SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 August 2021

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-2021-32016	An issue was discovered in JUMP AMS 3.6.0.04.009-2487. A JUMP SOAP endpoint permitted the writing of arbitrary files to a user-controlled location on the remote filesystem (with user-controlled content) via directory traversal, potentially leading to remote code and command execution.	9.9	More Details
CVE-2021-32017	An issue was discovered in JUMP AMS 3.6.0.04.009-2487. A JUMP SOAP endpoint permitted the listing of the content of the remote file system. This can be used to identify the complete server filesystem structure, i.e., identifying all the directories and files.	9.9	More Details
CVE-2020-5341	Deserialization of Untrusted Data Vulnerability Dell EMC Avamar Server versions 7.4.1, 7.5.0, 7.5.1, 18.2, 19.1 and 19.2 and Dell EMC Integrated Data Protection Appliance versions 2.0, 2.1, 2.2, 2.3, 2.4 and 2.4.1 contain a Deserialization of Untrusted Data Vulnerability. A remote unauthenticated attacker could exploit this vulnerability to send a serialized payload that would execute code on the system.	9.8	More Details
CVE-2021-22444	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause code injection.	9.8	More Details
CVE-2021-37578	Apache jUDDI uses several classes related to Java's Remote Method Invocation (RMI) which (as an extension to UDDI) provides an alternate transport for accessing UDDI services. RMI uses the default Java serialization mechanism to pass parameters in RMI invocations. A remote attacker can send a malicious serialized object to the above RMI entries. The objects get deserialized without any check on the incoming data. In the worst case, it may let the attacker run arbitrary code remotely. For both jUDDI web service applications and jUDDI clients, the usage of RMI is disabled by default. Since this is an optional feature and an extension to the UDDI protocol, the likelihood of impact is low. Starting with 3.3.10, all RMI related code was removed.	9.8	More Details
CVE-2021-37163	An insecure permissions issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus operated by released versions of software before Nexus Software 7.2.5.7. The device has two user accounts with passwords that are hardcoded.	9.8	More Details
CVE-2021-37164	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. In the tcpTxThread function, the received data is copied to a stack buffer. An off-by-3 condition can occur, resulting in a stack-based buffer overflow.	9.8	More Details
CVE-2021-37167	An insecure permissions issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. A user logged in using the default credentials can gain root access to the device, which provides permissions for all of the functionality of the device.	9.8	More Details
CVE-2021-22387	There is an Improper Control of Dynamically Managing Code Resources Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to remotely execute commands.	9.8	More Details
CVE-2021-22388	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed.	9.8	More Details
CVE-2021-22389	There is a Permission Control Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed.	9.8	More Details
CVE-2021-22390	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed.	9.8	More Details
CVE-2021-22438	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause malicious code to be executed.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37843	The resolution SAML SSO apps for Atlassian products allow a remote attacker to login to a user account when only the username is known (i.e., no other authentication is provided). The fixed versions are for Jira: 3.6.6.1, 4.0.12, 5.0.5; for Confluence 3.6.6, 4.0.12, 5.0.5; for Bitbucket 2.5.9, 3.6.6, 4.0.12, 5.0.5; for Bamboo 2.5.9, 3.6.6, 4.0.12, 5.0.5; and for Fisheye 2.5.9.	9.8	More Details
CVE-2021-32810	crossbeam-deque is a package of work-stealing deques for building task schedulers when programming in Rust. In versions prior to 0.7.4 and 0.8.0, the result of the race condition is that one or more tasks in the worker queue can be popped twice instead of other tasks that are forgotten and never popped. If tasks are allocated on the heap, this can cause double free and a memory leak. If not, this still can cause a logical bug. Crates using `Stealer::steal`, `Stealer::steal_batch`, or `Stealer::steal_batch_and_pop` are affected by this issue. This has been fixed in crossbeam-deque 0.8.1 and 0.7.4.	9.8	More Details
CVE-2021-37160	A firmware validation issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. There is no firmware validation (e.g., cryptographic signature validation) during a File Upload for a firmware update.	9.8	More Details
CVE-2021-37832	A SQL injection vulnerability exists in version 3.0.2 of Hotel Druid when SQLite is being used as the application database. A malicious attacker can issue SQL commands to the SQLite database through the vulnerable idappartamenti parameter.	9.8	More Details
CVE-2021-27952	Hardcoded default root credentials exist on the ecobee3 lite 4.5.81.200 device. This allows a threat actor to gain access to the password-protected bootloader environment through the serial console.	9.8	More Details
CVE-2021-33485	CODESYS Control Runtime system before 3.5.17.10 has a Heap-based Buffer Overflow.	9.8	More Details
CVE-2021-37558	A SQL injection vulnerability in a MediaWiki script in Centreon before 20.04.14, 20.10.8, and 21.04.2 allows remote unauthenticated attackers to execute arbitrary SQL commands via the host_name and service_description parameters. The vulnerability can be exploited only when a valid Knowledge Base URL is configured on the Knowledge Base configuration page and points to a MediaWiki instance. This relates to the proxy feature in class/centreon-knowledge/ProceduresProxy.class.php and include/configuration/configKnowledge/proxy/proxy.php.	9.8	More Details
CVE-2021-36622	Sourcecodester Online Covid Vaccination Scheduler System 1.0 is affected vulnerable to Arbitrary File Upload. The admin panel has an upload function of profile photo accessible at http://localhost/scheduler/admin/?page=user. An attacker could upload a malicious file such as shell.php with the Content-Type: image/png. Then, the attacker have to visit the uploaded profile photo to access the shell.	9.8	More Details
CVE-2021-36623	Arbitrary File Upload in Sourcecodester Phone Shop Sales Management System 1.0 enables RCE.	9.8	More Details
CVE-2020-19301	A vulnerability in the vae_admin_rule database table of vaeThink v1.0.1 allows attackers to execute arbitrary code via a crafted payload in the condition parameter.	9.8	More Details
CVE-2020-19302	An arbitrary file upload vulnerability in the avatar upload function of vaeThink v1.0.1 allows attackers to open a webshell via changing uploaded file suffixes to ".php".	9.8	More Details
CVE-2021-37161	A buffer overflow issue was discovered in the HMI3 Control Panel contained within the Swisslog Healthcare Nexus Panel, operated by released versions of software before Nexus Software 7.2.5.7. A buffer overflow allows an attacker to overwrite an internal queue data structure and can lead to remote code execution.	9.8	More Details
CVE-2021-37162	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. If an attacker sends a malformed UDP message, a buffer underflow occurs, leading to an out-of-bounds copy and possible remote code execution.	9.8	More Details
CVE-2021-37165	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When a message is sent to the HMI TCP socket, it is forwarded to the hmiProcessMsg function through the pendingQ, and may lead to remote code execution.	9.8	More Details
CVE-2021-34166	A SQL INJECTION vulnerability in Sourcecodester Simple Food Website 1.0 allows a remote attacker to Bypass Authentication and become Admin.	9.8	More Details
CVE-2020-36239	Jira Data Center, Jira Core Data Center, Jira Software Data Center from version 6.3.0 before 8.5.16, from 8.6.0 before 8.13.8, from 8.14.0 before 8.17.0 and Jira Service Management Data Center from version 2.0.2 before 4.5.16, from version 4.6.0 before 4.13.8, and from version 4.14.0 before 4.17.0 exposed a Ehcache RMI network service which attackers, who can connect to the service, on port 40001 and potentially 40011[0][1], could execute arbitrary code of their choice in Jira through deserialization due to a missing authentication vulnerability. While Atlassian strongly suggests restricting access to the Ehcache ports to only Data Center instances, fixed versions of Jira will now require a shared secret in order to allow access to the Ehcache service. [0] In Jira Data Center, Jira Core Data Center, and Jira Software Data Center versions prior to 7.13.1, the Ehcache object port can be randomly allocated. [1] In Jira Service Management Data Center versions prior to 3.16.1, the Ehcache object port can be randomly allocated.	9.8	More Details
CVE-2021-29781	IBM Partner Engagement Manager 2.0 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization flaw. By sending specially-crafted data, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 203091.	9.8	More Details
CVE-2020-18013	SQL Injextion vulnerability exists in Whatsns 4.0 via the ip parameter in index.php?admin_banned/add.htm.	9.8	More Details
CVE-2020-18175	SQL Injection vulnerability in Metinfo 6.1.3 via a dosafety_emailadd action in basic.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21806	SQL Injection Vulnerability in ECTouch v2 via the shop page in index.php..	9.8	More Details
CVE-2020-21808	SQL Injection vulnerability in NukeViet CMS 4.0.10 - 4.3.07 via:the topicsid parameter in modules/news/admin/addtotopics.php.	9.8	More Details
CVE-2020-21809	SQL Injection vulnerability in NukeViet CMS module Shops 4.0.29 and 4.3 via the (1) listid parameter in detail.php and the (2) group_price or groupid parameters in search_result.php.	9.8	More Details
CVE-2021-25200	Arbitrary file upload vulnerability in SourceCodester Learning Management System v 1.0 allows attackers to execute arbitrary code, via the file upload to \lms\student_avatar.php.	9.8	More Details
CVE-2021-33527	In MB connect line mbDIALUP versions <= 3.9R0.0 a remote attacker can send a specifically crafted HTTP request to the service running with NT AUTHORITY\SYSTEM that will not correctly validate the input. This can lead to an arbitrary code execution with the privileges of the service.	9.8	More Details
CVE-2021-34165	A SQL Injection vulnerability in Sourcecodester Basic Shopping Cart 1.0 allows a remote attacker to Bypass Authentication and become Admin.	9.8	More Details
CVE-2021-30124	The unofficial vscode-phpmd (aka PHP Mess Detector) extension before 1.3.0 for Visual Studio Code allows remote attackers to execute arbitrary code via a crafted phpmd.command value in a workspace folder.	9.8	More Details
CVE-2021-35458	Online Pet Shop We App 1.0 is vulnerable to Union SQL Injection in products.php (aka p=products) via the c or s parameter.	9.8	More Details
CVE-2021-36624	Sourcecodester Phone Shop Sales Managements System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.	9.8	More Details
CVE-2021-37594	In FreeRDP before 2.4.0 on Windows, wf_cliprdr_server_file_contents_request in client/Windows/wf_cliprdr.c has missing input checks for a FILECONTENTS_SIZE File Contents Request PDU.	9.8	More Details
CVE-2021-37595	In FreeRDP before 2.4.0 on Windows, wf_cliprdr_server_file_contents_request in client/Windows/wf_cliprdr.c has missing input checks for a FILECONTENTS_RANGE File Contents Request PDU.	9.8	More Details
CVE-2021-37759	A Session ID leak in the DEBUG log file in Graylog before 4.1.2 allows attackers to escalate privileges (to the access level of the leaked session ID).	9.8	More Details
CVE-2021-37760	A Session ID leak in the audit log in Graylog before 4.1.2 allows attackers to escalate privileges (to the access level of the leaked session ID).	9.8	More Details
CVE-2021-24472	The OnAir2 WordPress theme before 3.9.9.2 and QT KenthaRadio WordPress plugin before 2.0.2 have exposed proxy functionality to unauthenticated users, sending requests to this proxy functionality will have the web server fetch and display the content from any URI, this would allow for SSRF (Server Side Request Forgery) and RFI (Remote File Inclusion) vulnerabilities on the website.	9.8	More Details
CVE-2020-19305	An issue in /app/system/column/admin/index.class.php of Metinfo v7.0.0 causes the indeximg parameter to be deleted when the column is deleted, allowing attackers to escalate privileges.	9.8	More Details
CVE-2021-30571	Insufficient policy enforcement in DevTools in Google Chrome prior to 92.0.4515.107 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-2021-21538	Dell EMC iDRAC9 versions 4.40.00.00 and later, but prior to 4.40.10.00, contain an improper authentication vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain access to the virtual console.	9.6	More Details
CVE-2021-36159	libfetch before 2021-07-26, as used in apk-tools, xbps, and other products, mishandles numeric strings for the FTP and HTTP protocols. The FTP passive mode implementation allows an out-of-bounds read because strtol is used to parse the relevant numbers into address bytes. It does not check if the line ends prematurely. If it does, the for-loop condition checks for the '\0' terminator one byte too late.	9.1	More Details
CVE-2021-22435	There is a Configuration Defect Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service integrity and availability.	9.1	More Details
CVE-2021-37144	CSZ CMS 1.2.9 is vulnerable to Arbitrary File Deletion. This occurs in PHP when the unlink() function is called and user input might affect portions of or the whole affected parameter, which represents the path of the file to remove, without sufficient sanitization.	9.1	More Details
CVE-2021-37593	PEEL Shopping version 9.4.0 allows remote SQL injection. A public user/guest (unauthenticated) can inject a malicious SQL query in order to affect the execution of predefined SQL commands. Upon a successful SQL injection attack, an attacker can read sensitive data from the database and possibly modify database data.	9.1	More Details
CVE-2021-36701	In htmly version 2.8.1, is vulnerable to an Arbitrary File Deletion on the local host when delete backup files. The vulnerability may allow a remote attacker to delete arbitrary know files on the host.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description

