SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 October 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-2021-38454	A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.	10.0	More Details
CVE-2021-21940	A heap-based buffer overflow vulnerability exists in the pushMuxer processRtspInfo functionality of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted network packet can lead to a heap buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	10.0	More Details
CVE-2021-29798	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 203734.	9.8	More Details
CVE-2021-40543	Opensis-Classic Version 8.0 is affected by a SQL injection vulnerability due to a lack of sanitization of input data at two parameters $_GET['usrid'] and $_GET['prof_id'] in the PasswordCheck.php file.	9.8	More Details
CVE-2020-21725	OpenSNS v6.1.0 contains a blind SQL injection vulnerability in /Controller/ChinaCityController.class.php via the pid parameter.	9.8	More Details
CVE-2021-29903	IBM Sterling B2B Integrator Standard Edition 5.2.6.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 207506.	9.8	More Details
CVE-2021-38298	Zoho ManageEngine ADManager Plus before 7110 is vulnerable to blind XXE.	9.8	More Details
CVE-2021-35977	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution.	9.8	More Details
CVE-2021-36767	In Digi RealPort through 4.10.490, authentication relies on a challenge-response mechanism that gives access to the server password, making the protection ineffective. An attacker may send an unauthenticated request to the server. The server will reply with a weakly-hashed version of the server's access password. The attacker may then crack this hash offline in order to successfully login to the server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41566	The file extension of the TadTools file upload function fails to filter, thus remote attackers can upload any types of files and execute arbitrary code without logging in.	9.8	More Details
CVE-2021-42109	VITEC Exterity IPTV products through 2021-04-30 allow privilege escalation to root.	9.8	More Details
CVE-2020-22617	Ardour v5.12 contains a use-after-free vulnerability in the component ardour/libs/pbd/xml++.cc when using xmlFreeDoc and xmlXPathFreeContext.	9.8	More Details
CVE-2021-42139	Deno Standard Modules before 0.107.0 allows Code Injection via an untrusted YAML file in certain configurations.	9.8	More Details
CVE-2021-40889	CMSUno version 1.7.2 is affected by a PHP code execution vulnerability. sauvePass action in {webroot}/uno/central.php file calls to file_put_contents() function to write username in password.php file when a user successfully changed their password. The attacker can inject malicious PHP code into password.php and then use the login function to execute code.	9.8	More Details
CVE-2021-40887	Projectsend version r1295 is affected by a directory traversal vulnerability. Because of lacking sanitization input for files[] parameter, an attacker can add ../ to move all PHP files or any file on the system that has permissions to /upload/files/ folder.	9.8	More Details
CVE-2021-37123	There is an improper authentication vulnerability in Hero-CT060 before 1.0.0.200. The vulnerability is due to that when an user wants to do certain operation, the software does not insufficiently validate the user's identity. Successful exploit could allow the attacker to do certain operations which the user are supposed not to do.	9.8	More Details
CVE-2021-27664	Under certain configurations an unauthenticated remote user could be given access to credentials stored in the exacqVision Server.	9.8	More Details
CVE-2020-21865	ThinkPHP50-CMS v1.0 contains a remote code execution (RCE) vulnerability in the component /public/?s=captcha.	9.8	More Details
CVE-2021-26588	A potential security vulnerability has been identified in HPE 3PAR StoreServ, HPE Primera Storage and HPE Alletra 9000 Storage array firmware. An unauthenticated user could remotely exploit the low complexity issue to execute code as administrator. This vulnerability impacts completely the confidentiality, integrity, availability of the array. HPE has made the following software updates and mitigation information to resolve the vulnerability in 3PAR, Primera and Alletra 9000 firmware.	9.8	More Details
CVE-2020-27372	A buffer overflow vulnerability exists in Brandy Basic V Interpreter 1.21 in the run_interpreter function.	9.8	More Details
CVE-2021-40239	A Buffer Overflow vulnerability exists in the latest version of Miniftpd in the do_retr function in ftpproto.c	9.8	More Details
CVE-2021-40617	An SQL Injection vulnerability exists in openSIS Community Edition version 8.0 via ForgotPassUserName.php.	9.8	More Details
CVE-2021-38456	A use of hard-coded password vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to gain access through accounts using default passwords	9.8	More Details
CVE-2021-38458	A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.	9.8	More Details
CVE-2021-37726	A remote buffer overflow vulnerability was discovered in HPE Aruba Instant (IAP) version(s): Aruba Instant 8.7.x.x: 8.7.0.0 through 8.7.1.2. Aruba has released patches for Aruba Instant (IAP) that address this security vulnerability.	9.8	More Details
CVE-2021-38180	SAP Business One - version 10.0, allows an attacker to inject formulas when exporting data to Excel (CSV injection) due to improper sanitation during the data export. An attacker could thereby execute arbitrary commands on the victim's computer but only if the victim allows to execute macros while opening the file and the security settings of Excel allow for command execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40499	Client-side printing services SAP Cloud Print Manager and SAPSprint for SAP NetWeaver Application Server for ABAP - versions 7.70, 7.70 PI, 7.70 BYD, allow an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	9.8	More Details
CVE-2021-40618	An SQL Injection vulnerability exists in openSIS Classic 8.0 via the 1) ADDR_CONT_USRN, 2) ADDR_CONT_PSWD, 3) SECN_CONT_USRN or 4) SECN_CONT_PSWD parameters in HoldAddressFields.php.	9.8	More Details
CVE-2021-42090	An issue was discovered in Zammad before 4.1.1. The Form functionality allows remote code execution because deserialization is mishandled.	9.8	More Details
CVE-2020-21726	OpenSNS v6.1.0 contains a blind SQL injection vulnerability in /Controller/ChinaCityController.class.php via the cid parameter.	9.8	More Details
CVE-2021-42094	An issue was discovered in Zammad before 4.1.1. Command Injection can occur via custom Packages.	9.8	More Details
CVE-2021-37923	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-29908	The IBM TS7700 Management Interface is vulnerable to unauthenticated access. By accessing a specially-crafted URL, an attacker may gain administrative access to the Management Interface without authentication. IBM X-Force ID: 207747.	9.8	More Details
CVE-2020-21651	Myucms v2.2.1 contains a remote code execution (RCE) vulnerability in the component \controller\point.php, which can be exploited via the add() method.	9.8	More Details
CVE-2020-21652	Myucms v2.2.1 contains a remote code execution (RCE) vulnerability in the component \controller\Config.php, which can be exploited via the addqq() method.	9.8	More Details
CVE-2021-32172	Maian Cart v3.8 contains a preauthorization remote code execution (RCE) exploit via a broken access control issue in the Elfinder plugin.	9.8	More Details
CVE-2021-22930	Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.	9.8	More Details
CVE-2021-22958	A Server-Side Request Forgery vulnerability was found in concrete5 < 8.5.5 that allowed a decimal notation encoded IP address to bypass the limitations in place for localhost allowing interaction with local services. Impact can vary depending on services exposed.CVSSv2.0 AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N	9.8	More Details
CVE-2021-3832	Integria IMS in its 5.0.92 version is vulnerable to a Remote Code Execution attack through file uploading. An unauthenticated attacker could abuse the AsyncUpload() function in order to exploit the vulnerability.	9.8	More Details
CVE-2021-37762	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file overwrite leading to remote code execution.	9.8	More Details
CVE-2021-37919	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37920	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37921	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37918	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37924	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37929	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-42071	In Visual Tools DVR VX16 4.2.28.0, an unauthenticated attacker can achieve remote command execution via shell metacharacters in the cgi-bin/slogin/login.py User-Agent HTTP header.	9.8	More Details
CVE-2021-42013	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions.	9.8	More Details
CVE-2021-3833	Integria IMS login check uses a loose comparator ("==") to compare the MD5 hash of the password provided by the user and the MD5 hash stored in the database. An attacker with a specific formatted password could exploit this vulnerability in order to login in the system with different passwords.	9.8	More Details
CVE-2021-37930	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37931	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37928	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-37926	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution.	9.8	More Details
CVE-2021-42325	Froxlor through 0.10.29.1 allows SQL injection in Database/Manager/DbManagerMySQL.php via a custom DB name.	9.8	More Details
CVE-2021-37973	Use after free in Portals in Google Chrome prior to 94.0.4606.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-30633	Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-41974	Tad Book3 editing book page does not perform identity verification. Remote attackers can use the vulnerability to view and modify arbitrary content of books without permission.	9.1	More Details
CVE-2021-33724	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system contains an Arbitrary File Deletion vulnerability that possibly allows to delete an arbitrary file or directory under a user controlled path.	9.1	More Details
CVE-2021-33725	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to delete arbitrary files or directories under a user controlled path and does not correctly check if the relative path is still within the intended target directory.	9.1	More Details
CVE-2020-21653	Myucms v2.2.1 contains a server-side request forgery (SSRF) in the component \controller\index.php, which can be exploited via the sj() method.	9.1	More Details
CVE-2021-42091	An issue was discovered in Zammad before 4.1.1. SSRF can occur via GitHub or GitLab integration.	9.1	More Details
CVE-2020-21648	WDJA CMS v1.5.2 contains an arbitrary file deletion vulnerability in the component admin/cache/manage.php.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41128	Hygeia is an application for collecting and processing personal and case data in connection with communicable diseases. In affected versions all CSV Exports (Statistics & BAG MED) contain a CSV Injection Vulnerability. Users of the system are able to submit formula as exported fields which then get executed upon ingestion of the exported file. There is no validation or sanitization of these formula fields and so malicious may construct malicious code. This vulnerability has been resolved in version 1.30.4. There are no workarounds and all users are advised to upgrade their package.	9.1	More Details
CVE-2021-38923	IBM PowerVM Hypervisor FW1010 could allow a privileged user to gain access to another VM due to assigning duplicate WWPNs. IBM X-Force ID: 210162.	9.1	More Details
CVE-2021-21941	A use-after-free vulnerability exists in the pushMuxer CreatePushThread functionality of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted set of network packets can lead to remote code execution.	9.0	More Details
CVE-2021-35495	The Scheduler Connection component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for ActiveMatrix BPM, and TIBCO JasperReports Server for Microsoft Azure contains an easily exploitable vulnerability that allows an authenticated attacker with network access to obtain FTP server passwords for other users of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 7.2.1 and below, TIBCO JasperReports Server: versions 7.5.0 and 7.5.1, TIBCO JasperReports Server: version 7.8.0, TIBCO JasperReports Server: version 7.9.0, TIBCO JasperReports Server - Community Edition: versions 7.8.0 and below, TIBCO JasperReports Server - Developer Edition: versions 7.9.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 7.9.0 and below, TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.9.0 and below, and TIBCO JasperReports Server for Microsoft Azure: version 7.8.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-41916	A Cross-Site Request Forgery (CSRF) vulnerability in webTareas version 2.4 and earlier allows a remote attacker to create a new administrative profile and add a new user to the new profile. without the victim's knowledge, by enticing an authenticated admin user to visit an attacker's web page.	8.8	More Details
