middle techniques, to obtain sensitive information or possibly change some information due to improper validiation of JWT tokens.	6.5	More Details
CVE-2021-41594	In RSA Archer 6.9.SP1 P3, if some application functions are precluded by the Administrator, this can be bypassed by intercepting the API request at the /api/V2/internal/TaskPermissions/CheckTaskAccess endpoint. If the parameters of this request are replaced with empty fields, the attacker achieves access to the precluded functions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23869	In RuoYi v4.7.2 through the WebUI, user test1 does not have permission to reset the password of user test3, but the password of user test3 can be reset through the /system/user/resetPwd request.	6.5	More Details
CVE-2022-24797	Pomerium is an identity-aware access proxy. In distributed service mode, Pomerium's Authenticate service exposes pprof debug and prometheus metrics handlers to untrusted traffic. This can leak potentially sensitive environmental information or lead to limited denial of service conditions. This issue is patched in version v0.17.1 Workarounds: Block access to `/debug` and `/metrics` paths on the authenticate service. This can be done with any L7 proxy, including Pomerium's own proxy service.	6.5	More Details
CVE-2022-0807	Inappropriate implementation in Autofill in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2022-27248	A directory traversal vulnerability in IdeaRE RefTree before 2021.09.17 allows remote authenticated users to download arbitrary .dwg files from a remote server by specifying an absolute or relative path when invoking the affected DownloadDwg endpoint. An attack uses the path field to CaddemServiceJS/CaddemService.svc/rest/DownloadDwg.	6.5	More Details
CVE-2022-1224	Improper Authorization in GitHub repository phpipam/phpipam prior to 1.4.6.	6.5	More Details
CVE-2022-27966	Xshell v7.0.0099 and below contains a binary hijack vulnerability which allows attackers to execute arbitrary code via a crafted .exe file.	6.5	More Details
CVE-2021-20295	It was discovered that the update for the virt:rhel module in the RHSA-2020:4676 (https://access.redhat.com/errata/RHSA-2020:4676) erratum released as part of Red Hat Enterprise Linux 8.3 failed to include the fix for the qemu-kvm component issue CVE-2020-10756, which was previously corrected in virt:rhel/qemu-kvm via erratum RHSA-2020:4059 (https://access.redhat.com/errata/RHSA-2020:4059). CVE-2021-20295 was assigned to that Red Hat specific security regression. For more details about the original security issue CVE-2020-10756, refer to bug 1835986 or the CVE page: https://access.redhat.com/security/cve/CVE-2020-10756.	6.5	More Details
CVE-2022-1225	Incorrect Privilege Assignment in GitHub repository phpipam/phpipam prior to 1.4.6.	6.5	More Details
CVE-2021-41245	Combodo iTop is a web based IT Service Management tool. In versions prior to 2.7.6 and 3.0.0, CSRF tokens generated by `privUITransactionFile` aren't properly checked. Versions 2.7.6 and 3.0.0 contain a patch for this issue. As a workaround, use the session implementation by adding in the iTop config file.	6.5	More Details
CVE-2022-0806	Data leak in Canvas in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in screen sharing to potentially leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-27965	Xlpd v7.0.0094 and below contains a binary hijack vulnerability which allows attackers to execute arbitrary code via a crafted .exe file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1223	Incorrect Authorization in GitHub repository phpipam/phpipam prior to 1.4.6.	6.5	More Details
CVE-2022-27963	Xftp 7.0.0088p and below contains a binary hijack vulnerability which allows attackers to execute arbitrary code via a crafted .exe file.	6.5	More Details
CVE-2022-27964	Xmanager v7.0.0096 and below contains a binary hijack vulnerability which allows attackers to execute arbitrary code via a crafted .exe file.	6.5	More Details
CVE-2022-0804	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2022-22404	IBM App Connect Enterprise Certified Container Dashboard UI (IBM App Connect Enterprise Certified Container 1.5, 2.0, 2.1, 3.0, and 3.1) may be vulnerable to denial of service due to excessive rate limiting.	6.5	More Details
CVE-2022-0803	Inappropriate implementation in Permissions in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to tamper with the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2022-26947	Archer 6.x through 6.9 SP3 (6.9.3.0) contains a reflected XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability by tricking a victim application user into supplying malicious HTML or JavaScript code to the vulnerable web application; the malicious code is then reflected back to the victim and gets executed by the web browser in the context of the vulnerable web application.	6.3	More Details