CVE Number	Description
CVE-2021-24458	The get_ays_popupboxes() and get_popup_categories() functions of the Popup box WordPress plugin before 2.3.4 did not use whitelist or validate the orderby parame
CVE-2021-37840	aaPanel through 6.8.12 allows Cross-Site WebSocket Hijacking (CSWH) involving OS commands within WebSocket messages at a ws:// URL for /webssh (the victim n exploitation can occur with Firefox but not Chrome).
CVE-2021-30578	Uninitialized use in Media in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2021-30563	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-32772	Poddycast is a podcast app made with Electron. Prior to version 0.8.1, an attacker can create a podcast or episode with malicious characters and execute commands c allows the injection of HTML and JS code (cross-site scripting). Being an application made in electron, cross-site scripting can be scaled to remote code execution, mal 0.8.1.
CVE-2021-20783	Cross-site request forgery (CSRF) vulnerability in Optical BB unit E-WMTA2.3 allows a remote attacker to hijack the authentication of administrators via a specially craf
CVE-2021-30576	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit hea
CVE-2021-30575	Out of bounds write in Autofill in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to potentially exploit hea
CVE-2021-30574	Use after free in protocol handling in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30573	Use after free in GPU in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30572	Use after free in Autofill in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-29757	IBM QRadar User Behavior Analytics 4.1.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions trans
CVE-2021-30569	Use after free in sqlite in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30568	Heap buffer overflow in WebGL in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-31630	Command Injection in Open PLC Webserver v3 allows remote attackers to execute arbitrary code via the "Hardware Layer Code Box" component on the "/hardware" pa
CVE-2021-30567	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to open DevTools to potentially exploit heap corruption v
CVE-2021-24459	The get_results() and get_items() functions in the Survey Maker WordPress plugin before 1.5.6 did not use whitelist or validate the orderby parameter before using it in
CVE-2020-26806	admin/file.do in ObjectPlanet Opinio before 7.15 allows Unrestricted File Upload of executable JSP files, resulting in remote code execution, because filePath can have
CVE-2021-34802	A failure in resetting the security context in some transaction actions in Neo4j Graph Database 4.2 and 4.3 could allow authenticated users to execute commands with e