CVE-2021-38178	The software logistics system of SAP NetWeaver AS ABAP and ABAP Platform versions - 700, 701, 702, 710, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, enables a malicious user to transfer ABAP code artifacts or content, by-passing the established quality gates. By this vulnerability malicious code can reach quality and production, and can compromise the confidentiality, integrity, and availability of the system and its data.	8.8	More Details
CVE-2021-37974	Use after free in Safebrowsing in Google Chrome prior to 94.0.4606.71 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-2021-33729	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). An authenticated attacker that is able to import firmware containers to an affected system could execute arbitrary commands in the local database.	8.8	More Details
CVE-2021-33903	In LCOS 10.40 to 10.42.0473-RU3 with SNMPv3 enabled on LANCOM devices, changing the password of the root user via the CLI does not change the password of the root user for SNMPv3 access. (However, changing the password of the root user via LANconfig does change the password of the root user for SNMPv3 access.)	8.8	More Details
CVE-2021-25966	In “Orchard core CMS” application, versions 1.0.0-beta1-3383 to 1.0.0 are vulnerable to an improper session termination after password change. When a password has been changed by the user or by an administrator, a user that was already logged in, will still have access to the application even after the password was changed.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41801	The ReplaceText extension through 1.41 for MediaWiki has Incorrect Access Control. When a user is blocked after submitting a replace job, the job is still run, even if it may be run at a later time (due to the job queue backlog)	8.8	More Details
CVE-2020-21650	Myucms v2.2.1 contains a remote code execution (RCE) vulnerability in the component \controller\Config.php, which can be exploited via the add() method.	8.8	More Details
CVE-2021-24546	The Gutenberg Block Editor Toolkit – EditorsKit WordPress plugin before 1.31.6 does not sanitise and validate the Conditional Logic of the Custom Visibility settings, allowing users with a role as low contributor to execute Arbitrary PHP code	8.8	More Details
CVE-2021-24711	The del_reistered_domains AJAX action of the Software License Manager WordPress plugin before 4.5.1 does not have any CSRF checks, and is vulnerable to a CSRF attack	8.8	More Details
CVE-2021-37970	Use after free in File System API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-29004	rConfig 3.9.6 is affected by SQL Injection. A user must be authenticated to exploit the vulnerability. If --secure-file-priv in MySQL server is not set and the Mysql server is the same as rConfig, an attacker may successfully upload a webshell to the server and access it remotely.	8.8	More Details
CVE-2021-29005	Insecure permission of chmod command on rConfig server 3.9.6 exists. After installing rConfig apache user may execute chmod as root without password which may let an attacker with low privilege to gain root access on server.	8.8	More Details
CVE-2021-39317	A WordPress plugin and several WordPress themes developed by AccessPress Themes are vulnerable to malicious file uploads via the plugin_offline_installer AJAX action due to a missing capability check in the plugin_offline_installer_callback function found in the /demo-functions.php file or /welcome.php file of the affected products. The complete list of affected products and their versions are below: WordPress Plugin: AccessPress Demo Importer <=1.0.6 WordPress Themes: accesspress-basic <= 3.2.1 accesspress-lite <= 2.92 accesspress-mag <= 2.6.5 accesspress-parallax <= 4.5 accesspress-root <= 2.5 accesspress-store <= 2.4.9 agency-lite <= 1.1.6 arrival <= 1.4.2 bingle <= 1.0.4 bloger <= 1.2.6 brovy <= 1.3 construction-lite <= 1.2.5 doko <= 1.0.27 edict-lite <= 1.1.4 eightlaw-lite <= 2.1.5 eightmedi-lite <= 2.1.8 eight-sec <= 1.1.4 eightstore-lite <= 1.2.5 enlighten <= 1.3.5 fotography <= 2.4.0 opstore <= 1.4.3 parallaxsome <= 1.3.6 punte <= 1.1.2 revolve <= 1.3.1 ripple <= 1.2.0 sakala <= 1.0.4 scrollme <= 2.1.0 storevilla <= 1.4.1 swing-lite <= 1.1.9 the100 <= 1.1.2 the-launcher <= 1.3.2 the-monday <= 1.4.1 ultra-seven <= 1.2.8 uncode-lite <= 1.3.3 vmag <= 1.2.7 vmagazine-lite <= 1.3.5 vmagazine-news <= 1.0.5 wpparallax <= 2.0.6 wp-store <= 1.1.9 zigcy-baby <= 1.0.6 zigcy-cosmetics <= 1.0.5 zigcy-lite <= 2.0.9	8.8	More Details
CVE-2021-29837	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 204913.	8.8	More Details
CVE-2021-34748	A vulnerability in the web-based management interface of Cisco Intersight Virtual Appliance could allow an authenticated, remote attacker to perform a command injection attack on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by using the web-based management interface to execute a command using crafted input. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on an affected device.	8.8	More Details
CVE-2021-34735	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2021-34710	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37972	Out of bounds read in libjpeg-turbo in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-37975	Use after free in V8 in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-37962	Use after free in Performance Manager in Google Chrome prior to 94.0.4606.54 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-2021-30629	Use after free in Permissions in Google Chrome prior to 93.0.4577.82 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-2021-41919	webTareas version 2.4 and earlier allows an authenticated user to arbitrarily upload potentially dangerous files without restrictions. This is working by adding or replacing a personal profile picture. The affected endpoint is /includes/upload.php on the HTTP POST data. This allows an attacker to exploit the platform by injecting code or malware and, under certain conditions, to execute code on remote user browsers.	8.8	More Details
CVE-2021-41133	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.4 and 1.12.0, Flatpak apps with direct access to AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can trick portals and other host-OS services into treating the Flatpak app as though it was an ordinary, non-sandboxed host-OS process. They can do this by manipulating the VFS using recent mount-related syscalls that are not blocked by Flatpak's denylist seccomp filter, in order to substitute a crafted `/.flatpak-info` or make that file disappear entirely. Flatpak apps that act as clients for AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can escalate the privileges that the corresponding services will believe the Flatpak app has. Note that protocols that operate entirely over the D-Bus session bus (user bus), system bus or accessibility bus are not affected by this. This is due to the use of a proxy process `xdg-dbus-proxy`, whose VFS cannot be manipulated by the Flatpak app, when interacting with these buses. Patches exist for versions 1.10.4 and 1.12.0, and as of time of publication, a patch for version 1.8.2 is being planned. There are no workarounds aside from upgrading to a patched version.	8.8	More Details
CVE-2021-30625	Use after free in Selection API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who convinced the user the visit a malicious website to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30626	Out of bounds memory access in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30627	Type confusion in Blink layout in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-37961	Use after free in Tab Strip in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-42086	An issue was discovered in Zammad before 4.1.1. An Agent account can modify account data, and gain admin access, via a crafted request.	8.8	More Details
CVE-2021-30628	Stack buffer overflow in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30632	Out of bounds write in V8 in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-37956	Use after free in Offline use in Google Chrome on Android prior to 94.0.4606.54 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-2021-37957	Use after free in WebGPU in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-37959	Use after free in Task Manager in Google Chrome prior to 94.0.4606.54 allowed an attacker who convinced a user to enage in a series of user gestures to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-20489	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 197790.	8.8	More Details
CVE-2021-41117	keypair is a a RSA PEM key generator written in javascript. keypair implements a lot of cryptographic primitives on its own or by borrowing from other libraries where possible, including node-forge. An issue was discovered where this library was generating identical RSA keys used in SSH. This would mean that the library is generating identical P, Q (and thus N) values which, in practical terms, is impossible with RSA-2048 keys. Generating identical values, repeatedly, usually indicates an issue with poor random number generation, or, poor handling of CSPRNG output. Issue 1: Poor random number generation (`GHSL-2021-1012`). The library does not rely entirely on a platform provided CSPRNG, rather, it uses it's own counter-based CMAC approach. Where things go wrong is seeding the CMAC implementation with "true" random data in the function `defaultSeedFile`. In order to seed the AES-CMAC generator, the library will take two different approaches depending on the JavaScript execution environment. In a browser, the library will use [`window.crypto.getRandomValues()`] (https://github.com/juliangruber/keypair/blob/87c62f255baa12c1ec4f98a91600f82af80be6db/index.js#L971). However, in a nodeJS execution environment, the `window` object is not defined, so it goes down a much less secure solution, also of which has a bug in it. It does look like the library tries to use node's CSPRNG when possible unfortunately, it looks like the `crypto` object is null because a variable was declared with the same name, and set to `null`. So the node CSPRNG path is never taken. However, when `window.crypto.getRandomValues()` is not available, a Lehmer LCG random number generator is used to seed the CMAC counter, and the LCG is seeded with `Math.random`. While this is poor and would likely qualify in a security bug in itself, it does not explain the extreme frequency in which duplicate keys occur. The main flaw: The output from the Lehmer LCG is encoded incorrectly. The specific [line] [https://github.com/juliangruber/keypair/blob/87c62f255baa12c1ec4f98a91600f82af80be6db/index.js#L1008] with the flaw is: `b.putByte(String.fromCharCode(next & 0xFF))` The [definition] (https://github.com/juliangruber/keypair/blob/87c62f255baa12c1ec4f98a91600f82af80be6db/index.js#L350-L352) of `putByte` is `util.ByteBuffer.prototype.putByte = function(b) {this.data += String.fromCharCode(b);};`. Simplified, this is `String.fromCharCode(String.fromCharCode(next & 0xFF))`. The double `String.fromCharCode` is almost certainly unintentional and the source of weak seeding. Unfortunately, this does not result in an error. Rather, it results most of the buffer containing zeros. Since we are masking with 0xFF, we can determine that 97% of the output from the LCG are converted to zeros. The only outputs that result in meaningful values are outputs 48 through 57, inclusive. The impact is that each byte in the RNG seed has a 97% chance of being 0 due to incorrect conversion. When it is not, the bytes are 0 through 9. In summary, there are three immediate concerns: 1. The library has an insecure random number fallback path. Ideally the library would require a strong CSPRNG instead of attempting to use a LCG and `Math.random`. 2. The library does not correctly use a strong random number generator when run in NodeJS, even though a strong CSPRNG is available. 3. The fallback path has an issue in the implementation where a majority of the seed data is going to effectively be zero. Due to the poor random number generation, keypair generates RSA keys that are relatively easy to guess. This could enable an attacker to decrypt confidential messages or gain authorized access to an account belonging to the victim.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34698	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation.	8.6	More Details