CVE-2022-1211	A vulnerability classified as critical has been found in tildearrow Furnace dev73. This affects the FUR to VGM converter in console mode which causes stack-based overflows and crashes. It is possible to initiate the attack remotely but it requires user-interaction. A POC has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-22328	IBM SterlingPartner Engagement Manager 6.2.0 could allow a malicious user to elevate their privileges and perform unintended operations to another users data. IBM X-Force ID: 218871.	6.2	More Details
CVE-2022-24135	QingScan 1.3.0 is affected by Cross Site Scripting (XSS) vulnerability in all search functions.	6.1	More Details
CVE-2022-26644	Online Banking System Protect v1.0 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via parameters on user profile, system_info and accounts management.	6.1	More Details
CVE-2021-43707	Cross Site Scripting (XSS) vulnerability exists in Maccms v10 via link_Name parameter.	6.1	More Details
CVE-2022-23796	An issue was discovered in Joomla! 3.7.0 through 3.10.6. Lack of input validation could allow an XSS attack using com_fields.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23798	An issue was discovered in Joomla! 2.5.0 through 3.10.6 & 4.0.0 through 4.1.0. Inadequate validation of URLs could result into an invalid check whether an redirect URL is internal or not.	6.1	More Details
CVE-2022-23697	A remote cross-site scripting (xss) vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView.	6.1	More Details
CVE-2022-1243	CRHTLF can lead to invalid protocol extraction potentially leading to XSS in GitHub repository medialize/uri.js prior to 1.19.11.	6.1	More Details
CVE-2022-28378	Craft CMS before 3.7.29 allows XSS.	6.1	More Details
CVE-2022-21830	A blind self XSS vulnerability exists in RocketChat LiveChat <v1.9 that could allow an attacker to trick a victim pasting malicious code in their chat instance.	6.1	More Details
CVE-2022-1233	URL Confusion When Scheme Not Supplied in GitHub repository medialize/uri.js prior to 1.19.11.	6.1	More Details
CVE-2022-23800	An issue was discovered in Joomla! 4.0.0 through 4.1.0. Inadequate content filtering leads to XSS vulnerabilities in various components.	6.1	More Details
CVE-2022-24181	Cross-site scripting (XSS) via Host Header injection in PKP Open Journals System 2.4.8 >= 3.3 allows remote attackers to inject arbitary code via the X-Forwarded-Host Header.	6.1	More Details
CVE-2022-23801	An issue was discovered in Joomla! 4.0.0 through 4.1.0. Possible XSS atack vector through SVG embedding in com_media.	6.1	More Details
CVE-2021-43661	totolink EX300_v2 V4.0.3c.140_B20210429 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /home.asp.	6.1	More Details
CVE-2022-24131	DouPHP v1.6 Release 20220121 is affected by Cross Site Scripting (XSS) through /admin/login.php in the background, which will lead to JavaScript code execution.	6.1	More Details
CVE-2021-27493	Philips Vue PACS versions 12.2.x.x and prior does not ensure or incorrectly ensures structured messages or data are well formed and that certain security properties are met before being read from an upstream component or sent to a downstream component.	6.1	More Details
CVE-2022-1170	In the Noo JobMonster WordPress theme before 4.5.2.9 JobMonster there is a XSS vulnerability as the input for the search form is provided through unsanitized GET requests.	6.1	More Details
CVE-2022-0431	The Insights from Google PageSpeed WordPress plugin before 4.0.4 does not sanitise and escape various parameters before outputting them back in attributes in the plugin's settings dashboard, leading to Reflected Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28202	An XSS issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. The widthheight, widthheightpage, and nbytes properties of messages are not escaped when used in galleries or Special:RevisionDelete.	6.1	More Details
CVE-2022-26616	PKP Vendor Open Journal System v2.4.8 to v3.3.8 allows attackers to perform reflected cross-site scripting (XSS) attacks via crafted HTTP headers.	6.1	More Details
CVE-2022-27463	Open redirect vulnerability in objects/login.json.php in WWBN AVideo through 11.6, allows attackers to arbitrarily redirect users from a crafted url to the login page.	6.1	More Details
CVE-2022-27462	Cross Site Scripting (XSS) vulnerability in objects/function.php in function getDeviceID in WWBN AVideo through 11.6, via the yptDevice parameter to view/include/head.php.	6.1	More Details
CVE-2022-0864	The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.22.9 does not sanitise and escape the updraft_interval parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-20729	Cross-site scripting vulnerability in pfSense CE and pfSense Plus (pfSense CE software versions 2.5.2 and earlier, and pfSense Plus software versions 21.05 and earlier) allows a remote attacker to inject an arbitrary script via a malicious URL.	6.1	More Details
CVE-2022-0901	The Ad Inserter Free and Pro WordPress plugins before 2.7.12 do not sanitise and escape the REQUEST_URI before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting in browsers which do not encode characters	6.1	More Details
CVE-2022-1164	The Wyzi Theme was affected by reflected XSS vulnerabilities in the business search feature	6.1	More Details