CVE Number	Description
CVE-2021-35472	An issue was discovered in LemonLDAP::NG before 2.0.12. Session cache corruption can lead to authorization bypass or spoofing. By running a loop that makes many
CVE-2021-30566	Stack buffer overflow in Printing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to potentially exploit s
CVE-2021-30565	Out of bounds write in Tab Groups in Google Chrome on Linux and ChromeOS prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious e
CVE-2021-36004	Adobe InDesign version 16.0 (and earlier) is affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage this vu a victim must open a malicious file.
CVE-2021-30541	Use after free in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-34637	The Post Index WordPress plugin is vulnerable to Cross-Site Request Forgery via the OptionsPage function found in the ~/php/settings.php file which allows attackers t
CVE-2021-30559	Out of bounds write in ANGLE in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30560	Use after free in Blink XSLT in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30561	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30562	Use after free in WebSerial in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-34628	The Admin Custom Login WordPress plugin is vulnerable to Cross-Site Request Forgery due to the loginbgSave action found in the ~/includes/Login-form-setting/Logir
CVE-2021-34632	The SEO Backlinks WordPress plugin is vulnerable to Cross-Site Request Forgery via the loc_config function found in the ~/seo-backlinks.php file which allows attacke
CVE-2021-24492	The hndtst_action_instance_callback AJAX call of the Handsome Testimonials & Reviews WordPress plugin before 2.1.1, available to any authenticated users, does no SQL Injection issue.
CVE-2021-30579	Use after free in UI framework in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30564	Heap buffer overflow in WebXR in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-22761	Cross Site Request Forgery (CSRF) vulnerability in FlatPress 1.1 via the DeleteFile function in flat/admin.php.
CVE-2021-29736	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote user to gain elevated privileges on the system. IBM X-Force ID: 201300.
CVE-2021-24457	The get_portfolios() and get_portfolio_attributes() functions in the class-portfolio-responsive-gallery-list-table.php and class-portfolio-responsive-gallery-attributes-list-tal before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard
CVE-2021-24460	The get_fb_likeboxes() function in the Popup Like box – Page Plugin WordPress plugin before 3.5.3 did not use whitelist or validate the orderby parameter before using

CVE Number	Description
CVE-2021-24461	The get_faqs() function in the FAQ Builder AYS WordPress plugin before 1.3.6 did not use whitelist or validate the orderby parameter before using it in SQL statements
CVE-2021-24462	The get_gallery_categories() and get_galleries() functions in the Photo Gallery by Ays – Responsive Image Gallery WordPress plugin before 4.4.4 did not use whitelist in the admin dashboard
CVE-2021-37556	A SQL injection vulnerability in reporting export in Centreon before 20.04.14, 20.10.8, and 21.04.2 allows remote authenticated (but low-privileged) attackers to execute
CVE-2021-37557	A SQL injection vulnerability in image generation in Centreon before 20.04.14, 20.10.8, and 21.04.2 allows remote authenticated (but low-privileged) attackers to execu
CVE-2021-32814	Skytable is a NoSQL database with automated snapshots and TLS. Versions prior to 0.5.1 are vulnerable to a a directory traversal attack enabling remotely connected no known workarounds aside from upgrading.
CVE-2020-5353	The Dell Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale OneFS version 9.0.0 default configuration for Network File System (NFS) allows access to administrative access to the system.
CVE-2021-24463	The get_sliders() function in the Image Slider by Ays- Responsive Slider and Carousel WordPress plugin before 2.5.0 did not use whitelist or validate the orderby paran
CVE-2019-14453	An issue was discovered in Comelit "App lejos de casa (web)" 2.8.0. It allows privilege escalation via modified domus and logged fields, related to js/bridge.min.js and l 1C000000000S value for domus, in conjunction with a zero value for logged.
CVE-2021-30581	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit hea
CVE-2021-36741	An improper input validation vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG, and Worry-Free Business Security 10.0 SP1 allows a remo product's management console in order to exploit this vulnerability.
CVE-2021-30585	Use after free in sensor handling in Google Chrome on Windows prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HT
CVE-2020-18157	Cross Site Request Forgery (CSRF) vulnerability in MetInfo 6.1.3 via a doaddsave action in admin/index.php.
CVE-2021-30586	Use after free in dialog box handling in Windows in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to
CVE-2021-30588	Type confusion in V8 in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-18113	The DefaultOSWorkflowConfigurator class in Jira Server and Jira Data Center before version 8.18.1 allows remote attackers who can trick a system administrator to im various problematic OSWorkflow classes to be used as part of workflows. The fix for this issue blocks usage of unsafe conditions, validators, functions and registers tha are not affected by this fix.
CVE-2021-32018	An issue was discovered in JUMP AMS 3.6.0.04.009-2487. The JUMP SOAP API was vulnerable to arbitrary file reading due to an improper limitation of file loading on
CVE-2021-32804	The npm package "tar" (aka node-tar) before versions 6.1.1, 5.0.6, 4.4.14, and 3.3.2 has a arbitrary File Creation/Overwrite vulnerability due to insufficient absolute pat `preservePaths` flag is not set to `true`. This is achieved by stripping the absolute path root from any absolute file paths contained in a tar file. For example `/home/user `////home/user/.bashrc`. `node-tar` would only strip a single path root from such paths. When given an absolute file path with repeating path roots, the resulting path (e.g addressed in releases 3.2.2, 4.4.14, 5.0.6 and 6.1.1. Users may work around this vulnerability without upgrading by creating a custom `onentry` method which sanitizes CVE-2021-32803 which fixes a similar bug in later versions of tar.
CVE-2021-27954	A heap-based buffer overflow vulnerability exists on the ecobee3 lite 4.5.81.200 device in the HKProcessConfig function of the HomeKit Wireless Access Control setup

CVE Number	Description
CVE-2021-32803	The npm package "tar" (aka node-tar) before versions 6.1.2, 5.0.7, 4.4.15, and 3.2.3 has an arbitrary File Creation/Overwrite vulnerability via insufficient symlink protect achieved by ensuring that extracted directories are not symlinks. Additionally, in order to prevent unnecessary `stat` calls to determine whether a given path is a directo a symlink with the same name as the directory. This order of operations resulted in the directory being created and added to the `node-tar` directory cache. When a dire checks for symlinks occur. By first creating a directory, and then replacing that directory with a symlink, it was thus possible to bypass `node-tar` symlink checks on dire location, thus allowing arbitrary file creation and overwrite. This issue was addressed in releases 3.2.3, 4.4.15, 5.0.7 and 6.1.2.
CVE-2021-38084	An issue was discovered in the POP3 component of Courier Mail Server before 1.1.5. Meddler-in-the-middle attackers can pipeline commands after the POP3 STLS cc
CVE-2021-22384	There is an Information Disclosure Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass.
CVE-2020-11511	The LearnPress plugin before 3.2.6.9 for WordPress allows remote attackers to escalate the privileges of any user to LP Instructor via the accept-to-be-teacher action p
CVE-2021-36621	Sourcecodester Online Covid Vaccination Scheduler System 1.0 is vulnerable to SQL Injection. The username parameter is vulnerable to time-based SQL injection. Up authenticate as Administrator.
CVE-2021-22427	There is a Heap-based Buffer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass.
CVE-2021-22428	There is an Incomplete Cleanup Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass.
CVE-2021-22423	A component of the HarmonyOS has a Out-of-bounds Write Vulnerability. Local attackers may exploit this vulnerability to cause integer overflow.
CVE-2021-31504	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.3.84 (package 16.6.3.134). User int exists within the parsing of PDF files. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can
CVE-2021-22420	A component of the HarmonyOS has a External Control of System or Configuration Setting vulnerability. Local attackers may exploit this vulnerability to cause the unde
CVE-2021-22422	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause memory overwriting.
CVE-2021-22425	A component of the HarmonyOS has a Double Free vulnerability. Local attackers may exploit this vulnerability to cause Root Elevating Privileges.
CVE-2021-22416	A component of the HarmonyOS has a Data Processing Errors vulnerability. Local attackers may exploit this vulnerability to cause Kernel Code Execution.
CVE-2021-22421	A component of the HarmonyOS has a Improper Privilege Management vulnerability. Local attackers may exploit this vulnerability to cause further Elevation of Privilege
CVE-2021-22418	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause memory overwriting.
CVE-2021-31503	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.3.84 (package 16.6.3.134). User int exists within the parsing of IGS files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to
CVE-2021-21864	A unsafe deserialization vulnerability exists in the ComponentModel ComponentManager.StartupCultureSettings functionality of CODESYS GmbH CODESYS Develop to trigger this vulnerability.
CVE-2021-29741	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user to exploit a vulnerability in Korn Shell (ksh) to gain root privileges. IBM X-Force ID: 201478.
CVE-2021-30577	Insufficient policy enforcement in Installer in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to perform local privilege escalation via a crafted file.