CVE-2021-3323	Integer Underflow in 6LoWPAN IPHC Header Uncompression in Zephyr. Zephyr versions >= >=2.4.0 contain Integer Underflow (Wrap or Wraparound) (CWE-191). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-89j6-qpxf-pfpc	8.3	More Details
CVE-2020-21649	Myucms v2.2.1 contains a server-side request forgery (SSRF) in the component \controller\index.php, which can be exploited via the sql() method.	8.1	More Details
CVE-2021-41129	Pterodactyl is an open-source game server management panel built with PHP 7, React, and Go. A malicious user can modify the contents of a `confirmation_token` input during the two-factor authentication process to reference a cache value not associated with the login attempt. In rare cases this can allow a malicious actor to authenticate as a random user in the Panel. The malicious user must target an account with two-factor authentication enabled, and then must provide a correct two-factor authentication token before being authenticated as that user. Due to a validation flaw in the logic handling user authentication during the two-factor authentication process a malicious user can trick the system into loading credentials for an arbitrary user by modifying the token sent to the server. This authentication flaw is present in the `LoginCheckpointController@__invoke` method which handles two-factor authentication for a user. This controller looks for a request input parameter called `confirmation_token` which is expected to be a 64 character random alpha-numeric string that references a value within the Panel's cache containing a `user_id` value. This value is then used to fetch the user that attempted to login, and lookup their two-factor authentication token. Due to the design of this system, any element in the cache that contains only digits could be referenced by a malicious user, and whatever value is stored at that position would be used as the `user_id`. There are a few different areas of the Panel that store values into the cache that are integers, and a user who determines what those cache keys are could pass one of those keys which would cause this code pathway to reference an arbitrary user. At its heart this is a high-risk login bypass vulnerability. However, there are a few additional conditions that must be met in order for this to be successfully executed, notably: 1.) The account referenced by the malicious cache key must have two-factor authentication enabled. An account without two-factor authentication would cause an exception to be triggered by the authentication logic, thusly exiting this authentication flow. 2.) Even if the malicious user is able to reference a valid cache key that references a valid user account with two-factor authentication, they must provide a valid two-factor authentication token. However, due to the design of this endpoint once a valid user account is found with two-factor authentication enabled there is no rate-limiting present, thusly allowing an attacker to brute force combinations until successful. This leads to a third condition that must be met: 3.) For the duration of this attack sequence the cache key being referenced must continue to exist with a valid `user_id` value. Depending on the specific key being used for this attack, this value may disappear quickly, or be changed by other random user interactions on the Panel, outside the control of the attacker. In order to mitigate this vulnerability the underlying authentication logic was changed to use an encrypted session store that the user is therefore unable to control the value of. This completely removed the use of a user-controlled value being used. In addition, the code was audited to ensure this type of vulnerability is not present elsewhere.	8.1	More Details
CVE-2021-40884	Projectsend version r1295 is affected by sensitive information disclosure. Because of not checking authorization in ids parameter in files-edit.php and id parameter in process.php function, a user with uploader role can download and edit all files of users in application.	8.1	More Details
CVE-2021-42135	HashiCorp Vault and Vault Enterprise 1.8.x through 1.8.4 may have an unexpected interaction between glob-related policies and the Google Cloud secrets engine. Users may, in some situations, have more privileges than intended, e.g., a user with read permission for the /gcp/roleset/* path may be able to issue Google Cloud service account credentials.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35067	Meross MSG100 devices before 3.2.3 allow an attacker to replay the same data or similar data (e.g., an attacker who sniffs a Close message can transmit an acceptable Open message).	8.1	More Details
CVE-2021-24019	An insufficient session expiration vulnerability [CWE- 613] in FortiClientEMS versions 6.4.2 and below, 6.2.8 and below may allow an attacker to reuse the unexpired admin user session IDs to gain admin privileges, should the attacker be able to obtain that session ID (via other, hypothetical attacks)	8.1	More Details
CVE-2021-27395	A vulnerability has been identified in SIMATIC Process Historian 2013 and earlier (All versions), SIMATIC Process Historian 2014 (All versions < SP3 Update 6), SIMATIC Process Historian 2019 (All versions), SIMATIC Process Historian 2020 (All versions). An interface in the software that is used for critical functionalities lacks authentication, which could allow a malicious user to maliciously insert, modify or delete data.	8.1	More Details
CVE-2021-35979	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication.	8.1	More Details
CVE-2021-29644	Hitachi JP1/IT Desktop Management 2 Agent 9 through 12 contains a remote code execution vulnerability because of an Integer Overflow. An attacker with network access to port 31016 may exploit this issue to execute code with unrestricted privileges on the underlying OS.	8.1	More Details
CVE-2021-25470	An improper caller check logic of SMC call in TEEGRIS secure OS prior to SMR Oct-2021 Release 1 can be used to compromise TEE.	7.9	More Details
CVE-2021-37969	Inappropriate implementation in Google Updater in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to perform local privilege escalation via a crafted file.	7.8	More Details
CVE-2021-0595	In lockAllProfileTasks of RootWindowContainer.java, there is a possible way to access the work profile without the profile PIN, after logging in. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-177457096	7.8	More Details
CVE-2021-0683	In runTraceIpcStop of ActivityManagerShellCommand.java, there is a possible deletion of system files due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-185398942	7.8	More Details
CVE-2021-28129	While working on Apache OpenOffice 4.1.8 a developer discovered that the DEB package did not install using root, but instead used a userid and groupid of 500. This both caused issues with desktop integration and could allow a crafted attack on files owned by that user or group if they exist. Users who installed the Apache OpenOffice 4.1.8 DEB packaging should upgrade to the latest version of Apache OpenOffice.	7.8	More Details
CVE-2021-0636	When extracting the incorrectly formatted avi file, the memory is damaged, the playback interface shows that the video cannot be played, and the log is found to be crashed. This problem may lead to hacker malicious code attacks, resulting in the loss of user rights.Product: Androidversion: Android-10Android ID: A-189392423	7.8	More Details
CVE-2021-42252	An issue was discovered in aspeed_lpc_ctrl_mmap in drivers/soc/aspeed/aspeed-lpc-ctrl.c in the Linux kernel before 5.14.6. Local attackers able to access the Aspeed LPC control interface could overwrite memory in the kernel and potentially execute privileges, aka CID-b49a0e69a7b1. This occurs because a certain comparison uses values that are not memory sizes.	7.8	More Details
CVE-2021-0635	When extracting the incorrectly formatted flv file, the memory is damaged, the playback interface shows that the video cannot be played, and the log is found to be crashed. This problem may lead to hacker malicious code attacks, resulting in the loss of user rights.Product: Androidversion:Android-10Android ID: A-189402477	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0684	In TouchInputMapper::sync of TouchInputMapper.cpp, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-179839665	7.8	More Details
CVE-2021-0685	In ParsedIntentInfo of ParsedIntentInfo.java, there is a possible parcel serialization/deserialization mismatch due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-191055353	7.8	More Details
CVE-2021-0692	In sendBroadcastToInstaller of FirstScreenBroadcast.java, there is a possible activity launch 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-11 Android-9 Android-10Android ID: A-179289753	7.8	More Details
CVE-2021-26557	When Octopus Tentacle is installed using a custom folder location, folder ACLs are not set correctly and could lead to an unprivileged user using DLL side-loading to gain privileged access.	7.8	More Details
CVE-2021-20264	An insecure modification flaw in the /etc/passwd file was found in the openjdk-1.8 and openjdk-11 containers. This flaw allows an attacker with access to the container to modify the /etc/passwd and escalate their privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2021-26556	When Octopus Server is installed using a custom folder location, folder ACLs are not set correctly and could lead to an unprivileged user using DLL side-loading to gain privileged access.	7.8	More Details
CVE-2021-28702	PCI devices with RMRRs not deassigned correctly Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR"). These are typically used for platform tasks such as legacy USB emulation. If such a device is passed through to a guest, then on guest shutdown the device is not properly deassigned. The IOMMU configuration for these devices which are not properly deassigned ends up pointing to a freed data structure, including the IO Pagetables. Subsequent DMA or interrupts from the device will have unpredictable behaviour, ranging from IOMMU faults to memory corruption.	7.6	More Details
CVE-2021-42054	ACCEL-PPP 1.12.0 has an out-of-bounds read in triton_context_schedule if the client exits after authentication.	7.5	More Details
CVE-2021-27665	An unauthenticated remote user could exploit a potential integer overflow condition in the exacqVision Server with a specially crafted script and cause denial-of-service condition.	7.5	More Details
CVE-2021-41546	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.14.1), RUGGEDCOM ROX RX1400 (All versions < V2.14.1), RUGGEDCOM ROX RX1500 (All versions < V2.14.1), RUGGEDCOM ROX RX1501 (All versions < V2.14.1), RUGGEDCOM ROX RX1510 (All versions < V2.14.1), RUGGEDCOM ROX RX1511 (All versions < V2.14.1), RUGGEDCOM ROX RX1512 (All versions < V2.14.1), RUGGEDCOM ROX RX1524 (All versions < V2.14.1), RUGGEDCOM ROX RX1536 (All versions < V2.14.1), RUGGEDCOM ROX RX5000 (All versions < V2.14.1). Affected devices write crashdumps without checking if enough space is available on the filesystem. Once the crashdump fills the entire root filesystem, affected devices fail to boot successfully. An attacker can leverage this vulnerability to cause a permanent Denial-of-Service.	7.5	More Details
CVE-2021-27002	NetApp Cloud Manager versions prior to 3.9.10 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to retrieve sensitive data via the web proxy.	7.5	More Details
CVE-2021-38181	SAP NetWeaver AS ABAP and ABAP Platform - versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38925	IBM Sterling B2B Integrator Standard Edition 5.2.0. 0 through 6.1.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210171.	7.5	More Details
CVE-2020-28145	Arbitrary file deletion vulnerability was discovered in wuzhicms v 4.0.1 via coreframe\app\attachment\admin\index.php, which allows attackers to access sensitive information.	7.5	More Details
CVE-2021-25634	LibreOffice supports digital signatures of ODF documents and macros within documents, presenting visual aids that no alteration of the document occurred since the last signing and that the signature is valid. An Improper Certificate Validation vulnerability in LibreOffice allowed an attacker to modify a digitally signed ODF document to insert an additional signing time timestamp which LibreOffice would incorrectly present as a valid signature signed at the bogus signing time. This issue affects: The Document Foundation LibreOffice 7-0 versions prior to 7.0.6; 7-1 versions prior to 7.1.2.	7.5	More Details
CVE-2021-24651	The Poll Maker WordPress plugin before 3.4.2 allows unauthenticated users to perform SQL injection via the ays_finish_poll AJAX action. While the result is not disclosed in the response, it is possible to use a timing attack to exfiltrate data such as password hash.	7.5	More Details