CVE-2022-1167	There are unauthenticated reflected Cross-Site Scripting (XSS) vulnerabilities in CareerUp Careerup WordPress theme before 2.3.1, via the filter parameters.	6.1	More Details
CVE-2022-1168	There is a Cross-Site Scripting vulnerability in the JobSearch WP JobSearch WordPress plugin before 1.5.1.	6.1	More Details
CVE-2022-1169	There is a XSS vulnerability in Careerfy.	6.1	More Details
CVE-2022-27496	Cross-site scripting vulnerability in Zero-channel BBS Plus v0.7.4 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2022-23156	Wyse Device Agent version 14.6.1.4 and below contain an Improper Authentication vulnerability. A malicious user could potentially exploit this vulnerability by providing invalid input in order to obtain a connection to WMS server.	6.0	More Details
CVE-2022-23158	Wyse Device Agent version 14.6.1.4 and below contain a sensitive data exposure vulnerability. A local authenticated user with standard privilege could potentially exploit this vulnerability and provide incorrect port information and get connected to valid WMS server	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27609	Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows does not provide sufficient anti-tampering protection of services by users with Administrator privileges. This could result in a user disabling Forcepoint One Endpoint and the protection offered by it.	6.0	More Details
CVE-2022-27608	Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows is vulnerable to registry key tampering by users with Administrator privileges. This could result in a user disabling anti-tampering mechanisms which would then allow the user to disable Forcepoint One Endpoint and the protection offered by it.	6.0	More Details
CVE-2022-24795	yajl-ruby is a C binding to the YAJL JSON parsing and generation library. The 1.x branch and the 2.x branch of `yajl` contain an integer overflow which leads to subsequent heap memory corruption when dealing with large (~2GB) inputs. The reallocation logic at `yajl_buf.c#L64` may result in the `need` 32bit integer wrapping to 0 when `need` approaches a value of 0x80000000 (i.e. ~2GB of data), which results in a reallocation of buf->alloc into a small heap chunk. These integers are declared as `size_t` in the 2.x branch of `yajl`, which practically prevents the issue from triggering on 64bit platforms, however this does not preclude this issue triggering on 32bit builds on which `size_t` is a 32bit integer. Subsequent population of this under-allocated heap chunk is based on the original buffer size, leading to heap memory corruption. This vulnerability mostly impacts process availability. Maintainers believe exploitation for arbitrary code execution is unlikely. A patch is available and anticipated to be part of yajl-ruby version 1.4.2. As a workaround, avoid passing large inputs to YAJL.	5.9	More Details
CVE-2021-45892	An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4. There is storage of Passwords in a Recoverable Format.	5.9	More Details
CVE-2021-45894	An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4. There is Cleartext Transmission of Sensitive Information.	5.9	More Details
CVE-2022-25160	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions, Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions, Mitsubishi Electric MELSEC iQ-R series R00/01/02CPU all versions, Mitsubishi Electric MELSEC iQ-R series R04/08/16/32/120(EN)CPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120SFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PCPU all versions, Mitsubishi Electric MELSEC iQ-R series R08/16/32/120PSFCPU all versions, Mitsubishi Electric MELSEC iQ-R series R16/32/64MTCPU all versions, Mitsubishi Electric MELSEC iQ-R series RJ71C24(-R2/R4) all versions, Mitsubishi Electric MELSEC iQ-R series RJ71EN71 all versions, Mitsubishi Electric MELSEC iQ-R series RJ72GF15-T2 all versions, Mitsubishi Electric MELSEC Q series Q03/04/06/13/26UDVCPU all versions, Mitsubishi Electric MELSEC Q series Q04/06/13/26UDPVCPU all versions, Mitsubishi Electric MELSEC Q series QJ71C24N(-R2/R4) all versions and Mitsubishi Electric MELSEC Q series QJ71E71-100 all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user’s system.	5.9	More Details
CVE-2022-0741	Improper input validation in all versions of GitLab CE/EE using sendmail to send emails allowed an attacker to steal environment variables via specially crafted email addresses.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26948	The Archer RSS feed integration for Archer 6.x through 6.9 SP1 (6.9.1.0) is affected by an insecure credential storage vulnerability. A malicious attacker may obtain access to credential information to use it in further attacks.	5.8	More Details
CVE-2022-28648	In JetBrains YouTrack before 2022.1.43563 HTML code from the issue description was being rendered	5.7	More Details
CVE-2022-26356	Racy interactions between dirty vram tracking and paging log dirty hypercalls Activation of log dirty mode done by XEN_DMOP_track_dirty_vram (was named HVMOP_track_dirty_vram before Xen 4.9) is racy with ongoing log dirty hypercalls. A suitably timed call to XEN_DMOP_track_dirty_vram can enable log dirty while another CPU is still in the process of tearing down the structures related to a previously enabled log dirty mode (XEN_DOMCTL_SHADOW_OP_OFF). This is due to lack of mutually exclusive locking between both operations and can lead to entries being added in already freed slots, resulting in a memory leak.	5.6	More Details