CVE Number	Description
CVE-2021-36742	A improper input validation vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG and Worry-Free Business Security 10.0 SP1 allows a local a on the target system in order to exploit this vulnerability.
CVE-2021-36983	replay-sorcery-kms in Replay Sorcery 0.6.0 allows a local attacker to gain root privileges via a symlink attack on /tmp/replay-sorcery or /tmp/replay-sorcery/device.sock
CVE-2020-19303	An arbitrary file upload vulnerability in /fileupload.php of hdcms 5.7 allows attackers to execute arbitrary code via a crafted file.
CVE-2021-21546	Dell EMC NetWorker versions 18.x,19.x prior to 19.3.0.4 and 19.4.0.0 contain an Information Disclosure in Log Files vulnerability. A local low-privileged user of the Net
CVE-2021-22396	There is a privilege escalation vulnerability in some Huawei products. Due to improper privilege management, a local attacker with common privilege may access some V100R005C00,V100R005C10;eSE620X vESS V100R001C10SPC200,V100R001C20SPC200.
CVE-2021-21865	A unsafe deserialization vulnerability exists in the PackageManagement.plugin ExtensionMethods.Clone() functionality of CODESYS GmbH CODESYS Development S vulnerability.
CVE-2021-33526	In MB connect line mbDIALUP versions <= 3.9R0.0 a low privileged local attacker can send a command to the service running with NT AUTHORITY\SYSTEM instructi
CVE-2021-21866	A unsafe deserialization vulnerability exists in the ObjectManager.plugin ProfileInformation.ProfileData functionality of CODESYS GmbH CODESYS Development Syst this vulnerability.
CVE-2021-22443	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause random address access.
CVE-2021-22442	There is an Improper Validation of Integrity Check Value Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset
CVE-2021-22415	There is an Incorrect Calculation of Buffer Size Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause kernel exceptions with the co
CVE-2021-33196	In archive/zip in Go before 1.15.13 and 1.16.x before 1.16.5, a crafted file count (in an archive's header) can cause a NewReader or OpenReader panic.
CVE-2021-22414	There is a Memory Buffer Errors Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset.
CVE-2021-22413	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset.
CVE-2021-22445	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset.
CVE-2021-22446	There is an Information Disclosure Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset.
CVE-2021-22412	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause random kernel address access.
CVE-2021-27943	The pairing procedure used by the Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs and mobile application is vulnerable to a brute-force attack (against on
CVE-2021-22381	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause an infinite loop in DoS.

CVE Number	Description
CVE-2021-22392	There is an Incorrect Calculation of Buffer Size in Huawei Smartphone.Successful exploitation of this vulnerability may cause verification bypass and directions to abno
CVE-2020-5351	Dell EMC Data Protection Advisor versions 6.4, 6.5 and 18.1 contain an undocumented account with limited privileges that is protected with a hard-coded password. A privileges.
CVE-2021-22379	There is an Integer Underflow (Wrap or Wraparound) Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS of Samgr.
CVE-2021-33198	In Go before 1.15.13 and 1.16.x before 1.16.5, there can be a panic for a large exponent to the math/big.Rat SetString or UnmarshalText method.
CVE-2021-3673	A vulnerability was found in Radare2 in version 5.3.1. Improper input validation when reading a crafted LE binary can lead to resource exhaustion and DoS.
CVE-2021-37847	crypto/digest.c in Pengutronix barebox through 2021.07.0 leaks timing information because memcmp is used during digest verification.
CVE-2021-37166	A buffer overflow issue leading to denial of service was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of softwa extensive time for the GUI to connect to the TCP socket, allowing the connection to be hijacked by an external attacker.
CVE-2021-27953	A NULL pointer dereference vulnerability exists on the ecobee3 lite 4.5.81.200 device in the HomeKit Wireless Access Control setup process. A threat actor can exploit
CVE-2021-37848	common/password.c in Pengutronix barebox through 2021.07.0 leaks timing information because strncmp is used during hash comparison.
CVE-2021-32811	Zope is an open-source web application server. Zope versions prior to versions 4.6.3 and 5.3 have a remote code execution security issue. In order to be affected, one `Products.PythonScripts` add-on package installed. By default, one must have the admin-level Zope "Manager" role to add or edit Script (Python) objects through the w vulnerable. As a workaround, a site administrator can restrict adding/editing Script (Python) objects through the web using the standard Zope user/role permission mecl restricted to trusted users only. This is the default configuration in Zope.
CVE-2021-34575	In MB connect line mymbCONNECT24, mbCONNECT24 in versions <= 2.8.0 an unauthenticated user can enumerate valid users by checking what kind of response th
CVE-2021-22391	There is an Incorrect Calculation of Buffer Size in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset.
CVE-2021-27491	Ypsomed mylife Cloud, mylife Mobile Application:Ypsomed mylife Cloud,All versions prior to 1.7.2,Ypsomed mylife App,All versions prior to 1.7.5,The Ypsomed mylife (
CVE-2021-22447	There is an Improper Check for Unusual or Exceptional Conditions Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the syste
CVE-2021-28966	In Ruby through 3.0 on Windows, a remote attacker can submit a crafted path when a Web application handles a parameter with TmpDir.
CVE-2021-33486	All versions of the CODESYS V3 Runtime Toolkit for VxWorks from version V3.5.8.0 and before version V3.5.17.10 have Improper Handling of Exceptional Conditions.
CVE-2021-32558	An issue was discovered in Sangoma Asterisk 13.x before 13.38.3, 16.x before 16.19.1, 17.x before 17.9.4, and 18.x before 18.5.1, and Certified Asterisk before 16.8-c
CVE-2021-20114	When installed following the default/recommended settings, TCExam <= 14.8.1 allowed unauthenticated users to access the /cache/backup/ directory, which included s
CVE-2021-36386	report_vbuild in report.c in Fetchmail before 6.4.20 sometimes omits initialization of the vsnprintf va_list argument, which might allow mail servers to cause a denial of s platform results in an impact beyond an inconvenience to the client user.