CVE-2021-41794	ogs_fqdn_parse in Open5GS 1.0.0 through 2.3.3 inappropriately trusts a client-supplied length value, leading to a buffer overflow. The attacker can send a PFCP Session Establishment Request with "internet" as the PDI Network Instance. The first character is interpreted as a length value to be used in a memcpy call. The destination buffer is only 100 bytes long on the stack. Then, 'i' gets interpreted as 105 bytes to copy from the source buffer to the destination buffer.	7.5	More Details
CVE-2021-41770	Ping Identity PingFederate before 10.3.1 mishandles pre-parsing validation, leading to an XXE attack that can achieve XML file disclosure.	7.5	More Details
CVE-2021-40500	SAP BusinessObjects Business Intelligence Platform (Crystal Reports) - versions 420, 430, allows an unauthenticated attacker to exploit missing XML validations at endpoints to read sensitive data. These endpoints are normally exposed over the network and successful exploitation can enable the attacker to retrieve arbitrary files from the server.	7.5	More Details
CVE-2021-40978	The mkdocs 1.2.2 built-in dev-server allows directory traversal using the port 8000, enabling remote exploitation to obtain :sensitive information. NOTE: the vendor has disputed this as described in https://github.com/mkdocs/mkdocs/issues/2601.] and https://github.com/nisdn/CVE-2021-40978/issues/1	7.5	More Details
CVE-2021-42040	An issue was discovered in MediaWiki through 1.36.2. A parser function related to loop control allowed for an infinite loop (and php-fpm hang) within the Loops extension because egLoopsCountLimit is mishandled. This could lead to memory exhaustion.	7.5	More Details
CVE-2021-38460	A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.	7.5	More Details
CVE-2021-41055	Gajim 1.2.x and 1.3.x before 1.3.3 allows remote attackers to cause a denial of service (crash) via a crafted XMPP Last Message Correction (XEP-0308) message in multi-user chat, where the message ID equals the correction ID.	7.5	More Details
CVE-2021-41799	MediaWiki before 1.36.2 allows a denial of service (resource consumption because of lengthy query processing time). ApiQueryBacklinks (action=query&list=backlinks) can cause a full table scan.	7.5	More Details
CVE-2021-38452	A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25633	LibreOffice supports digital signatures of ODF documents and macros within documents, presenting visual aids that no alteration of the document occurred since the last signing and that the signature is valid. An Improper Certificate Validation vulnerability in LibreOffice allowed an attacker to create a digitally signed ODF document, by manipulating the documentsignatures.xml or macrosignatures.xml stream within the document to combine multiple certificate data, which when opened caused LibreOffice to display a validly signed indicator but whose content was unrelated to the signature shown. This issue affects: The Document Foundation LibreOffice 7-0 versions prior to 7.0.6; 7-1 versions prior to 7.1.2.	7.5	More Details
CVE-2021-37199	A vulnerability has been identified in SINUMERIK 808D (All versions), SINUMERIK 828D (All versions < V4.95). Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.	7.5	More Details
CVE-2021-20584	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow a remote attacker to upload arbitrary files, caused by improper access controls. IBM X-Force ID: 199397.	7.5	More Details
CVE-2021-41920	webTareas version 2.4 and earlier allows an unauthenticated user to perform Time and Boolean-based blind SQL Injection on the endpoint /includes/library.php, via the sor_cible, sor_champs, and sor_ordre HTTP POST parameters. This allows an attacker to access all the data in the database and obtain access to the webTareas application.	7.5	More Details
CVE-2021-3321	Integer Underflow in Zephyr in IEEE 802154 Fragment Reassembly Header Removal. Zephyr versions >= >=2.4.0 contain Integer Overflow to Buffer Overflow (CWE-680). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-w44j-66g7-xw99	7.5	More Details
CVE-2021-41975	TadTools special page is vulnerable to authorization bypass, thus remote attackers can use the specific parameter to delete arbitrary files in the system without logging in.	7.5	More Details
CVE-2021-42095	Xshell before 7.0.0.76 allows attackers to cause a crash by triggering rapid changes to the title bar.	7.5	More Details
CVE-2021-42089	An issue was discovered in Zammad before 4.1.1. The REST API discloses sensitive information.	7.5	More Details
CVE-2021-38862	IBM Data Risk Manager (iDNA) 2.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 207980.	7.5	More Details
CVE-2021-33726	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to download arbitrary files under a user controlled path and does not correctly check if the relative path is still within the intended target directory.	7.5	More Details
CVE-2021-25485	Path traversal vulnerability in FactoryAirCommnadManger prior to SMR Oct-2021 Release 1 allows attackers to write file as system UID via BT remote socket.	7.5	More Details
CVE-2021-1594	A vulnerability in the REST API of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to perform a command injection attack and elevate privileges to root. This vulnerability is due to insufficient input validation for specific API endpoints. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting and modifying specific internode communications from one ISE persona to another ISE persona. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying operating system. To exploit this vulnerability, the attacker would need to decrypt HTTPS traffic between two ISE personas that are located on separate nodes.	7.5	More Details
CVE-2021-42260	TinyXML through 2.6.2 has an infinite loop in TiXmlParsingData::Stamp in tinyxmlparser.cpp via the TIXML_UTF_LEAD_0 case. It can be triggered by a crafted XML message and leads to a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41121	Vyper is a Pythonic Smart Contract Language for the EVM. In affected versions when performing a function call inside a literal struct, there is a memory corruption issue that occurs because of an incorrect pointer to the the top of the stack. This issue has been resolved in version 0.3.0.	7.5	More Details
CVE-2021-35496	The XMLA Connections component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for ActiveMatrix BPM, and TIBCO JasperReports Server for Microsoft Azure contains a difficult to exploit vulnerability that allows a low privileged attacker with network access to interfere with XML processing in the affected component. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 7.2.1 and below, TIBCO JasperReports Server: versions 7.5.0 and 7.5.1, TIBCO JasperReports Server: version 7.8.0, TIBCO JasperReports Server: version 7.9.0, TIBCO JasperReports Server - Community Edition: versions 7.8.0 and below, TIBCO JasperReports Server - Developer Edition: versions 7.9.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 7.9.0 and below, TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.9.0 and below, and TIBCO JasperReports Server for Microsoft Azure: version 7.8.0.	7.5	More Details
CVE-2021-41832	It is possible for an attacker to manipulate documents to appear to be signed by a trusted source. All versions of Apache OpenOffice up to 4.1.10 are affected. Users are advised to update to version 4.1.11. See CVE-2021-25635 for the LibreOffice advisory.	7.5	More Details
CVE-2021-41830	It is possible for an attacker to manipulate signed documents and macros to appear to come from a trusted source. All versions of Apache OpenOffice up to 4.1.10 are affected. Users are advised to update to version 4.1.11. See CVE-2021-25633 for the LibreOffice advisory.	7.5	More Details
CVE-2021-25492	Lack of boundary checking of a buffer in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows OOB read.	7.3	More Details
CVE-2021-25495	A possible heap buffer overflow vulnerability in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows arbitrary code execution.	7.3	More Details
CVE-2021-25487	Lack of boundary checking of a buffer in set_skb_priv() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read and it results in arbitrary code execution by dereference of invalid function pointer.	7.3	More Details
CVE-2021-0583	In onCreate of BluetoothPairingDialog, there is a possible way to enable Bluetooth without user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-182282956	7.3	More Details
CVE-2021-0598	In onCreate of ConfirmConnectActivity.java, there is a possible pairing of untrusted Bluetooth devices due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180422108	7.3	More Details
CVE-2021-25496	A possible buffer overflow vulnerability in maetd_dec_slice of libSPenBase library of Samsung Notes prior to Samsung Notes version 4.3.02.61 allows arbitrary code execution.	7.3	More Details
CVE-2021-25497	A possible buffer overflow vulnerability in maetd_cpy_slice of libSPenBase library of Samsung Notes prior to Samsung Notes version 4.3.02.61 allows arbitrary code execution.	7.3	More Details
CVE-2021-25498	A possible buffer overflow vulnerability in maetd_eco_cb_mode of libSPenBase library of Samsung Notes prior to Samsung Notes version 4.3.02.61 allows arbitrary code execution.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42093	An issue was discovered in Zammad before 4.1.1. An admin can execute code on the server via a crafted request that manipulates triggers.	7.2	More Details
CVE-2021-37732	A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) version(s): Aruba Instant 6.4.x.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x.x: 6.5.4.18 and below; Aruba Instant 8.5.x.x: 8.5.0.11 and below; Aruba Instant 8.6.x.x: 8.6.0.6 and below; Aruba Instant 8.7.x.x: 8.7.1.0 and below. Aruba has released patches for Aruba Instant (IAP) that address this security vulnerability.	7.2	More Details
CVE-2021-41947	A SQL injection vulnerability exists in Subrion CMS v4.2.1 in the visual-mode.	7.2	More Details
CVE-2021-33734	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2020-21654	emlog v6.0 contains a vulnerability in the component admin\template.php, which allows attackers to getshell via a crafted Zip file.	7.2	More Details
CVE-2021-33731	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-25479	A possible heap-based buffer overflow vulnerability in Exynos CP Chipset prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution.	7.2	More Details
CVE-2021-33728	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to upload JSON objects that are deserialized to JAVA objects. Due to insecure deserialization of user-supplied content by the affected software, a privileged attacker could exploit this vulnerability by sending a crafted serialized Java object. An exploit could allow the attacker to execute arbitrary code on the device with root privileges.	7.2	More Details
CVE-2021-33735	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-33736	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-33730	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-37727	A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) version(s): 6.4.x.x: 6.4.4.8-4.2.4.18 and below; Aruba Instant 6.5.x.x: 6.5.4.20 and below; Aruba Instant 8.5.x.x: 8.5.0.12 and below; Aruba Instant 8.6.x.x: 8.6.0.11 and below; Aruba Instant 8.7.x.x: 8.7.1.3 and below. Aruba has released patches for Aruba Instant (IAP) that address this security vulnerability.	7.2	More Details
CVE-2021-20122	The Telus Wi-Fi Hub (PRV65B444A-S-TS) with firmware version 3.00.20 is affected by an authenticated command injection vulnerability in multiple parameters passed to tr69_cmd.cgi. A remote attacker connected to the router's LAN and authenticated with a super user account, or using a bypass authentication vulnerability like CVE-2021-20090 could leverage this issue to run commands or gain a shell as root on the target device.	7.2	More Details
CVE-2021-25478	A possible stack-based buffer overflow vulnerability in Exynos CP Chipset prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37730	A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) version(s): Aruba Instant 6.4.x.x: 6.4.4.8-4.2.4.18 and below; Aruba Instant 6.5.x.x: 6.5.4.20 and below; Aruba Instant 8.5.x.x: 8.5.0.12 and below; Aruba Instant 8.6.x.x: 8.6.0.11 and below; Aruba Instant 8.7.x.x: 8.7.1.3 and below. Aruba has released patches for Aruba Instant (IAP) that address this security vulnerability.	7.2	More Details
CVE-2021-41126	October is a Content Management System (CMS) and web platform built on the the Laravel PHP Framework. In affected versions administrator accounts which had previously been deleted may still be able to sign in to the backend using October CMS v2.0. The issue has been patched in v2.1.12 of the october/october package. There are no workarounds for this issue and all users should update.	7.2	More Details