CVE-2021-23287	The vulnerability exists due to insufficient validation of input of certain resources within the IPM software. This issue affects: Intelligent Power Manager (IPM 1) versions prior to 1.70.	5.6	More Details
CVE-2021-23288	The vulnerability exists due to insufficient validation of input from certain resources by the IPP software. The attacker would need access to the local Subnet and an administrator interaction to compromise the system. This issue affects: Intelligent Power Protector versions prior to 1.69.	5.6	More Details
CVE-2021-39756	In Framework, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-184354287	5.5	More Details
CVE-2021-39742	In Voicemail, there is a possible way to retrieve a trackable identifier due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-186405602	5.5	More Details
CVE-2021-39740	In Messaging, there is a possible way to bypass attachment restrictions due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-209965112	5.5	More Details
CVE-2021-39757	In PermissionController, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-176094662	5.5	More Details
CVE-2021-39748	In InputMethodEditor, there is a possible way to access some files accessible to Settings due to an unsafe PendingIntent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-203777141	5.5	More Details
CVE-2021-39744	In DevicePolicyManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-192369136	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39751	In Settings, there is a possible way to read Bluetooth device names without proper permissions due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-172838801	5.5	More Details
CVE-2021-39755	In DevicePolicyManager, there is a possible way to reveal the existence of an installed package without proper query permissions due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-204995407	5.5	More Details
CVE-2021-39754	In ContextImpl, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:Android ID: A-207133709	5.5	More Details
CVE-2021-39747	In Settings Provider, there is a possible way to list values of non-readable global settings due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-208268457	5.5	More Details
CVE-2021-39753	In DomainVerificationService, there is a possible way to access app domain verification information due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-200035185	5.5	More Details
CVE-2022-1244	heap-buffer-overflow in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of inducing denial of service.	5.5	More Details
CVE-2021-39745	In DevicePolicyManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-206127671	5.5	More Details
CVE-2022-24191	In HTMLDOC 1.9.14, an infinite loop in the gif_read_lzw function can lead to a pointer arbitrarily pointing to heap memory and resulting in a buffer overflow.	5.5	More Details
CVE-2022-1068	Modbus Tools Modbus Slave (versions 7.4.2 and prior) is vulnerable to a stack-based buffer overflow in the registration field. This may cause the program to crash when a long character string is used.	5.5	More Details
CVE-2022-28388	usb_8dev_start_xmit in drivers/net/can/usb/usb_8dev.c in the Linux kernel through 5.17.1 has a double free.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39774	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-205989472	5.5	More Details
CVE-2021-39765	In Gallery, there is a possible permission bypass due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-201535427	5.5	More Details
CVE-2021-39778	In Telecomm, there is a possible way to determine whether an app is installed, without query permissions, due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-196406138	5.5	More Details
CVE-2021-39766	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-198296421	5.5	More Details
CVE-2021-39791	In WallpaperManagerService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-194112606	5.5	More Details
CVE-2022-1222	Inf loop in GitHub repository gpac/gpac prior to 2.1.0-DEV.	5.5	More Details
CVE-2021-39769	In Device Policy, there is a possible way to determine whether an app is installed, without query permissions, due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-193663287	5.5	More Details
CVE-2021-39761	In Media, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-179783181	5.5	More Details
CVE-2021-39770	In Framework, there is a possible disclosure of the device owner package due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-193033501	5.5	More Details
CVE-2022-28389	mcba_usb_start_xmit in drivers/net/can/usb/mcba_usb.c in the Linux kernel through 5.17.1 has a double free.	5.5	More Details