CVE Number	Description
CVE-2021-33323	The Dynamic Data Mapping module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 7, autosaves form values for u
CVE-2021-36754	PowerDNS Authoritative Server 4.5.0 before 4.5.1 allows anybody to crash the process by sending a specific query (QTYPE 65535) that causes an out-of-bounds exce
CVE-2020-16839	On Crestron DM-NVX-DIR, DM-NVX-DIR80, and DM-NVX-ENT devices before the DM-XIO/1-0-3-802 patch, the password can be changed by sending an unauthentic
CVE-2021-33322	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 18, and 7.2 before fix pack 5, password reset tokens are not invalidated at
CVE-2021-33321	Insecure default configuration in Liferay Portal 6.2.3 through 7.3.2, and Liferay DXP before 7.3, allows remote attackers to enumerate user email address via the forgot
CVE-2021-37601	muc.lib.lua in Prosody 0.11.0 through 0.11.9 allows remote attackers to obtain sensitive information (list of admins, members, owners, and banned entities of a Multi-Us
CVE-2021-35193	Patterson Application Service in Patterson Eaglesoft 18 through 21 accepts the same certificate authentication across different customers' installations (that have the sa credentials only occurs after a username/password authentication step; however, this authentication step is on the client side, and an attacker can develop their own cli
CVE-2020-14999	A logic bug in system monitoring driver of Acronis Agent after 12.5.21540 and before 12.5.23094 allowed to bypass Windows memory protection and access sensitive d
CVE-2020-10590	Replicated Classic 2.x versions have an improperly secured API that exposes sensitive data from the Replicated Admin Console configuration. An attacker with networl configure the Admin Console.
CVE-2020-19304	An issue in /admin/index.php?n=system&c=filept&a=doGetFileList of Metinfo v7.0.0 allows attackers to perform a directory traversal and access sensitive information.
CVE-2021-33403	An integer overflow in the transfer function of a smart contract implementation for Lancer Token, an Ethereum ERC20 token, allows the owner to cause unexpected fina
CVE-2021-34270	An integer overflow in the mintToken function of a smart contract implementation for Doftcoin Token, an Ethereum ERC20 token, allows the owner to cause unexpected
CVE-2021-23415	This affects the package elFinder.AspNet before 1.1.1. The user-controlled file name is not properly sanitized before it is used to create a file system path.
CVE-2021-34272	A security flaw in the 'owned' function of a smart contract implementation for RobotCoin (RBTC), a tradeable Ethereum ERC20 token, allows attackers to hijack victim a
CVE-2021-34273	A security flaw in the 'owned' function of a smart contract implementation for BTC2X (B2X), a tradeable Ethereum ERC20 token, allows attackers to hijack victim accou
CVE-2020-26565	ObjectPlanet Opinio before 7.14 allows Expression Language Injection via the admin/permissionList.do from parameter. This can be used to retrieve possibly sensitive
CVE-2021-36763	In CODESYS V3 web server before 3.5.17.10, files or directories are accessible to External Parties.
CVE-2021-32066	An issue was discovered in Ruby through 2.6.7, 2.7.x through 2.7.3, and 3.x through 3.0.1. Net::IMAP does not raise an exception when StartTLS fails with an an unkno the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2021-21553	Dell PowerScale OneFS versions 8.1.0-9.1.0 contain an Incorrect User Management vulnerability.under some specific conditions, this can allow the CompAdmin user t

CVE Number	Description
CVE-2021-33195	Go before 1.15.13 and 1.16.x before 1.16.5 has functions for DNS lookups that do not validate replies from DNS servers, and thus a return value may contain an unsaf
CVE-2021-33335	Privilege escalation vulnerability in Liferay Portal 7.0.3 through 7.3.4, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 9 allows remote authenticated use
CVE-2020-20698	A remote code execution (RCE) vulnerability in /1.com.php of S-CMS PHP v3.0 allows attackers to getshell via modification of a PHP file.
CVE-2021-29696	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could allow a remote authenticated attacker to execute arbitrary commands on
CVE-2021-35450	A Server Side Template Injection in the Entando Admin Console 6.3.9 and before allows a user with privileges to execute FreeMarker template with command executio
CVE-2021-24456	The Quiz Maker WordPress plugin before 6.2.0.9 did not properly sanitise and escape the order and orderby parameters before using them in SQL statements, leading
CVE-2021-24430	The Speed Booster Pack PageSpeed Optimization Suite WordPress plugin before 4.2.0 did not validate its caching_exclude_urls and caching_include_query_string
CVE-2021-36766	Concrete5 through 8.5.5 deserializes Untrusted Data. The vulnerable code is located within the controllers/single_page/dashboard/system/environment/logging.php Log call to the file_exists() PHP function. This can be exploited by malicious users to inject arbitrary PHP objects into the application scope (PHP Object Injection via phar://
CVE-2021-24484	The get_reports() function in the Secure Copy Content Protection and Content Locking WordPress plugin before 2.6.7 did not use whitelist or validate the orderby para
CVE-2021-24483	The get_poll_categories(), get_polls() and get_reports() functions in the Poll Maker WordPress plugin before 3.2.1 did not use whitelist or validate the orderby paramete
CVE-2021-32610	In Archive_Tar before 1.4.14, symlinks can refer to targets outside of the extracted archive, a different vulnerability than CVE-2020-36193.
CVE-2021-27495	Ypsomed mylife Cloud, mylife Mobile Application:Ypsomed mylife Cloud,All versions prior to 1.7.2,Ypsomed mylife App,All versions prior to 1.7.5,he Ypsomed mylife Cl
CVE-2021-31799	In RDoc 3.11 through 6.x before 6.3.1, as distributed with Ruby through 3.0.1, it is possible to execute arbitrary code via l and tags in a filename.
CVE-2021-27942	Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs allow a threat actor to execute arbitrary code from a USB drive via the Smart Cast functionality, because f
CVE-2021-22397	There is a privilege escalation vulnerability in Huawei ManageOne 8.0.0. External parameters of some files are lack of verification when they are be called. Attackers ca
CVE-2021-22521	A privileged escalation vulnerability has been identified in Micro Focus ZENworks Configuration Management, affecting version 2020 Update 1 and all prior versions. Tl
CVE-2021-28094	OX Documents before 7.10.5-rev7 has Incorrect Access Control for converted documents because hash collisions can occur, due to use of CRC32.
CVE-2021-23414	This affects the package video.js before 7.14.3. The src attribute of track tag allows to bypass HTML escaping and execute arbitrary code.
CVE-2021-32001	K3s in SUSE Rancher allows any user with direct access to the datastore, or a copy of a datastore backup, to extract the cluster's confidential keying material (cluster c This issue affects: SUSE Rancher K3s version v1.19.12+k3s1, v1.20.8+k3s1, v1.21.2+k3s1 and prior versions; RKE2 version v1.19.12+rke2r1, v1.20.8+rke2r1, v1.21.2

CVE Number	Description
CVE-2021-21581	Dell EMC iDRAC9 versions prior to 5.00.00.00 contain a cross-site scripting vulnerability. A remote attacker could potentially exploit this vulnerability to run malicious H
CVE-2020-26564	ObjectPlanet Opinio before 7.15 allows XXE attacks via three steps: modify a .css file to have <!ENTITY content, create a .xml file for a generic survey template (contai XXE can then be triggered at a admin/preview.do?action=previewSurvey&surveyId= URI.
CVE-2021-32806	Products.isurlinportal is a replacement for isURLInPortal method in Plone. Versions of Products.isurlinportal prior to 1.2.0 have an Open Redirect vulnerability. Various in the portal. The url `https:example.org` without slashes is considered to be in the portal. When redirecting, some browsers go to `https://example.org`, others give an Products.isurlinportal 1.2.0.
CVE-2021-31878	An issue was discovered in PJSIP in Asterisk before 16.19.1 and before 18.5.1. To exploit, a re-INVITE without SDP must be received after Asterisk has sent a BYE re
CVE-2021-37914	In Argo Workflows through 3.1.3, if EXPRESSION_TEMPLATES is enabled and untrusted users are allowed to specify input parameters when running workflows, an a
CVE-2021-21563	Dell EMC PowerScale OneFS versions 8.1.2-9.1.0.x contain an Improper Check for Unusual or Exceptional Conditions in its auditing component.This can lead to an au
CVE-2021-28093	OX Documents before 7.10.5-rev5 has Incorrect Access Control of converted images because hash collisions can occur, due to use of Adler32.
CVE-2021-37587	In Charm 0.43, any single user can decrypt DAC-MACS or MA-ABE-YJ14 data.
CVE-2021-30584	Incorrect security UI in Downloads in Google Chrome on Android prior to 92.0.4515.107 allowed a remote attacker to perform domain spoofing via a crafted HTML pag
CVE-2021-30583	Insufficient policy enforcement in image handling in iOS in Google Chrome on iOS prior to 92.0.4515.107 allowed a remote attacker to leak cross-origin data via a craft
CVE-2021-30582	Inappropriate implementation in Animation in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-30580	Insufficient policy enforcement in Android intents in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious application t
CVE-2021-33333	The Portal Workflow module in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 93, 7.1 before fix pack 19 and 7.2 before fix pack 6, does not proper
CVE-2020-26180	Dell EMC Isilon OneFS supported versions 8.1 and later and Dell EMC PowerScale OneFS supported version 9.0.0 contain an access issue with the remotesupport us
CVE-2021-23418	The package glances before 3.2.1 are vulnerable to XML External Entity (XXE) Injection via the use of Fault to parse untrusted XML data, which is known to be vulnera
CVE-2020-4974	IBM Jazz Foundation products are vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the
CVE-2021-36703	The "blog title" field in the "Settings" menu "config" page of "dashboard" in htmly 2.8.1 has a storage cross site scripting (XSS) vulnerability. It allows remote attackers t
CVE-2021-35265	A reflected cross-site scripting (XSS) vulnerability in MaxSite CMS before V106 via product/page/* allows remote attackers to inject arbitrary web script to a page.
CVE-2021-37596	Telegram Web K Alpha 0.6.1 allows XSS via a document name.