CVE-2021-40189	PHPFusion 9.03.110 is affected by a remote code execution vulnerability. The theme function will extract a file to "webroot/themes/{Theme Folder], where an attacker can access and execute arbitrary code.	7.2	More Details
CVE-2021-33732	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-40188	PHPFusion 9.03.110 is affected by an arbitrary file upload vulnerability. The File Manager function in admin panel does not filter all PHP extensions such as ".php, .php7, .phtml, .php5, ...". An attacker can upload a malicious file and execute code on the server.	7.2	More Details
CVE-2021-33733	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-42257	check_smart before 6.9.1 allows unintended drive access by an unprivileged user because it only checks for a substring match of a device path (the /dev/bus substring and a number), aka an unanchored regular expression.	7.1	More Details
CVE-2021-25499	Intent redirection vulnerability in SamsungAccountSDKSigninActivity of Galaxy Store prior to version 4.5.32.4 allows attacker to access content provider of Galaxy Store.	7.1	More Details
CVE-2021-3330	RCE/DOS: Linked-list corruption leading to large out-of-bounds write while sorting for forged fragment list in Zephyr. Zephyr versions >= >=2.4.0 contain Out-of-bounds Write (CWE-787). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fj4r-373f-9456	7.1	More Details
CVE-2021-29645	Hitachi JP1/IT Desktop Management 2 Agent 9 through 12 calls the SendMessageTimeoutW API with arbitrary arguments via a local pipe, leading to a local privilege escalation vulnerability. An attacker who exploits this issue could execute arbitrary code on the local system.	7.0	More Details
CVE-2021-0688	In lockNow of PhoneWindowManager.java, there is a possible lock screen bypass due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-161149543	7.0	More Details
CVE-2021-34788	A vulnerability in the shared library loading mechanism of Cisco AnyConnect Secure Mobility Client for Linux and Mac OS could allow an authenticated, local attacker to perform a shared library hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for shared library files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with root privileges. To exploit this vulnerability, the attacker must have a valid account on the system.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39184	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. A vulnerability in versions prior to 11.5.0, 12.1.0, and 13.3.0 allows a sandboxed renderer to request a "thumbnail" image of an arbitrary file on the user's system. The thumbnail can potentially include significant parts of the original file, including textual data in many cases. Versions 15.0.0-alpha.10, 14.0.0, 13.3.0, 12.1.0, and 11.5.0 all contain a fix for the vulnerability. Two workarounds aside from upgrading are available. One may make the vulnerability significantly more difficult for an attacker to exploit by enabling `contextIsolation` in one's app. One may also disable the functionality of the `createThumbnailFromPath` API if one does not need it.	6.8	More Details
CVE-2021-0691	In the SELinux policy configured in system_app.te, there is a possible way for system_app to gain code execution in other processes due to an overly-permissive SELinux policy. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-188554048	6.7	More Details
CVE-2021-25270	A local attacker could execute arbitrary code with administrator privileges in HitmanPro.Alert before version Build 901.	6.7	More Details
CVE-2021-25738	Loading specially-crafted yaml with the Kubernetes Java Client library can lead to code execution.	6.7	More Details
CVE-2021-3312	An XML external entity (XXE) vulnerability in Alkacon OpenCms 11.0, 11.0.1 and 11.0.2 allows remote authenticated users with edit privileges to exfiltrate files from the server's file system by uploading a crafted SVG document.	6.5	More Details
CVE-2021-3322	Unexpected Pointer Aliasing in IEEE 802154 Fragment Reassembly in Zephyr. Zephyr versions >= >=2.4.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-p86r-gc4r-4mq3	6.5	More Details
CVE-2021-38915	IBM Data Risk Manager 2.0.6 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 209947.	6.5	More Details
CVE-2021-23448	All versions of package config-handler are vulnerable to Prototype Pollution when loading config files.	6.5	More Details
CVE-2021-33723	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). An authenticated attacker could change the user profile of any user without proper authorization. With this, the attacker could change the password of any user in the affected system.	6.5	More Details
CVE-2021-33727	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). An authenticated attacker could download the user profile of any user. With this, the attacker could leak confidential information of any user in the affected system.	6.5	More Details
CVE-2021-32029	A flaw was found in postgresql. Using an UPDATE ... RETURNING command on a purpose-crafted table, an authenticated database user could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.	6.5	More Details
CVE-2020-4654	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow an authenticated user to obtain sensitive information due to improper permission control. IBM X-Force ID: 186090.	6.5	More Details
CVE-2021-42084	An issue was discovered in Zammad before 4.1.1. An attacker with valid agent credentials may send a series of crafted requests that cause an endless loop and thus cause denial of service.	6.5	More Details
CVE-2021-20473	IBM Sterling File Gateway User Interface 2.2.0.0 through 6.1.1.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 196944.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3671	A null pointer de-reference was found in the way samba kerberos server handled missing sname in TGS-REQ (Ticket Granting Server - Request). An authenticated user could use this flaw to crash the samba server.	6.5	More Details
CVE-2021-40439	Apache OpenOffice has a dependency on expat software. Versions prior to 2.1.0 were subject to CVE-2013-0340 a "Billion Laughs" entity expansion denial of service attack and exploit via crafted XML files. ODF files consist of a set of XML files. All versions of Apache OpenOffice up to 4.1.10 are subject to this issue. expat in version 4.1.11 is patched.	6.5	More Details
CVE-2021-39351	The WP Bannerize WordPress plugin is vulnerable to authenticated SQL injection via the id parameter found in the ~/Classes/wpBannerizeAdmin.php file which allows attackers to exfiltrate sensitive information from vulnerable sites. This issue affects versions 2.0.0 - 4.0.2.	6.5	More Details
CVE-2021-29006	rConfig 3.9.6 is affected by a Local File Disclosure vulnerability. An authenticated user may successfully download any file on the server.	6.5	More Details
CVE-2021-41865	HashiCorp Nomad and Nomad Enterprise 1.1.1 through 1.1.5 allowed authenticated users with job submission capabilities to cause denial of service by submitting incomplete job specifications with a Consul mesh gateway and host networking mode. Fixed in 1.1.6.	6.5	More Details
CVE-2021-0690	In ih264d_mark_err_slice_skip of ih264d_parse_pslice.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-182152757	6.5	More Details
CVE-2020-21658	A Cross-Site Request Forgery (CSRF) in WDJA CMS v1.5.2 allows attackers to arbitrarily add administrator accounts via a crafted URL.	6.5	More Details
CVE-2021-37976	Inappropriate implementation in Memory in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2021-40886	Projectsend version r1295 is affected by a directory traversal vulnerability. A user with Uploader role can add value `2` for `chunks` parameter to bypass `fileName` sanitization.	6.5	More Details
CVE-2021-37734	A remote unauthorized read access to files vulnerability was discovered in Aruba Instant version(s): 6.4.x.x: 6.4.4.8-4.2.4.18 and below; Aruba Instant 6.5.x.x: 6.5.4.19 and below; Aruba Instant 8.5.x.x: 8.5.0.12 and below; Aruba Instant 8.6.x.x: 8.6.0.11 and below; Aruba Instant 8.7.x.x: 8.7.1.3 and below; Aruba Instant 8.8.x.x: 8.8.0.0 and below. Aruba has released patches for Aruba Instant (IAP) that address this security vulnerability.	6.5	More Details
CVE-2021-32028	A flaw was found in postgresql. Using an INSERT ... ON CONFLICT ... DO UPDATE command on a purpose-crafted table, an authenticated database user could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.	6.5	More Details
CVE-2021-20375	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow an authenticated user to intercept and replace a message sent by another user due to improper access controls. IBM X-Force ID: 195567.	6.5	More Details
CVE-2021-21683	The file browser in Jenkins 2.314 and earlier, LTS 2.303.1 and earlier may interpret some paths to files as absolute on Windows, resulting in a path traversal vulnerability allowing attackers with Overall/Read permission (Windows controller) or Job/Workspace permission (Windows agents) to obtain the contents of arbitrary files.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34706	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access sensitive information or conduct a server-side request forgery (SSRF) attack through an affected device. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the web application to perform arbitrary HTTP requests on behalf of the attacker.	6.4	More Details
CVE-2021-41130	Extensible Service Proxy, a.k.a. ESP is a proxy which enables API management capabilities for JSON/REST or gRPC API services. ESPv1 can be configured to authenticate a JWT token. Its verified JWT claim is passed to the application by HTTP header "X-Endpoint-API-UserInfo", the application can use it to do authorization. But if there are two "X-Endpoint-API-UserInfo" headers from the client, ESPv1 only replaces the first one, the 2nd one will be passed to the application. An attacker can send two "X-Endpoint-API-UserInfo" headers, the second one with a fake JWT claim. Application may use the fake JWT claim to do the authorization. This impacts following ESPv1 usages: 1) Users have configured ESPv1 to do JWT authentication with Google ID Token as described in the referenced google endpoint document. 2) Users backend application is using the info in the "X-Endpoint-API-UserInfo" header to do the authorization. It has been fixed by v1.58.0. You need to patch it in the following ways: * If your docker image is using tag ":1", needs to re-start the container to pick up the new version. The tag ":1" will automatically point to the latest version. * If your docker image tag pings to a specific minor version, e.g. ":1.57". You need to update it to ":1.58" and re-start the container. There are no workaround for this issue.	6.4	More Details
CVE-2021-25481	An improper error handling in Exynos CP booting driver prior to SMR Oct-2021 Release 1 allows local attackers to bypass a Secure Memory Protector of Exynos CP Memory.	6.4	More Details
CVE-2021-24719	The Enfold Enfold WordPress theme before 4.8.4 was vulnerable to Reflected Cross-Site Scripting (XSS). The vulnerability is present on Enfold versions previous than 4.8.4 which use Avia Page Builder.	6.1	More Details
CVE-2021-38183	SAP NetWeaver - versions 700, 701, 702, 730, does not sufficiently encode user-controlled inputs, allowing an attacker to cause a potential victim to supply a malicious content to a vulnerable web application, which is then reflected to the victim and executed by the web browser, resulting in Cross-Site Scripting vulnerability.	6.1	More Details
CVE-2021-24563	The Frontend Uploader WordPress plugin through 1.3.2 does not prevent HTML files from being uploaded via its form, allowing unauthenticated user to upload a malicious HTML file containing JavaScript for example, which will be triggered when someone access the file directly	6.1	More Details
CVE-2021-40542	Opensis-Classic Version 8.0 is affected by cross-site scripting (XSS). An unauthenticated user can inject and execute JavaScript code through the link_url parameter in Ajax_url_encode.php.	6.1	More Details
CVE-2021-41798	MediaWiki before 1.36.2 allows XSS. Month related MediaWiki messages are not escaped before being used on the Special:Search results page.	6.1	More Details
CVE-2021-42134	The Unicorn framework before 0.36.1 for Django allows XSS via a component. NOTE: this issue exists because of an incomplete fix for CVE-2021-42053.	6.1	More Details
CVE-2021-40541	PHPFusion 9.03.110 is affected by cross-site scripting (XSS) in the preg patterns filter html tag without "//" in descript() function An authenticated user can trigger XSS by appending "//" in the end of text.	6.1	More Details