CVE-2021-39773	In VpnManagerService, there is a possible disclosure of installed VPN packages due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-191276656	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39779	In getCallStateUsingPackage of Telecom Service, there is a missing permission check. This could lead to local information disclosure of the call state with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-190400974	5.5	More Details
CVE-2021-39775	In People, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-206465854	5.5	More Details
CVE-2021-27223	A denial-of-service issue existed in one of modules that was incorporated in Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security. A local user could cause Windows crash by running a specially crafted binary module. The fix was delivered automatically. Credits: (Straghkov Denis, Kurmangaleev Shamil, Fedotov Andrey, Kuts Daniil, Mishechkin Maxim, Akolzin Vitaliy) @ ISPRAS	5.5	More Details
CVE-2021-39777	In Telephony, there is a possible way to determine whether an app is installed, without query permissions, due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-194743207	5.5	More Details
CVE-2022-28356	In the Linux kernel before 5.17.1, a refcount leak bug was found in net/llc/af_llc.c.	5.5	More Details
CVE-2021-30331	Possible buffer overflow due to improper data validation of external commands sent via DIAG interface in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	5.5	More Details
CVE-2021-39760	In AudioService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-194110526	5.5	More Details
CVE-2021-39788	In TelecomManager, there is a possible way to check if a particular self managed phone account was registered on the device due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-191768014	5.5	More Details
CVE-2022-1018	When opening a malicious solution file provided by an attacker, the application suffers from an XML external entity vulnerability due to an unsafe call within a dynamic link library file. An attacker could exploit this to pass data from local files to a remote web server, leading to a loss of confidentiality.	5.5	More Details
CVE-2022-23700	A local unauthorized read access to files vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView.	5.5	More Details
CVE-2022-1178	Stored Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.4.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1181	Stored Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.2.	5.4	More Details
CVE-2022-1179	Non-Privilege User Can Created New Rule and Lead to Stored Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.4.	5.4	More Details
CVE-2021-33616	RSA Archer 6.x through 6.9 SP1 P4 (6.9.1.4) allows stored XSS.	5.4	More Details
CVE-2020-28847	Cross Site Scripting (XSS) vulnerability in xCss Valine v1.4.14 via the nick parameter to /classes/Comment.	5.4	More Details
CVE-2022-0602	Cross-site Scripting (XSS) - DOM in GitHub repository tastyigniter/tastyigniter prior to 3.3.0.	5.4	More Details
CVE-2021-43478	A vulnerability exists in Hoosk 1.8.0 in /install/index.php, due to a failure to check if config.php already exists in the root directory, which could let a malicious user reinstall the website.	5.4	More Details
CVE-2021-25048	The KingComposer WordPress plugin through 2.9.6 does not have authorisation, CSRF and sanitisation/escaping when creating profile, allowing any authenticated users to create arbitrary ones, with Cross-Site Scripting payloads in them	5.4	More Details
CVE-2022-26615	A cross-site scripting (XSS) vulnerability in College Website Content Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the User Profile Name text fields.	5.4	More Details
CVE-2022-0837	The Amelia WordPress plugin before 1.0.48 does not have proper authorisation when handling Amelia SMS service, allowing any customer to send paid test SMS notification as well as retrieve sensitive information about the admin, such as the email, account balance and payment history. A malicious actor can abuse this vulnerability to drain out the account balance by keep sending SMS notification.	5.4	More Details
CVE-2021-43505	Multiple Cross Site Scripting (XSS) vulnerabilities exist in Ssourcecodester Simple Client Management System v1 via (1) Add new Client and (2) Add new invoice.	5.4	More Details
CVE-2022-25373	Zoho ManageEngine SupportCenter Plus before 11020 allows Stored XSS in the request history.	5.4	More Details
CVE-2022-24811	Combodi iTop is a web based IT Service Management tool. Prior to versions 2.7.6 and 3.0.0, cross-site scripting is possible for scripts outside of script tags when displaying HTML attachments. This issue is fixed in versions 2.7.6 and 3.0.0. There are currently no known workarounds.	5.4	More Details
CVE-2021-36826	Authenticated (subscriber or higher user role if allowed to access projects) Stored Cross-Site Scripting (XSS) vulnerability in weDevs WP Project Manager plugin <= 2.4.13 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25113	The Dropdown Menu Widget WordPress plugin through 1.9.7 does not have authorisation and CSRF checks when saving its settings, allowing low privilege users such as subscriber to update them. Due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site Scripting issues	5.4	More Details