CVE Number	Description
CVE-2021-33332	Cross-site scripting (XSS) vulnerability in the Portlet Configuration module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before f _com_liferay_portlet_configuration_css_web_portlet_PortletConfigurationCSSPortlet_portletResource parameter.
CVE-2021-33331	Open redirect vulnerability in the Notifications module in Liferay Portal 7.0.0 through 7.3.1, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19 and 7.2 before
CVE-2020-21854	Cross Site Scripting vulnerabiity exists in WDScanner 1.1 in the system management page.
CVE-2020-26563	ObjectPlanet Opinio before 7.14 allows reflected XSS via the survey/admin/surveyAdmin.do?action=viewSurveyAdmin query string. (There is also stored XSS if input t
CVE-2021-37916	Joplin before 2.0.9 allows XSS via button and form in the note body.
CVE-2021-37833	A reflected cross-site scripting (XSS) vulnerability exists in multiple pages in version 3.0.2 of the Hotel Druid application that allows for arbitrary execution of JavaScript
CVE-2021-21576	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain a DOM-based cross-site scripting vulnerability. A remote attacker could potentially exploit this vulnerability to run
CVE-2021-21579	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect users t
CVE-2020-15948	eGain Chat 15.5.5 allows XSS via the Name (aka full_name) field.
CVE-2021-24477	The Migrate Users WordPress plugin through 1.0.1 does not sanitise or escape its Delimiter option before outputting in a page, leading to a Stored Cross-Site Scripting CSRF attack.
CVE-2021-21578	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect users t
CVE-2021-24474	The Awesome Weather Widget WordPress plugin through 3.0.2 does not sanitize the id parameter of its awesome_weather_refresh AJAX action, leading to an unauth
CVE-2021-37746	textview_uri_security_check in textview.c in Claws Mail before 3.18.0, and Sylpheed through 3.7.0, does not have sufficient link checks before accepting a click.
CVE-2020-5329	Dell EMC Avamar Server contains an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect application users to arbitrar
CVE-2021-24488	The slider import search feature and tab parameter of the Post Grid WordPress plugin before 2.1.8 settings are not properly sanitised before being output back in the pa
CVE-2021-21577	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain a DOM-based cross-site scripting vulnerability. A remote attacker could potentially exploit this vulnerability to run
CVE-2021-37216	QSAN Storage Manager header page parameters does not filter special characters. Remote attackers can inject JavaScript without logging in and launch reflected XSS
CVE-2021-24496	The Community Events WordPress plugin before 1.4.8 does not sanitise, validate or escape its importrowscount and successimportcount GET parameters before outpu administrator
CVE-2021-24498	The Calendar Event Multi View WordPress plugin before 1.4.01 does not sanitise or escape the 'start' and 'end' GET parameters before outputting them in the page (via

CVE Number	Description
CVE-2021-32019	There is missing input validation of host names displayed in OpenWrt before 19.07.8. The Connection Status page of the luci web-interface allows XSS, which can be u
CVE-2021-29979	Hubs Cloud allows users to download shared content, specifically HTML and JS, which could allow javascript execution in the Hub Cloud instance's primary hosting do
CVE-2021-36702	The "content" field in the "regular post" page of the "add content" menu under "dashboard" in htmly 2.8.1 has a storage cross site scripting (XSS) vulnerability. It allows content.
CVE-2020-22765	Cross Site Scripting (XSS) vulnerability in NukeViet cms 4.4.0 via the editor in the News module.
CVE-2021-20789	Open redirect vulnerability in GroupSession (GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud from ver3.0.3 to the versi an arbitrary web site and conduct a phishing attack via a specially crafted URL.
CVE-2021-34635	The Poll Maker WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the mcount parameter found in the ~/admin/partials/settings/poll-maker-settings.ph
CVE-2021-24504	The WP LMS – Best WordPress LMS Plugin WordPress plugin through 1.1.2 does not properly sanitise or validate its User Field Titles, allowing XSS payload to be use user (including unauthenticated)
CVE-2021-33326	Cross-site scripting (XSS) vulnerability in the Frontend JS module in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20 and
CVE-2021-27499	Ypsomed mylife Cloud, mylife Mobile Application, Ypsomed mylife Cloud: All versions prior to 1.7.2, Ypsomed mylife App: All versions prior to 1.7.5,The application laye man-in-the-middle attackers to tamper with messages.
CVE-2021-37588	In Charm 0.43, any two users can collude to achieve the ability to decrypt YCT14 data.
CVE-2021-23417	All versions of package deepmergefn are vulnerable to Prototype Pollution via deepMerge function.
CVE-2021-22424	A component of the HarmonyOS has a Kernel Memory Leakage Vulnerability. Local attackers may exploit this vulnerability to cause Kernel Denial of Service.
CVE-2021-34556	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel atta
CVE-2021-22419	A component of the HarmonyOS has a Insufficient Verification of Data Authenticity vulnerability. Local attackers may exploit this vulnerability to cause persistent dos.
CVE-2021-35477	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel atta value.
CVE-2021-37600	An integer overflow in util-linux through 2.37.1 can potentially cause a buffer overflow if an attacker were able to use system resources in a way that leads to a large nu
CVE-2021-22400	Some Huawei Smartphones has an insufficient input validation vulnerability due to the lack of parameter validation. An attacker may trick a user into installing a malicio 10.0.1.10(C00E10R1P1),10.0.1.105(C00E103R3P3),10.0.1.115(C00E110R3P3),10.0.1.123(C00E121R3P3),10.0.1.135(C00E130R3P3),10.0.1.135(C00E130R4P1),10 and 10.1.0.202(C00E79R5P1).
CVE-2021-22417	A component of the HarmonyOS has a Data Processing Errors vulnerability. Local attackers may exploit this vulnerability to cause Kernel Memory Leakage.
CVE-2021-20112	A stored cross-site scripting vulnerability exists in TCExam <= 14.8.1. Valid files uploaded via tce_select_mediafile.php with a filename beggining with a period will be r triggered when another user views the file.

