SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 June 2022

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-40212	An exploitable out-of-bounds write vulnerability in PotPlayer 1.7.21523 build 210729 may lead to code execution, information disclosure, and denial of service.	9.8	More Details
CVE-2022-31874	ASUS RT-N53 3.0.0.4.376.3754 has a command injection vulnerability in the SystemCmd parameter of the apply.cgi interface.	9.8	More Details
CVE-2022-30329	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. An OS injection vulnerability exists within the web interface, allowing an attacker with valid credentials to execute arbitrary shell commands.	9.8	More Details
CVE-2021-41408	VoIPmonitor WEB GUI up to version 24.61 is affected by SQL injection through the "api.php" file and "user" parameter.	9.8	More Details
CVE-2021-45024	ASG technologies (A Rocket Software Company) ASG-Zena Cross Platform Server Enterprise Edition 4.2.1 is vulnerable to XML External Entity (XXE).	9.8	More Details
CVE-2022-31296	Online Discussion Forum Site 1 was discovered to contain a blind SQL injection vulnerability via the component /odfs/posts/view_post.php.	9.8	More Details
CVE-2022-31784	A vulnerability in the management interface of MiVoice Business through 9.3 PR1 and MiVoice Business Express through 8.0 SP3 PR3 could allow an unauthenticated attacker (that has network access to the management interface) to conduct a buffer overflow attack due to insufficient validation of URL parameters. A successful exploit could allow arbitrary code execution.	9.8	More Details
CVE-2021-40903	A vulnerability in Antminer Monitor 0.50.0 exists because of backdoor or misconfiguration inside a settings file in flask server. Settings file has a predefined secret string, which would be randomly generated, however it is static.	9.8	More Details
CVE-2022-31355	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via /ordering/index.php?q=category&search=.	9.8	More Details
CVE-2022-31356	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via /ordering/admin/store/index.php?view=edit&id=.	9.8	More Details
CVE-2022-31357	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via /ordering/admin/inventory/index.php?view=edit&id=.	9.8	More Details
CVE-2022-22485	In some cases, an unsuccessful attempt to log into IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.14.000 does not cause the administrator's invalid sign-on count to be incremented on the IBM Spectrum Protect Server. An attacker could exploit this vulnerability using brute force techniques to gain unauthorized administrative access to the IBM Spectrum Protect Server. IBM X-Force ID: 226325.	9.8	More Details
CVE-2022-30422	Proietti Tech srl Planet Time Enterprise 4.2.0.1,4.2.0.0,4.1.0.0,4.0.0.0,3.3.1.0,3.3.0.0 is vulnerable to Remote code execution via the Viewstate parameter.	9.8	More Details
CVE-2022-21806	A use-after-free vulnerability exists in the mips_collector appsrv_server functionality of Anker Eufy Homebase 2 2.1.8.5h. A specially-crafted set of network packets can lead to remote code execution. The device is exposed to attacks from the network.	9.8	More Details
CVE-2022-29496	A stack-based buffer overflow vulnerability exists in the BlynkConsole.h runCommand functionality of Blynk -Library v1.0.1. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger this vulnerability.	9.8	More Details
CVE-2022-31941	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via \rdms\admin?page=user\manage_user&id=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34005	An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. There is Remote Code Execution due to a hardcoded password for the sa account on the Microsoft SQL Express 2019 instance installed by default during TitanFTP NextGen installation, aka NX-I674 (sub-issue 1). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation.	9.8	More Details
CVE-2022-20127	In ce_t4t_data_cback of ce_t4t.cc, there is a possible out of bounds write due to a double free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221862119	9.8	More Details
CVE-2022-2023	Incorrect Use of Privileged APIs in GitHub repository polonel/trudesk prior to 1.2.4.	9.8	More Details
CVE-2022-1905	The Events Made Easy WordPress plugin before 2.2.81 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	9.8	More Details
CVE-2022-31794	An issue was discovered on Fujitsu ETERNUS CentricStor CS8000 (Control Center) devices before 8.1A SP02 P04. The vulnerability resides in the requestTempFile function in hw_view.php. An attacker is able to influence the unitName POST parameter and inject special characters such as semicolons, backticks, or command-substitution sequences in order to force the application to execute arbitrary commands.	9.8	More Details
CVE-2022-31795	An issue was discovered on Fujitsu ETERNUS CentricStor CS8000 (Control Center) devices before 8.1A SP02 P04. The vulnerability resides in the grel_finfo function in grel.php. An attacker is able to influence the username (user), password (pw), and file-name (file) parameters and inject special characters such as semicolons, backticks, or command-substitution sequences in order to force the application to execute arbitrary commands.	9.8	More Details
CVE-2022-22317	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 218281.	9.8	More Details
CVE-2022-22318	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	9.8	More Details
CVE-2022-2128	Unrestricted Upload of File with Dangerous Type in GitHub repository polonel/trudesk prior to 1.2.4.	9.8	More Details
CVE-2022-31800	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.	9.8	More Details
CVE-2022-31801	An unauthenticated, remote attacker could upload malicious logic to the devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.	9.8	More Details