CVE-2022-26244	A stored cross-site scripting (XSS) vulnerability in Hospital Patient Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the "special" field.	5.4	More Details
CVE-2022-0350	Cross-site Scripting (XSS) - Stored in GitHub repository vanessa219/vditor prior to 3.8.13.	5.4	More Details
CVE-2022-26950	Archer 6.x through 6.9 P2 (6.9.0.2) is affected by an open redirect vulnerability. A remote unprivileged attacker may potentially redirect legitimate users to arbitrary web sites and conduct phishing attacks. The attacker could then steal the victims' credentials and silently authenticate them to the Archer application without the victims realizing an attack occurred.	5.4	More Details
CVE-2022-0825	The Amelia WordPress plugin before 1.0.49 does not have proper authorisation when managing appointments, allowing any customer to update other's booking status, as well as retrieve sensitive information about the bookings, such as the full name and phone number of the person who booked it.	5.4	More Details
CVE-2021-43462	A Cross Site Scripting (XSS) vulnerability exists in Rumble Mail Server 0.51.3135 via the username parameter.	5.4	More Details
CVE-2021-43461	Cross Site Scripting (XSS) vulnerability exists in Rumble Mail Server 0.51.3135 via the servername parameter.	5.4	More Details
CVE-2021-43459	A Cross Site Scripting (XSS) vulnerability exists in Rumble Mail Server 0.51.3135 via the (1) domain and (2) path parameters.	5.4	More Details
CVE-2022-0425	A DNS rebinding vulnerability in the Irker IRC Gateway integration in all versions of GitLab CE/EE since version 7.9 allows an attacker to trigger Server Side Request Forgery (SSRF) attacks.	5.4	More Details
CVE-2022-23136	There is a stored XSS vulnerability in ZTE home gateway product. An attacker could modify the gateway name by inserting special characters and trigger an XSS attack when the user views the current topology of the device through the management page.	5.4	More Details
CVE-2022-1148	Improper authorization in GitLab Pages included with GitLab CE/EE affecting all versions from 11.5 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to steal a user's access token on an attacker-controlled private GitLab Pages website and reuse that token on the victim's other private websites	5.3	More Details
CVE-2022-23794	An issue was discovered in Joomla! 3.0.0 through 3.10.6 & 4.0.0 through 4.1.0. Uploading a file name of an excess length causes the error. This error brings up the screen with the path of the source code of the web application.	5.3	More Details
CVE-2022-26949	Archer 6.x through 6.9 SP2 P1 (6.9.2.1) contains an improper access control vulnerability on attachments. A remote authenticated malicious user could potentially exploit this vulnerability to gain access to files that should only be allowed by extra privileges.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24813	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. Without the patch for this issue, anonymous comments can be made using Special:RequestWikiQueue when sent directly via POST. A patch for this issue is available in the `master` branch of CreateWiki's GitHub repository.	5.3	More Details
CVE-2022-1166	The JobMonster Theme was vulnerable to Directory Listing in the /wp-content/uploads/jobmonster/ folder, as it did not include a default PHP file, or .htaccess file. This could expose personal data such as people's resumes. Although Directory Listing can be prevented by securely configuring the web server, vendors can also take measures to make it less likely to happen.	5.3	More Details
CVE-2022-1121	A lack of appropriate timeouts in GitLab Pages included in GitLab CE/EE all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an attacker to cause unlimited resource consumption.	5.3	More Details
CVE-2022-25245	Zoho ManageEngine ServiceDesk Plus before 13001 allows anyone to know the organisation's default currency name.	5.3	More Details
CVE-2022-22355	IBM MQ Appliance 9.2 CD and 9.2 LTS are vulnerable to a denial of service in the Login component of the application which could allow an attacker to cause a drop in performance.	5.3	More Details
CVE-2020-14479	Sensitive information can be obtained through the handling of serialized data. The issue results from the lack of proper authentication required to query the server	5.3	More Details
CVE-2022-25356	Alt-N MDaemon Security Gateway through 8.5.0 allows SecurityGateway.dll?view=login XML Injection.	5.3	More Details
CVE-2022-1172	Null Pointer Dereference Caused Segmentation Fault in GitHub repository gpac/gpac prior to 2.1.0-DEV.	5.0	More Details
CVE-2021-32503	Unauthenticated users can access sensitive web URLs through GET request, which should be restricted to maintenance users only. A malicious attacker could use this sensitive information’s to launch further attacks on the system.	4.9	More Details
CVE-2022-28063	Simple Bakery Shop Management System v1.0 contains a file disclosure via /bsms/?page=products.	4.9	More Details
CVE-2021-42946	A Cross Site Scripting (XSS) vulnerability exists in htmly.2.8.1 via the Copyright field in the /admin/config page.	4.8	More Details