CVE Number	Description
CVE-2021-36654	CMSuno 1.7 is vulnerable to an authenticated stored cross site scripting in modifying the filename parameter (tgo) while updating the theme.
CVE-2021-37743	app/View/GalaxyElements/ajax/index.ctp in MISP 2.4.147 allows Stored XSS when viewing galaxy cluster elements in JSON format.
CVE-2021-20111	A stored cross-site scripting vulnerability exists in TCExam <= 14.8.1. Valid files uploaded via tce_filemanager.php with a filename beggining with a period will be rende when another user views the file.
CVE-2021-37742	app/View/Elements/GalaxyClusters/view_relation_tree.ctp in MISP 2.4.147 allows Stored XSS when viewing galaxy cluster relationships.
CVE-2021-36605	engineercms 1.03 is vulnerable to Cross Site Scripting (XSS). There is no escaping in the nickname field on the user list page. When viewing this page, the JavaScript
CVE-2021-33328	Cross-site scripting (XSS) vulnerability in the Asset module's edit vocabulary page in Liferay Portal 7.0.0 through 7.3.4, and Liferay DXP 7.0 before fix pack 96, 7.1 befo _com_liferay_journal_web_portlet_JournalPortlet_name or (2) _com_liferay_document_library_web_portlet_DLAdminPortlet_name parameter.
CVE-2021-3351	OpenPLC runtime V3 through 2016-03-14 allows stored XSS via the Device Name to the web server's Add New Device page.
CVE-2021-28674	The node management page in SolarWinds Orion Platform before 2020.2.5 HF1 allows an attacker to create or delete a node (outside of the attacker's perimeter) via a Services/NodeManagement.asmx/DeleteObjNow is incorrect. To exploit this, an attacker must be authenticated and must have node management rights associated wit
CVE-2021-35478	Nagios Log Server before 2.1.9 contains Reflected XSS in the dropdown box for the alert history and audit log function. All parameters used for filtering are affected. Th
CVE-2021-24470	The Yada Wiki WordPress plugin before 3.4.1 did not sanitise, validate or escape the anchor attribute of its shortcode, leading to a Stored Cross-Site Scripting issue
CVE-2021-24478	The Bookshelf WordPress plugin through 2.0.4 does not sanitise or escape its "Paypal email address" setting before outputting it in the page, leading to an authenticate
CVE-2021-24468	The Leaflet Map WordPress plugin before 3.0.0 does not escape some shortcode attributes before they are used in JavaScript code or HTML, which could allow users
CVE-2021-24473	The User Profile Picture WordPress plugin before 2.6.0 was affected by an IDOR issue, allowing users with the upload_image capability (by default author and above) t
CVE-2020-5004	IBM Jazz Foundation products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the ir
CVE-2020-18158	Cross Site Scripting (XSS) vulnerability in HuCart 5.7.4 via nickname in index.php.
CVE-2021-24443	The About Me widget of the Youzify – BuddyPress Community, User Profile, Social Network & Membership WordPress plugin before 1.0.7 does not properly sanitise its affected user profile. This could allow a low privilege user to gain unauthorised access to the admin side of the blog by targeting an admin, inducing them to view their p
CVE-2021-24503	The Popular Brand Icons – Simple Icons WordPress plugin before 2.7.8 does not sanitise or validate some of its shortcode parameters, such as "color", "size" or "class approved by an admin to have the XSS triggered in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and eve
CVE-2021-35479	Nagios Log Server before 2.1.9 contains Stored XSS in the custom column view for the alert history and audit log function through the affected pp parameter. This affec
CVE-2021-24464	The YouTube Embed, Playlist and Popup by WpDevArt WordPress plugin before 2.3.9 did not escape, validate or sanitise some of its shortcode options, available to us

CVE Number	Description
CVE-2021-24455	The Tutor LMS – eLearning and online course solution WordPress plugin before 1.9.2 did not escape the Summary field of Announcements (when outputting it in an at when viewing the Announcements list, and could result in privilege escalation when viewed by an admin.
CVE-2020-19118	Cross Site Scripting (XSS) vulnerabiity in YzmCMS 5.2 via the site_code parameter in admin/index/init.html.
CVE-2021-23416	This affects all versions of package curly-bracket-parser. When used as a template library, it does not properly sanitize the user input.
CVE-2021-24476	The Steam Group Viewer WordPress plugin through 2.1 does not sanitise or escape its "Steam Group Address" settings before outputting it in the page, leading to an a
CVE-2021-20540	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could disclose sensitive information to an unauthorized user through HTTP GE
CVE-2021-30483	isomorphic-git before 1.8.2 allows Directory Traversal via a crafted repository.
CVE-2021-21565	Dell PowerScale OneFS versions 9.1.0.3 and earlier contain a denial of service vulnerability. SmartConnect had an error condition that may be triggered to loop, using
CVE-2021-37606	Meow hash 0.5/calico does not sufficiently thwart key recovery by an attacker who can query whether there's a collision in the bottom bits of the hashes of two messag differences.
CVE-2021-26085	Affected versions of Atlassian Confluence Server allow remote attackers to view restricted resources via a Pre-Authorization Arbitrary File Read vulnerability in the /s/ e
CVE-2021-20539	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could disclose sensitive information to an unauthorized user through HTTP GE
CVE-2021-20113	An exposure of sensitive information vulnerability exists in TCExam <= 14.8.1. If a password reset request was made for an email address that was not registered with appear. A malicious actor could abuse this to enumerate the email addresses of
CVE-2021-29297	Buffer Overflow in Emerson GE Automation Proficy Machine Edition v8.0 allows an attacker to cause a denial of service and application crash via crafted traffic from a I
CVE-2021-29298	Improper Input Validation in Emerson GE Automation Proficy Machine Edition v8.0 allows an attacker to cause a denial of service and application crash via crafted traff
CVE-2021-36156	An issue was discovered in Grafana Loki through 2.2.1. The header value X-Scope-OrgID is used to construct file paths for rules files, and if crafted to conduct directory some of the contents in the error message.
CVE-2021-36157	An issue was discovered in Grafana Cortex through 1.9.0. The header value X-Scope-OrgID is used to construct file paths for rules files, and if crafted to conduct direct include some of the contents in the error message. (Other Cortex API requests can also be sent a malicious OrgID header, e.g., tricking the ingester into writing metrics
CVE-2021-33617	Zoho ManageEngine Password Manager Pro before 11.2 11200 allows login/AjaxResponse.jsp?RequestType=GetUserDomainName&userName= username enumera
CVE-2021-20541	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could disclose sensitive information to an unauthorized user through HTTP GE
CVE-2021-33197	In Go before 1.15.13 and 1.16.x before 1.16.5, some configurations of ReverseProxy (from net/http/httputil) result in a situation where an attacker is able to drop arbitra
CVE-2021-22552	An untrusted memory read vulnerability in Asylo versions up to 0.6.1 allows an untrusted attacker to pass a syscall number in MessageReader that is then used by sys Asylo 0.6.3 or past https://github.com/google/asylo/commit/90d7619e9dd99bcdb6cd28c7649d741d254d9a1a