CVE-2021-41567	The new add subject parameter of Tad Uploader view book list function fails to filter special characters. Unauthenticated attackers can remotely inject JavaScript syntax and execute stored XSS attacks.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42112	The "File upload question" functionality in LimeSurvey 3.x-LTS through 3.27.18 allows XSS in assets/scripts/modaldialog.js and assets/scripts/uploader.js.	6.1	More Details
CVE-2021-35059	OpenWay WAY4 ACS before 1.2.278-2693 allows XSS via the /way4acs/enroll action parameter.	6.1	More Details
CVE-2021-20031	A Host Header Redirection vulnerability in SonicOS potentially allows a remote attacker to redirect firewall management users to arbitrary web domains.	6.1	More Details
CVE-2021-21684	Jenkins Git Plugin 4.8.2 and earlier does not escape the Git SHA-1 checksum parameters provided to commit notifications when displaying them in a build cause, resulting in a stored cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-42088	An issue was discovered in Zammad before 4.1.1. The Chat functionality allows XSS because clipboard data is mishandled.	6.1	More Details
CVE-2021-41565	TadTools special page parameter does not properly restrict the input of specific characters, thus remote attackers can inject JavaScript syntax without logging in, and further perform reflective XSS attacks.	6.1	More Details
CVE-2021-39350	The FV Flowplayer Video Player WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the player_id parameter found in the ~/view/stats.php file which allows attackers to inject arbitrary web scripts, in versions 7.5.0.727 - 7.5.2.727.	6.1	More Details
CVE-2021-41563	Tad Book3 editing book function does not filter special characters. Unauthenticated attackers can remotely inject JavaScript syntax and execute stored XSS attacks.	6.1	More Details
CVE-2021-42043	An issue was discovered in Special:MediaSearch in the MediaSearch extension in MediaWiki through 1.36.2. The suggestion text (a parameter to mediasearch-did-you-mean) was not being properly sanitized and allowed for the injection and execution of HTML and JavaScript via the intitle: search operator within the query.	6.1	More Details
CVE-2021-36150	SilverStripe Framework through 4.8.1 allows XSS.	6.1	More Details
CVE-2021-20481	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 197503.	6.1	More Details
CVE-2021-20561	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199230.	6.1	More Details
CVE-2021-42041	An issue was discovered in CentralAuth in MediaWiki through 1.36.2. The rightsnone MediaWiki message was not being properly sanitized and allowed for the injection and execution of HTML and JavaScript via the setchange log.	6.1	More Details
CVE-2021-34742	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25469	A possible stack-based buffer overflow vulnerability in Widevine trustlet prior to SMR Oct-2021 Release 1 allows arbitrary code execution.	6.0	More Details
CVE-2021-25490	A keyblob downgrade attack in keymaster prior to SMR Oct-2021 Release 1 allows attacker to trigger IV reuse vulnerability with privileged process.	6.0	More Details
CVE-2021-25271	A local attacker could read or write arbitrary files with administrator privileges in HitmanPro before version Build 318.	6.0	More Details
CVE-2021-25482	SQL injection vulnerabilities in CMFA framework prior to SMR Oct-2021 Release 1 allow untrusted application to overwrite some CMFA framework information.	5.9	More Details
CVE-2021-20600	Uncontrolled resource consumption in Mitsubishi Electric MELSEC iQ-R series C Controller Module R12CCPU-V Firmware Versions "16" and prior allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending a large number of packets in a short time while the module starting up. System reset is required for recovery.	5.9	More Details
CVE-2021-1534	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.	5.8	More Details
CVE-2021-35494	The Rest API component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for ActiveMatrix BPM, and TIBCO JasperReports Server for Microsoft Azure contain a race condition that allows a low privileged authenticated attacker via the REST API to obtain read access to temporary objects created by other users on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 7.2.1 and below, TIBCO JasperReports Server: versions 7.5.0 and 7.5.1, TIBCO JasperReports Server: version 7.8.0, TIBCO JasperReports Server: version 7.9.0, TIBCO JasperReports Server - Community Edition: versions 7.8.0 and below, TIBCO JasperReports Server - Developer Edition: versions 7.9.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 7.9.0 and below, TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.9.0 and below, and TIBCO JasperReports Server for Microsoft Azure: version 7.8.0.	5.7	More Details
CVE-2021-41125	Scrapy is a high-level web crawling and scraping framework for Python. If you use `HttpAuthMiddleware` (i.e. the `http_user` and `http_pass` spider attributes) for HTTP authentication, all requests will expose your credentials to the request target. This includes requests generated by Scrapy components, such as `robots.txt` requests sent by Scrapy when the `ROBOTSTXT_OBEY` setting is set to `True`, or as requests reached through redirects. Upgrade to Scrapy 2.5.1 and use the new `http_auth_domain` spider attribute to control which domains are allowed to receive the configured HTTP authentication credentials. If you are using Scrapy 1.8 or a lower version, and upgrading to Scrapy 2.5.1 is not an option, you may upgrade to Scrapy 1.8.1 instead. If you cannot upgrade, set your HTTP authentication credentials on a per-request basis, using for example the `w3lib.http.basic_auth_header` function to convert your credentials into a value that you can assign to the `Authorization` header of your request, instead of defining your credentials globally using `HttpAuthMiddleware`.	5.7	More Details
CVE-2021-0681	In system properties, there is a possible information disclosure 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 SoCAndroid ID: A-192535337	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22263	An issue has been discovered in GitLab affecting all versions starting from 13.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. A user account with 'external' status which is granted 'Maintainer' role on any project on the GitLab instance where 'project tokens' are allowed may elevate its privilege to 'Internal' and access Internal projects.	5.5	More Details
CVE-2021-33602	A vulnerability affecting the F-Secure Antivirus engine was discovered when the engine tries to unpack a zip archive (LZW decompression method), and this can crash the scanning engine. The vulnerability can be exploited remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine.	5.5	More Details
CVE-2021-0695	In get_sock_stat of xt_qtaguid.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-184018316References: Upstream kernel	5.5	More Details
CVE-2021-0693	In openFile of HeapDumpProvider.java, there is a possible way to retrieve generated heap dumps from debuggable apps due to an unprotected provider. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-184046948	5.5	More Details
CVE-2021-40832	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine.	5.5	More Details
CVE-2020-22679	Memory leak in the sgpd_parse_entry function in MP4Box in gpac 0.8.0 allows attackers to cause a denial of service (DoS) via a crafted input.	5.5	More Details
CVE-2021-40498	A vulnerability has been identified in SAP SuccessFactors Mobile Application for Android - versions older than 2108, which allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service, which can lead to denial of service. The vulnerability is related to Android implementation methods that are widely used across Android mobile applications, and such methods are embedded into the SAP SuccessFactors mobile application. These Android methods begin executing once the user accesses their profile on the mobile application. While executing, it can also pick up the activities from other Android applications that are running in the background of the users device and are using the same types of methods in the application. Such vulnerability can also lead to phishing attacks that can be used for staging other types of attacks.	5.5	More Details
CVE-2021-0689	In RGB_to_BGR1_portable of SkSwizzler_opts.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-190188264	5.5	More Details
CVE-2021-25488	Lack of boundary checking of a buffer in recv_data() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read.	5.5	More Details
CVE-2021-33603	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine.	5.5	More Details
CVE-2021-0682	In sendAccessibilityEvent of NotificationManagerService.java, there is a possible disclosure of notification data due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-159624555	5.5	More Details
CVE-2020-22675	An issue was discovered in gpac 0.8.0. The GetGhostNum function in stbl_read.c has a heap-based buffer overflow which can lead to a denial of service (DOS) via a crafted input.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0686	In getDefaultSmsPackage of RoleManagerService.java, there is a possible way to get information about the default sms app of a different device user 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-11 Android-10Android ID: A-177927831	5.5	More Details
CVE-2020-22673	Memory leak in the senc_Parse function in MP4Box in gpac 0.8.0 allows attackers to cause a denial of service (DoS) via a crafted input.	5.5	More Details
CVE-2021-0644	In conditionallyRemoveIdentifiers of SubscriptionController.java, there is a possible way to retrieve a trackable identifier due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-181053462	5.5	More Details
CVE-2021-3848	An arbitrary file creation by privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1, and Worry-Free Business Security Services could allow a local attacker to create an arbitrary file with higher privileges that could lead to a denial-of-service (DoS) on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	5.5	More Details
CVE-2020-22678	An issue was discovered in gpac 0.8.0. The gf_media_nalu_remove_emulation_bytes function in av_parsers.c has a heap-based buffer overflow which can lead to a denial of service (DOS) via a crafted input.	5.5	More Details
CVE-2020-22674	An issue was discovered in gpac 0.8.0. An invalid memory dereference exists in the function FixTrackID located in isom_intern.c, which allows attackers to cause a denial of service (DoS) via a crafted input.	5.5	More Details
CVE-2021-0680	In system properties, there is a possible information disclosure 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 SoCAndroid ID: A-192535676	5.5	More Details
CVE-2021-34711	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system.	5.5	More Details
CVE-2021-29906	IBM App Connect Enterprise Certified Container 1.0, 1.1, 1.2, 1.3, 1.4 and 1.5 could disclose sensitive information to a local user when it is configured to use an IBM Cloud API key to connect to cloud-based connectors. IBM X-Force ID: 207630.	5.5	More Details
CVE-2020-22677	An issue was discovered in gpac 0.8.0. The dump_data_hex function in box_dump.c has a heap-based buffer overflow which can lead to a denial of service (DOS) via a crafted input.	5.5	More Details
CVE-2021-34766	A vulnerability in the web UI of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to elevate privileges and create, read, update, or delete records and settings in multiple functions. This vulnerability is due to insufficient authorization of the System User and System Operator role capabilities. An attacker could exploit this vulnerability by directly accessing a web resource. A successful exploit could allow the attacker to create, read, update, or delete records and settings in multiple functions without the necessary permissions on the web UI.	5.4	More Details
CVE-2021-24545	The WP HTML Author Bio WordPress plugin through 1.2.0 does not sanitise the HTML allowed in the Bio of users, allowing them to use malicious JavaScript code, which will be executed when anyone visit a post in the frontend made by such user. As a result, user with a role as low as author could perform Cross-Site Scripting attacks against users, which could potentially lead to privilege escalation when an admin view the related post/s.	5.4	More Details
CVE-2021-24712	The Appointment Hour Booking WordPress plugin before 1.3.17 does not properly sanitize values used when creating new calendars.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24683	The Weather Effect WordPress plugin before 1.3.4 does not have any CSRF checks in place when saving its settings, and do not validate or escape them, which could lead to Stored Cross-Site Scripting issue.	5.4	More Details
CVE-2020-21656	XYHCMS v3.6 contains a stored cross-site scripting (XSS) vulnerability in the component xyhai.php?s=/Link/index.	5.4	More Details