CVE-2021-42869	A Cross Site Scripting (XSS) vulnerability exists in Chikista Patient Management Software 2.0.2 via the last_name parameter in the (1) patient/insert, (2) patient_report, (3) /appointment_report, (4) visit_report, and (5) /bill_detail_report pages.	4.8	More Details
CVE-2021-42868	A Cross Site Scripting (XSS) vulnerability exists in Chikista Patient Management Software 2.0.2 in the first_name parameter in (1) patient/insert, (2) patient_report, (3) appointment_report, (4) visit_report, and (5) bill_detail_report pages. .	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1163	Cross-site Scripting (XSS) - Stored in GitHub repository mineweb/minewebcms prior to next.	4.8	More Details
CVE-2021-42867	A Cross Site Scripting (XSS) vulnerability exists in DanPros htmly 2.8.1 via the Description field in (1) admin/config, and (2) index.php pages.	4.8	More Details
CVE-2021-42866	A Cross Site Scripting vulnerabilty exists in Pixelimity 1.0 via the Site Description field in pixelimity/admin/setting.php	4.8	More Details
CVE-2021-44310	An issue was discovered in Firmware Analysis and Comparison Tool v3.2. With administrator privileges, the attacker could perform stored XSS attacks by inserting JavaScript and HTML code in user creation functionality.	4.8	More Details
CVE-2022-26565	A cross-site scripting (XSS) vulnerability in Totaljs all versions before commit 95f54a5commit, allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page Name text field when creating a new page.	4.8	More Details
CVE-2022-27441	A stored cross-site scripting (XSS) vulnerability in TPCMS v3.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Phone text box.	4.8	More Details
CVE-2022-1120	Missing filtering in an error message in GitLab CE/EE affecting all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 exposed sensitive information when an include directive fails in the CI/CD configuration.	4.8	More Details
CVE-2022-0958	The Mark Posts WordPress plugin before 2.0.1 does not escape new markers, 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-2022-0884	The Profile Builder WordPress plugin before 3.6.8 does not sanitise and escape Form Fields titles and description, which could allow high privilege user such as admin to perform Criss-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-27436	A cross-site scripting (XSS) vulnerability in /public/admin/index.php?add_user at Ecommerce-Website v1.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username text field.	4.8	More Details
CVE-2022-28649	In JetBrains YouTrack before 2022.1.43563 it was possible to include an iframe from a third-party domain in the issue description	4.6	More Details
CVE-2022-23157	Wyse Device Agent version 14.6.1.4 and below contain a sensitive data exposure vulnerability. A authenticated malicious user could potentially exploit this vulnerability in order to view sensitive information from the WMS Server.	4.4	More Details
CVE-2022-0406	Improper Authorization in GitHub repository janeczku/calibre-web prior to 0.6.16.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1174	A potential DoS vulnerability was discovered in Gitlab CE/EE versions 13.7 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to trigger high CPU usage via a special crafted input added in Issues, Merge requests, Milestones, Snippets, Wiki pages, etc.	4.3	More Details
CVE-2022-27907	Sonatype Nexus Repository Manager 3.x before 3.38.0 allows SSRF.	4.3	More Details
CVE-2022-24523	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2022-1105	An improper access control vulnerability in GitLab CE/EE affecting all versions from 13.11 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an unauthorized user to access pipeline analytics even when public pipelines are disabled	4.3	More Details
CVE-2022-1100	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 13.1 prior to 14.7.7, 14.8.0 prior to 14.8.5, and 14.9.0 prior to 14.9.2. The api to update an asset as a link from a release had a regex check which caused exponential number of backtracks for certain user supplied values resulting in high CPU usage.	4.3	More Details
CVE-2022-1099	Adding a very large number of tags to a runner in GitLab CE/EE affecting all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an attacker to impact the performance of GitLab	4.3	More Details
CVE-2022-1177	Accounting User Can Download Patient Reports in openemr in GitHub repository openemr/openemr prior to 6.1.0.	4.3	More Details
CVE-2022-0405	Improper Access Control in GitHub repository janeczku/calibre-web prior to 0.6.16.	4.3	More Details
CVE-2022-0373	Improper access control in GitLab CE/EE versions 12.4 to 14.5.4, 14.5 to 14.6.4, and 12.6 to 14.7.1 allows project non-members to retrieve the service desk email address	4.3	More Details
CVE-2022-0390	Improper access control in Gitlab CE/EE versions 12.7 to 14.5.4, 14.6 to 14.6.4, and 14.7 to 14.7.1 allowed for project non-members to retrieve issue details when it was linked to an item from the vulnerability dashboard.	4.3	More Details