CVE Number	Description
CVE-2021-34630	In the Pro and Enterprise versions of GTranslate < 2.8.65, the gtranslate_request_uri_var function runs at the top of all pages and echoes out the contents of $_SERVE vulnerable to Reflected XSS in older browsers such as Internet Explorer 9 or below, or in cases where an attacker is able to modify the request en route between the cl
CVE-2021-29697	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could allow a remote authenticated attacker to obtain sensitive information thro
CVE-2021-33325	The Portal Workflow module in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 93, 7.1 before fix pack 19, and 7.2 before fix pack 7, user's clear tex obtain a user's password.
CVE-2021-20787	Cross-site scripting vulnerability in GroupSession (GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud from ver3.0.3 to the arbitrary script by sending a specially crafted request to a specific URL.
CVE-2021-28095	OX Documents before 7.10.5-rev5 has Incorrect Access Control for documents that contain XML structures because hash collisions can occur, due to use of CRC32.
CVE-2021-25273	Stored XSS can execute as administrator in quarantined email detail view in Sophos UTM before version 9.706.
CVE-2021-20785	Cross-site scripting vulnerability in GroupSession (GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud from ver3.0.3 to the arbitrary script by sending a specially crafted request to a specific URL.
CVE-2020-20699	A cross site scripting (XSS) vulnerability in S-CMS PHP v3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the Copyright
CVE-2020-20700	A stored cross site scripting (XSS) vulnerability in /app/form_add/of S-CMS PHP v3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload e
CVE-2020-20701	A stored cross site scripting (XSS) vulnerability in /app/config/of S-CMS PHP v3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.
CVE-2021-32813	Traefik is an HTTP reverse proxy and load balancer. Prior to version 2.4.13, there exists a potential header vulnerability in Traefik's handling of the Connection header. team has addressed this issue to prevent any potential abuse. If one has a chain of Traefik middlewares, and one of them sets a request header, then sending a reque request header. A patch is available in version 2.4.13. There are no known workarounds aside from upgrading.
CVE-2021-24450	The User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar) WordPress plugin before 3.1.8 did not sanitise or escape some of payloads in them even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue
CVE-2021-24428	The RSS for Yandex Turbo WordPress plugin through 1.30 does not sanitise or escape some of its settings before saving and outputing them in the admin dashboard,
CVE-2021-27503	Ypsomed mylife Cloud, mylife Mobile Application, Ypsomed mylife Cloud: All versions prior to 1.7.2, Ypsomed mylife App: All versions prior to 1.7.5,The application enc hard-coded secrets, which allows man-in-the-middle attackers to tamper with messages.
CVE-2021-24481	The Any Hostname WordPress plugin through 1.0.6 does not sanitise or escape its "Allowed hosts" setting, leading to an authenticated stored XSS issue as high privile
CVE-2021-24480	The Event Geek WordPress plugin through 2.5.2 does not sanitise or escape its "Use your own " setting before outputting it in the page, leading to an authenticated (ac
CVE-2021-24479	The DrawBlog WordPress plugin through 0.90 does not sanitise or validate some of its settings before outputting them back in the page, leading to an authenticated sto
CVE-2021-24448	The User Registration & User Profile – Profile Builder WordPress plugin before 3.4.8 does not sanitise or escape its 'Modify default Redirect Delay timer' setting, allowir Stored Cross-Site Scripting issue
CVE-2021-24444	The TaxoPress – Create and Manage Taxonomies, Tags, Categories WordPress plugin before 3.0.7.2 does not sanitise its Taxonomy description field, allowing high pr Stored Cross-Site Scripting issue.

CVE Number	Description
CVE-2021-24425	The Floating Notification Bar, Sticky Menu on Scroll, and Sticky Header for Any Theme – myStickymenu WordPress plugin before 2.5.2 does not sanitise or escape its be triggered in the plugin's setting, as well as all front-page of the blog (when the Welcome bar is active)
CVE-2021-32812	Monkshu is an enterprise application server for mobile apps (iOS and Android), responsive HTML 5 apps, and JSON API services. In version 2.90 and earlier, there is a bug in the server which will cause a 500 error, and the response will then embed the URL provided by the hacker. The impact is moderate as the hacker must also be a in version 2.95. As a workaround, one may use a disk caching plugin.
CVE-2021-3636	It was found in OpenShift, before version 4.8, that the generated certificate for the in-cluster Service CA, incorrectly included additional certificates. The Service CA is a trusted Service CA. The incorrect inclusion of additional CAs in this certificate would allow an attacker that compromises any of the additional CAs to masquerade as a
CVE-2021-22398	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2
CVE-2021-20505	The PowerVM Logical Partition Mobility(LPM) (PowerVM Hypervisor FW920, FW930, FW940, and FW950) encryption key exchange protocol can be compromised. If a information to perform a series of PowerVM service procedures to decrypt the captured migration traffic IBM X-Force ID: 198232
CVE-2021-21562	Dell EMC PowerScale OneFS contains an untrusted search path vulnerability. This vulnerability allows a user with (ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONS under the application’s direct control.
CVE-2021-32807	The module `AccessControl` defines security policies for Python code used in restricted code within Zope applications. Restricted code is any code that resides in Zope Python modules and only exempt a few that are deemed safe, such as Python's `string` module. However, full access to the `string` module also allows access to the c libraries. Those unsafe Python libraries can be used for remote code execution. By default, you need to have the admin-level Zope "Manager" role to add or edit `Script very unusual configuration to begin with - are at risk. The problem has been fixed in AccessControl 4.3 and 5.2. Only AccessControl versions 4 and 5 are vulnerable, ar the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing these scripts th
CVE-2021-33334	The Dynamic Data Mapping module in Liferay Portal 7.0.0 through 7.3.2, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19, and 7.2 before fix pack 6, does forms and form entries in a site via the forms section in site administration.
CVE-2021-33324	The Layout module in Liferay Portal 7.1.0 through 7.3.1, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 5, does not properly check permission of pages
CVE-2021-34574	In MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual in all versions through v2.11.2 an authenticated attacker can c is send to the server.
CVE-2021-35343	Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.Ajax.php in SeedDMS v5.1.x<5.1.23 and v6.0.x<6.0.16 allows a remote attacker to edit document name
CVE-2021-33330	Liferay Portal 7.2.0 through 7.3.2, and Liferay DXP 7.2 before fix pack 9, allows access to Cross-origin resource sharing (CORS) protected resources if the user is only targeted user’s email address and current CSRF token.
CVE-2021-33327	The Portlet Configuration module in Liferay Portal 7.2.0 through 7.3.3, and Liferay DXP 7.0 fix pack pack 93 and 94, 7.1 fix pack 18, and 7.2 before fix pack 8, does not enabled.
CVE-2021-20788	Server-side request forgery (SSRF) vulnerability in GroupSession (GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud fror authenticated attacker to conduct a port scan from the product and/or obtain information from the internal Web server.
CVE-2021-34629	The SendGrid WordPress plugin is vulnerable to authorization bypass via the get_ajax_statistics function found in the ~/lib/class-sendgrid-statistics.php file which allow
CVE-2021-36543	Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.UnlockDocument.php in SeedDMS v5.1.x <5.1.23 and v6.0.x <6.0.16 allows a remote attacker to unlock
CVE-2021-20786	Cross-site request forgery (CSRF) vulnerability in GroupSession (GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud from to hijack the authentication of administrators via a specially crafted URL.
CVE-2021-33320	The Flags module in Liferay Portal 7.3.1 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20, and 7.2 before fix pack 5, does not limit the rate at v
CVE-2021-30589	Insufficient validation of untrusted input in Sharing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to bypass navigation restrictions via a crafted cli

CVE Number	Description
CVE-2021-30587	Inappropriate implementation in Compositing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL
CVE-2021-21580	Dell EMC iDRAC8 versions prior to 2.80.80.80 & Dell EMC iDRAC9 versions prior to 5.00.00.00 contain a Content spoofing / Text injection, where a malicious URL can
CVE-2021-36542	Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.LockDocument.php in SeedDMS v5.1.x<5.1.23 and v6.0.x <6.0.16 allows a remote attacker to lock any d
CVE-2021-20332	Specific MongoDB Rust Driver versions can include credentials used by the connection pool to authenticate connections in the monitoring event that is emitted when th that such monitoring is not enabled by default. This issue affects MongoDB Rust Driver version 2.0.0-alpha, MongoDB Rust Driver version 2.0.0-alpha1 and MongoDB
CVE-2021-32000	A UNIX Symbolic Link (Symlink) Following vulnerability in the clone-master-clean-up.sh script of clone-master-clean-up in SUSE Linux Enterprise Server 12 SP3, SUSE Enterprise Server 12 SP3 clone-master-clean-up version 1.6-4.6.1 and prior versions. SUSE Linux Enterprise Server 15 SP1 clone-master-clean-up version 1.6-3.9.1 a
CVE-2021-32787	Sourcegraph is a code search and navigation engine. Sourcegraph before version 3.30.0 has two potential information leaks. The site-admin area can be accessed by indexes. It is not possible to alter the information, nor interact with any other features in the site-admin area. The issue is patched in version 3.30.0, where the informati
CVE-2021-24371	The Import feature of the RSVPMaker WordPress plugin before 8.7.3 (/wp-admin/tools.php?page=rsvpmaker_export_screen) takes an URL input and calls curl on it, w a SSRF attack.
CVE-2021-36379	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that