CVE-2021-24577	The Coming soon and Maintenance mode WordPress plugin before 3.5.3 does not properly sanitize inputs submitted by authenticated users when setting adding or modifying coming soon or maintenance mode pages, leading to stored XSS.	5.4	More Details
CVE-2021-24690	The Chained Quiz WordPress plugin before 1.2.7.2 does not properly sanitize or escape inputs in the plugin's settings.	5.4	More Details
CVE-2021-24720	The GeoDirectory Business Directory WordPress plugin before 2.1.1.3 was vulnerable to Authenticated Stored Cross-Site Scripting (XSS).	5.4	More Details
CVE-2021-24576	The Easy Accordion WordPress plugin before 2.0.22 does not properly sanitize inputs when adding new items to an accordion.	5.4	More Details
CVE-2020-15941	A path traversal vulnerability [CWE-22] in FortiClientEMS versions 6.4.1 and below; 6.2.8 and below may allow an authenticated attacker to inject directory traversal character sequences to add/delete the files of the server via the name parameter of Deployment Packages.	5.4	More Details
CVE-2021-40292	A Stored Cross Site Sripting (XSS) vulnerability exists in DzzOffice 2.02.1 via the settingnew parameter.	5.4	More Details
CVE-2021-23447	This affects the package teddy before 0.5.9. A type confusion vulnerability can be used to bypass input sanitization when the model content is an array (instead of a string).	5.4	More Details
CVE-2021-41917	webTareas version 2.4 and earlier allows an authenticated user to store arbitrary web script or HTML by creating or editing a client name in the clients section, due to incorrect sanitization of user-supplied data and achieve a Stored Cross-Site Scripting attack against the platform users and administrators. The affected endpoint is /clients/editclient.php, on the HTTP POST cn parameter.	5.4	More Details
CVE-2021-41918	webTareas version 2.4 and earlier allows an authenticated user to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Reflected Cross-Site Scripting attack against the platform users and administrators. The issue affects every endpoint on the application because it is related on how each URL is echoed back on every response page.	5.4	More Details
CVE-2020-21729	JEECMS x1.1 contains a stored cross-site scripting (XSS) vulnerability in the component of /member-vipcenter.htm, which allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2021-42085	An issue was discovered in Zammad before 4.1.1. There is stored XSS via a custom Avatar.	5.4	More Details
CVE-2021-42092	An issue was discovered in Zammad before 4.1.1. Stored XSS may occur via an Article during addition of an attachment to a Ticket.	5.4	More Details
CVE-2021-20571	IBM Sterling B2B Integrator 5.2.0.0 through 6.1.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199246.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37958	Inappropriate implementation in Navigation in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.	5.4	More Details
CVE-2021-29855	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 205684.	5.4	More Details
CVE-2021-40888	Projectsend version r1295 is affected by Cross Site Scripting (XSS) due to lack of sanitization when echo output data in returnFilesIds() function. A low privilege user can call this function through process.php file and execute scripting code.	5.4	More Details
CVE-2021-40191	Dzzoffice Version 2.02.1 is affected by cross-site scripting (XSS) due to a lack of sanitization of input data at all upload functions in webroot/dzz/attach/Uploader.class.php and return a wrong response in content-type of output data in webroot/dzz/attach/controller.php.	5.4	More Details
CVE-2021-3834	Integria IMS in its 5.0.92 version does not filter correctly some fields related to the login.php file. An attacker could exploit this vulnerability in order to perform a cross-site scripting attack (XSS).	5.4	More Details
CVE-2021-29764	IBM Sterling B2B Integrator 5.2.0.0 through 6.1.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 202268.	5.4	More Details
CVE-2021-29836	IBM Sterling B2B Integrator Standard Edition 5.2.0.0. through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204912.	5.4	More Details
CVE-2021-42053	The Unicorn framework through 0.35.3 for Django allows XSS via component.name.	5.4	More Details
CVE-2021-37735	A remote denial of service vulnerability was discovered in Aruba Instant version(s): Aruba Instant 6.5.x.x: 6.5.4.18 and below; Aruba Instant 8.5.x.x: 8.5.0.10 and below; Aruba Instant 8.6.x.x: 8.6.0.4 and below. Aruba has released patches for Aruba Instant (IAP) that address this security vulnerability.	5.3	More Details
CVE-2020-19003	An issue in Gate One 1.2.0 allows attackers to bypass to the verification check done by the origins list and connect to Gate One instances used by hosts not on the origins list.	5.3	More Details
CVE-2021-42326	Redmine before 4.1.5 and 4.2.x before 4.2.3 may disclose the names of users on activity views due to an insufficient access filter.	5.3	More Details
CVE-2021-40497	SAP BusinessObjects Analysis (edition for OLAP) - versions 420, 430, allows an attacker to exploit certain application endpoints to read sensitive data. These endpoints are normally exposed over the network and successful exploitation could lead to exposure of some system specific data like its version.	5.3	More Details
CVE-2021-40495	There are multiple Denial-of Service vulnerabilities in SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755. An unauthorized attacker can use the public SICF service /sap/public/bc/abap to reduce the performance of SAP NetWeaver Application Server ABAP and ABAP Platform.	5.3	More Details
CVE-2021-41825	Verint Workforce Optimization (WFO) 15.2.5.1033 allows HTML injection via the /wfo/control/signin username parameter.	5.3	More Details
CVE-2021-25467	Assuming system privilege is gained, possible buffer overflow vulnerabilities in the Vision DSP kernel driver prior to SMR Oct-2021 Release 1 allows privilege escalation to Root by hijacking loaded library.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41568	Tad Web is vulnerable to authorization bypass, thus remote attackers can exploit the vulnerability to use the original function of viewing bulletin boards and uploading files in the system.	5.3	More Details
CVE-2021-42137	An issue was discovered in Zammad before 5.0.1. In some cases, there is improper enforcement of the privilege requirement for viewing a list of tickets that shows title, state, etc.	5.3	More Details
CVE-2021-37922	Zoho ManageEngine ADManager Plus version 7110 and prior is vulnerable to path traversal which allows copying of files from one directory to another.	5.3	More Details
CVE-2021-41564	Tad Honor viewing book list function is vulnerable to authorization bypass, thus remote attackers can use special parameters to delete articles arbitrarily without logging in.	5.3	More Details
CVE-2021-41976	Tad Uploader edit book list function is vulnerable to authorization bypass, thus remote attackers can use the function to amend the folder names in the book list without logging in.	5.3	More Details
CVE-2021-41800	MediaWiki before 1.36.2 allows a denial of service (resource consumption because of lengthy query processing time). Visiting Special:Contributions can sometimes result in a long running SQL query because PoolCounter protection is mishandled.	5.3	More Details
CVE-2021-41831	It is possible for an attacker to manipulate the timestamp of signed documents. All versions of Apache OpenOffice up to 4.1.10 are affected. Users are advised to update to version 4.1.11. See CVE-2021-25634 for the LibreOffice advisory.	5.3	More Details
CVE-2021-35060	/way4acs/enroll in OpenWay WAY4 ACS before 1.2.278-2693 allows unauthenticated attackers to leverage response differences to discover whether a specific payment card number is stored in the system.	5.3	More Details
CVE-2021-0687	In ellipsize of Layout.java, there is a possible ANR due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-188913943	5.0	More Details
CVE-2021-34757	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory.	4.9	More Details
CVE-2021-42087	An issue was discovered in Zammad before 4.1.1. An admin can discover the application secret via the API.	4.9	More Details
CVE-2021-34744	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory.	4.9	More Details
CVE-2021-33722	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system has a Path Traversal vulnerability when exporting a firmware container. With this a privileged authenticated attacker could create arbitrary files on an affected system.	4.9	More Details
CVE-2021-38179	Debug function of Admin UI of SAP Business One Integration is enabled by default. This allows Admin User to see the captured packet contents which may include User credentials.	4.9	More Details
CVE-2021-24656	The Simple Social Media Share Buttons WordPress plugin before 3.2.4 does not escape the Share Title settings before outputting it in the frontend pages or posts (depending on the settings used), allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42044	An issue was discovered in the Mentor dashboard in the GrowthExperiments extension in MediaWiki through 1.36.2. The Growthexperiments-mentor-dashboard-mentee-overview-add-filter-total-edits-headline, growthexperiments-mentor-dashboard-mentee-overview-add-filter-starred-headline, growthexperiments-mentor-dashboard-mentee-overview-info-text, growthexperiments-mentor-dashboard-mentee-overview-info-legend-headline, and growthexperiments-mentor-dashboard-mentee-overview-active-ago MediaWiki messages were not being properly sanitized and allowed for the injection and execution of HTML and JavaScript.	4.8	More Details
CVE-2021-35214	The vulnerability in SolarWinds Pingdom can be described as a failure to invalidate user session upon password or email address change. When running multiple active sessions in separate browser windows, it was observed a password or email address change could be changed without terminating the user session. This issue has been resolved on September 13, 2021.	4.8	More Details
CVE-2021-24681	The Duplicate Page WordPress plugin through 4.4.2 does not sanitise or escape the Duplicate Post Suffix settings before outputting it, which could allow high privilege users to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24691	The Quiz And Survey Master WordPress plugin before 7.3.2 does not escape the Quiz Url Slug setting before outputting it in some pages, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24709	The Weather Effect WordPress plugin before 1.3.6 does not properly validate and escape some of its settings (like *_size_leaf, *_flakes_leaf, *_speed) which could lead to Stored Cross-Site Scripting issues	4.8	More Details
CVE-2021-24737	The Comments – wpDiscuz WordPress plugin through 7.3.0 does not properly sanitise or escape the Follow and Unfollow messages before outputting them in the page, which could allow high privilege users to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-42042	An issue was discovered in SpecialEditGrowthConfig in the GrowthExperiments extension in MediaWiki through 1.36.2. The growthexperiments-edit-config-error-invalid-title MediaWiki message was not being properly sanitized and allowed for the injection and execution of HTML and JavaScript.	4.8	More Details
CVE-2021-27003	Clustered Data ONTAP versions prior to 9.5P18, 9.6P15, 9.7P14, 9.8P5 and 9.9.1 are missing an X-Frame-Options header which could allow a clickjacking attack.	4.7	More Details
CVE-2021-34772	A vulnerability in the web-based management interface of Cisco Orbital could allow an unauthenticated, remote attacker to redirect users to a malicious webpage. This vulnerability is due to improper validation of URL paths in the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted URL. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability, known as an open redirect attack, is used in phishing attacks to persuade users to visit malicious sites.	4.7	More Details
CVE-2021-25480	A lack of replay attack protection in GUTI REALLOCATION COMMAND message process in Qualcomm modem prior to SMR Oct-2021 Release 1 can lead to remote denial of service on mobile network connection.	4.4	More Details
CVE-2021-25477	An improper error handling in Mediatek RRC Protocol stack prior to SMR Oct-2021 Release 1 allows modem crash and remote denial of service.	4.4	More Details
CVE-2021-34758	A vulnerability in the memory management of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an authenticated, local attacker to corrupt a shared memory segment, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient access controls to a shared memory resource. An attacker could exploit this vulnerability by corrupting a shared memory segment on an affected device. A successful exploit could allow the attacker to cause the device to reload. The device will recover from the corruption upon reboot.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25474	Assuming a shell privilege is gained, an improper exception handling for multi_sim_bar_show_on_qspanel value in SystemUI prior to SMR Oct-2021 Release 1 allows an attacker to cause a permanent denial of service in user device before factory reset.	4.4	More Details