CVE-2022-28352	WeeChat (aka Wee Enhanced Environment for Chat) 3.2 to 3.4 before 3.4.1 does not properly verify the TLS certificate of the server, after certain GnuTLS options are changed, which allows man-in-the-middle attackers to spoof a TLS chat server via an arbitrary certificate. NOTE: this only affects situations where weechat.network.gnutls_ca_system or weechat.network.gnutls_ca_user is changed without a WeeChat restart.	4.3	More Details
CVE-2022-1210	A vulnerability classified as problematic was found in LibTIFF 4.3.0. Affected by this vulnerability is the TIFF File Handler of tiff2ps. Opening a malicious file leads to a denial of service. The attack can be launched remotely but requires user interaction. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25613	Authenticated Persistent Cross-Site Scripting (XSS) vulnerability in FV Flowplayer Video Player (WordPress plugin) versions <= 7.5.18.727 via &fv_wp_flowplayer_field_splash parameter.	4.1	More Details
CVE-2021-36851	Authenticated (editor or higher user role) Cross-Site Scripting (XSS) vulnerability in Web-Settler Testimonial Slider – Free Testimonials Slider Plugin (WordPress plugin) via parameters mpsp_posts_bg_color, mpsp_posts_description_color, mpsp_slide_nav_button_color.	4.1	More Details
CVE-2022-25620	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Group Functionality of Profelis IT Consultancy SambaBox allows AUTHENTICATED user to cause execute arbitrary codes on the vulnerable server. This issue affects: Profelis IT Consultancy SambaBox 4.0 version 4.0 and prior versions on x86.	3.8	More Details
CVE-2022-25619	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in ping tool of Profelis IT Consultancy SambaBox allows AUTHENTICATED user to cause run arbitrary code. This issue affects: Profelis IT Consultancy SambaBox 4.0 version 4.0 and prior versions on x86.	3.8	More Details
CVE-2022-1188	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 where a blind SSRF attack through the repository mirroring feature was possible.	3.7	More Details
CVE-2021-20238	It was found in OpenShift Container Platform 4 that ignition config, served by the Machine Config Server, can be accessed externally from clusters without authentication. The MCS endpoint (port 22623) provides ignition configuration used for bootstrapping Nodes and can include some sensitive data, e.g. registry pull secrets. There are two scenarios where this data can be accessed. The first is on Baremetal, OpenStack, Ovirt, Vsphere and KubeVirt deployments which do not have a separate internal API endpoint and allow access from outside the cluster to port 22623 from the standard OpenShift API Virtual IP address. The second is on cloud deployments when using unsupported network plugins, which do not create iptables rules that prevent to port 22623. In this scenario, the ignition config is exposed to all pods within the cluster and cannot be accessed externally.	3.7	More Details
CVE-2021-33024	Philips Vue PACS versions 12.2.x.x and prior transmits or stores authentication credentials, but it uses an insecure method susceptible to unauthorized interception and/or retrieval.	3.7	More Details
CVE-2022-0489	An issue has been discovered in GitLab CE/EE affecting all versions starting with 8.15 . It was possible to trigger a DOS by using the math feature with a specific formula in issue comments.	3.5	More Details
CVE-2022-1180	Reflected Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.4.	3.5	More Details
CVE-2022-25618	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in wpDataTables (WordPress plugin) versions <= 2.1.27	3.4	More Details
CVE-2020-35501	A flaw was found in the Linux kernels implementation of audit rules, where a syscall can unexpectedly not be correctly not be logged by the audit subsystem	3.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39739	In ArrayMap, there is a possible leak of the content of SMS messages due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-184525194	3.3	More Details
CVE-2022-0740	Incorrect authorization in the Asana integration's branch restriction feature in all versions of GitLab CE/EE starting from version 7.8.0 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 makes it possible to close Asana tasks from unrestricted branches.	3.1	More Details
CVE-2022-1189	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.2 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 that allowed for an unauthorised user to read the the approval rules of a private project.	3.1	More Details
CVE-2022-1111	A business logic error in Project Import in GitLab CE/EE versions 14.9 prior to 14.9.2, 14.8 prior to 14.8.5, and 14.0 prior to 14.7.7 under certain conditions caused imported projects to show an incorrect user in the 'Access Granted' column in the project membership pages	2.4	More Details
CVE-2022-27049	Raidrive before v2021.12.35 allows attackers to arbitrarily move log files by pre-creating a mountpoint and log files before Raidrive is installed.	2.0	More Details
CVE-2021-46443	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-46439	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation sho	N/A	More Details
CVE-2022-27306	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details