CVE-2021-25473	Assuming a shell privilege is gained, an improper exception handling for multi_sim_bar_hide_by_meadia_full value in SystemUI prior to SMR Oct-2021 Release 1 allows an attacker to cause a permanent denial of service in user device before factory reset.	4.4	More Details
CVE-2021-25468	A possible guessing and confirming a byte memory vulnerability in Widevine trustlet prior to SMR Oct-2021 Release 1 allows attackers to read arbitrary memory address.	4.4	More Details
CVE-2021-37966	Inappropriate implementation in Compositing in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2021-29700	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authneticated attacker to obtain sensitive information from configuration files that could aid in further attacks against the system. IBM X-Force ID: 200656.	4.3	More Details
CVE-2021-40496	SAP Internet Communication framework (ICM) - versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 785, allows an attacker with logon functionality, to exploit the authentication function by using POST and form field to repeat executions of the initial command by a GET request and exposing sensitive data. This vulnerability is normally exposed over the network and successful exploitation can lead to exposure of data like system details.	4.3	More Details
CVE-2021-28661	Default SilverStripe GraphQL Server (aka silverstripe/graphql) 3.x through 3.4.1 permission checker not inherited by query subclass.	4.3	More Details
CVE-2021-24021	An improper neutralization of input vulnerability [CWE-79] in FortiAnalyzer versions 6.4.3 and below, 6.2.7 and below and 6.0.10 and below may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the column settings of Logview in FortiAnalyzer, should the attacker be able to obtain that POST request, via other, hypothetical attacks.	4.3	More Details
CVE-2021-41115	Zulip is an open source team chat server. In affected versions Zulip allows organization administrators on a server to configure "linkifiers" that automatically create links from messages that users send, detected via arbitrary regular expressions. Malicious organization administrators could subject the server to a denial-of-service via regular expression complexity attacks; most simply, by configuring a quadratic-time regular expression in a linkifier, and sending messages that exploited it. A regular expression attempted to parse the user-provided regexes to verify that they were safe from ReDoS -- this was both insufficient, as well as _itself_ subject to ReDoS if the organization administrator entered a sufficiently complex invalid regex. Affected users should [upgrade to the just-released Zulip 4.7](https://zulip.readthedocs.io/en/latest/production/upgrade-or-modify.html#upgrading-to-a-release), or [`main`](https://zulip.readthedocs.io/en/latest/production/upgrade-or-modify.html#upgrading-from-a-git-repository).	4.3	More Details
CVE-2021-30630	Inappropriate implementation in Blink in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-37971	Incorrect security UI in Web Browser UI in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2021-20552	IBM Sterling File Gateway 6.0.0.0 through 6.1.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199170.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37963	Side-channel information leakage in DevTools in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to bypass site isolation via a crafted HTML page.	4.3	More Details
CVE-2021-36178	A insufficiently protected credentials in Fortinet FortiSDNConnector version 1.1.7 and below allows attacker to disclose third-party devices credential information via configuration page lookup.	4.3	More Details
CVE-2021-20372	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow a remote authenticated user to cause a denial of another user's service due to insufficient permission checking. IBM X-Force ID: 195518.	4.3	More Details
CVE-2021-20376	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow an authenticated attacker to enumerate usernames due to there being an observable discrepancy in returned messages. IBM X-Force ID: 195568.	4.3	More Details
CVE-2021-37968	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-37967	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-37965	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-34777	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.	4.3	More Details
CVE-2021-29761	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authenticated user to obtain sensitive information from the dashboard that they should not have access to. IBM X-Force ID: 202265.	4.3	More Details
CVE-2021-34779	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.	4.3	More Details
CVE-2021-42009	An authenticated Apache Traffic Control Traffic Ops user with Portal-level privileges can send a request with a specially-crafted email subject to the /deliveryservices/request Traffic Ops endpoint to send an email, from the Traffic Ops server, with an arbitrary body to an arbitrary email address. Apache Traffic Control 5.1.x users should upgrade to 5.1.3 or 6.0.0. 4.1.x users should upgrade to 5.1.3.	4.3	More Details
CVE-2021-34702	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information. This vulnerability is due to improper enforcement of administrator privilege levels for low-value sensitive data. An attacker with read-only administrator access to the web-based management interface could exploit this vulnerability by browsing to the page that contains the sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34782	A vulnerability in the API endpoints for Cisco DNA Center could allow an authenticated, remote attacker to gain access to sensitive information that should be restricted. The attacker must have valid device credentials. This vulnerability is due to improper access controls on API endpoints. An attacker could exploit the vulnerability by sending a specific API request to an affected application. A successful exploit could allow the attacker to obtain sensitive information about other users who are configured with higher privileges on the application.	4.3	More Details
CVE-2021-21682	Jenkins 2.314 and earlier, LTS 2.303.1 and earlier accepts names of jobs and other entities with a trailing dot character, potentially replacing the configuration and data of other entities on Windows.	4.3	More Details
CVE-2021-34780	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.	4.3	More Details
CVE-2021-34776	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.	4.3	More Details
CVE-2021-29760	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authenticated user to download unauthorized files through the dashboard user interface. IBM X-Force ID: 202213.	4.3	More Details
CVE-2021-34778	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.	4.3	More Details
CVE-2021-34775	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities.	4.3	More Details
CVE-2021-29758	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authenticated user to perform actions that they should not be able to access due to improper access controls. IBM X-Force ID: 202169.	4.3	More Details
CVE-2021-36175	An improper neutralization of input vulnerability [CWE-79] in FortiWebManager versions 6.2.3 and below, 6.0.2 and below may allow a remote authenticated attacker to inject malicious script/tags via the name/description/comments parameter of various sections of the device.	4.1	More Details
CVE-2021-25476	An information disclosure vulnerability in Widevine TA log prior to SMR Oct-2021 Release 1 allows attackers to bypass the ASLR protection mechanism in TEE.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20121	The Telus Wi-Fi Hub (PRV65B444A-S-TS) with firmware version 3.00.20 is vulnerable to an authenticated arbitrary file read. An authenticated user with physical access to the device can read arbitrary files from the device by preparing and connecting a specially prepared USB drive to the device, and making a series of crafted requests to the device's web interface.	4.0	More Details
CVE-2021-25494	A possible buffer overflow vulnerability in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows arbitrary code execution.	4.0	More Details
CVE-2021-25493	Lack of boundary checking of a buffer in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows OOB read	4.0	More Details
CVE-2021-25484	Improper authentication in InputManagerService prior to SMR Oct-2021 Release 1 allows monitoring the touch event.	4.0	More Details
CVE-2021-25483	Lack of boundary checking of a buffer in livfivextractor library prior to SMR Oct-2021 Release 1 allows OOB read.	4.0	More Details
CVE-2021-25472	An improper access control vulnerability in BluetoothSettingsProvider prior to SMR Oct-2021 Release 1 allows untrusted application to overwrite some Bluetooth information.	4.0	More Details
CVE-2021-25475	A possible heap-based buffer overflow vulnerability in DSP kernel driver prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution.	3.9	More Details
CVE-2021-41136	Puma is a HTTP 1.1 server for Ruby/Rack applications. Prior to versions 5.5.1 and 4.3.9, using `puma` with a proxy which forwards HTTP header values which contain the LF character could allow HTTP request smugggling. A client could smuggle a request through a proxy, causing the proxy to send a response back to another unknown client. The only proxy which has this behavior, as far as the Puma team is aware of, is Apache Traffic Server. If the proxy uses persistent connections and the client adds another request in via HTTP pipelining, the proxy may mistake it as the first request's body. Puma, however, would see it as two requests, and when processing the second request, send back a response that the proxy does not expect. If the proxy has reused the persistent connection to Puma to send another request for a different client, the second response from the first client will be sent to the second client. This vulnerability was patched in Puma 5.5.1 and 4.3.9. As a workaround, do not use Apache Traffic Server with `puma`.	3.7	More Details
CVE-2021-25471	A lack of replay attack protection in Security Mode Command process prior to SMR Oct-2021 Release 1 can lead to denial of service on mobile network connection and battery depletion.	3.7	More Details
CVE-2021-37964	Inappropriate implementation in ChromeOS Networking in Google Chrome on ChromeOS prior to 94.0.4606.54 allowed an attacker with a rogue wireless access point to to potentially carryout a wifi impersonation attack via a crafted ONC file.	3.3	More Details
CVE-2021-25489	Assuming radio permission is gained, missing input validation in modem interface driver prior to SMR Oct-2021 Release 1 results in format string bug leading to kernel panic.	3.3	More Details
CVE-2021-36170	An information disclosure vulnerability [CWE-200] in FortiAnalyzerVM and FortiManagerVM versions 7.0.0 and 6.4.6 and below may allow an authenticated attacker to read the FortiCloud credentials which were used to activate the trial license in cleartext.	3.2	More Details
CVE-2021-41802	HashiCorp Vault and Vault Enterprise through 1.7.4 and 1.8.3 allowed a user with write permission to an entity alias ID sharing a mount accessor with another user to acquire this other user’s policies by merging their identities. Fixed in Vault and Vault Enterprise 1.7.5 and 1.8.4.	2.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25486	Exposure of information vulnerability in ipcdump prior to SMR Oct-2021 Release 1 allows an attacker detect device information via analyzing packet in log.	2.5	More Details
CVE-2021-25491	A vulnerability in mfc driver prior to SMR Oct-2021 Release 1 allows memory corruption via NULL-pointer dereference.	2.3	More Details
CVE-2021-40725	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm listbox that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	N/A	More Details
CVE-2021-20604	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-2021-20605	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-2021-20602	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-2021-40726	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm field that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	N/A	More Details
CVE-2021-41796	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: non	N/A	More Details
CVE-2021-41797	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: non	N/A	More Details
CVE-2021-41070	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: non	N/A	More Details
CVE-2021-41071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-20603	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