CVE-2022-31374	An arbitrary file upload vulnerability /images/background/1.php in of SolarView Compact 6.0 allows attackers to execute arbitrary code via a crafted php file.	9.8	More Details
CVE-2022-33139	A vulnerability has been identified in Cerberus DMS (All versions), Desigo CC (All versions), Desigo CC Compact (All versions), SIMATIC WinCC OA V3.16 (All versions in default configuration), SIMATIC WinCC OA V3.17 (All versions in non-default configuration), SIMATIC WinCC OA V3.18 (All versions in non-default configuration). Affected applications use client-side only authentication, when neither server-side authentication (SSA) nor Kerberos authentication is enabled. In this configuration, attackers could impersonate other users or exploit the client-server protocol without being authenticated.	9.8	More Details
CVE-2022-29774	iSpy v7.2.2.0 is vulnerable to remote command execution via path traversal.	9.8	More Details
CVE-2022-29775	iSpyConnect iSpy v7.2.2.0 allows attackers to bypass authentication via a crafted URL.	9.8	More Details
CVE-2022-26147	The Quectel RG502Q-EA modem before 2022-02-23 allow OS Command Injection.	9.8	More Details
CVE-2022-33754	CA Automic Automation 12.2 and 12.3 contain an insufficient input validation vulnerability in the Automic agent that could allow a remote attacker to potentially execute arbitrary code.	9.8	More Details
CVE-2022-33752	CA Automic Automation 12.2 and 12.3 contain an insufficient input validation vulnerability in the Automic agent that could allow a remote attacker to potentially execute arbitrary code.	9.8	More Details
CVE-2022-33750	CA Automic Automation 12.2 and 12.3 contain an authentication error vulnerability in the Automic agent that could allow a remote attacker to potentially execute arbitrary commands.	9.8	More Details
CVE-2022-24562	In IOBit IOTransfer 4.3.1.1561, an unauthenticated attacker can send GET and POST requests to Airserv and gain arbitrary read/write access to the entire file-system (with admin privileges) on the victim's endpoint, which can result in data theft and remote code execution.	9.8	More Details
CVE-2022-20130	In transportDec_OutOfBandConfig of tpdec_lib.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224314979	9.8	More Details
CVE-2022-20140	In read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-227618988	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20145	In startLegacyVpnPrivileged of Vpn.java, there is a possible way to retrieve VPN credentials due to a protocol downgrade attack. This could lead to remote escalation of privilege if a malicious Wi-Fi AP is used, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-201660636	9.8	More Details
CVE-2022-20160	Product: AndroidVersions: Android kernelAndroid ID: A-210083655References: N/A	9.8	More Details
CVE-2022-20164	Product: AndroidVersions: Android kernelAndroid ID: A-204891956References: N/A	9.8	More Details
CVE-2022-20167	Product: AndroidVersions: Android kernelAndroid ID: A-204956204References: N/A	9.8	More Details
CVE-2022-20170	Product: AndroidVersions: Android kernelAndroid ID: A-209421931References: N/A	9.8	More Details
CVE-2022-20171	Product: AndroidVersions: Android kernelAndroid ID: A-215565667References: N/A	9.8	More Details
CVE-2022-20173	Product: AndroidVersions: Android kernelAndroid ID: A-207116951References: N/A	9.8	More Details
CVE-2022-20191	Product: AndroidVersions: Android kernelAndroid ID: A-209324757References: N/A	9.8	More Details
CVE-2022-20210	The UE and the EMM communicate with each other using NAS messages. When a new NAS message arrives from the EMM, the modem parses it and fills in internal objects based on the received data. A bug in the parsing code could be used by an attacker to remotely crash the modem, which could lead to DoS or RCE.Product: AndroidVersions: Android SoCAndroid ID: A-228868888	9.8	More Details
CVE-2019-4575	IBM Financial Transaction Manager for Digital Payments for Multi-Platform 3.2.0 through 3.2.9 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: 166801.	9.8	More Details
CVE-2021-40940	Monstra 3.0.4 does not filter the case of php, which leads to an unrestricted file upload vulnerability.	9.8	More Details
CVE-2022-32101	kkcms v1.3.7 was discovered to contain a SQL injection vulnerability via the cid parameter at /template/wapian/vlist.php.	9.8	More Details
CVE-2022-2068	In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).	9.8	More Details
CVE-2022-32301	YoudianCMS v9.5.0 was discovered to contain a SQL injection vulnerability via the IdList parameter at /App/Lib/Action/Home/ApiAction.class.php.	9.8	More Details
CVE-2017-20049	A vulnerability, was found in legacy Axis devices such as P3225 and M3005. This affects an unknown part of the component CGI Script. The manipulation leads to improper privilege management. It is possible to initiate the attack remotely.	9.8	More Details
CVE-2022-20798	A vulnerability in the external authentication functionality of Cisco Secure Email and Web Manager, formerly known as Cisco Security Management Appliance (SMA), and Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass authentication and log in to the web management interface of an affected device. This vulnerability is due to improper authentication checks when an affected device uses Lightweight Directory Access Protocol (LDAP) for external authentication. An attacker could exploit this vulnerability by entering a specific input on the login page of the affected device. A successful exploit could allow the attacker to gain unauthorized access to the web-based management interface of the affected device.	9.8	More Details
CVE-2022-20825	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Cisco has not released software updates that address this vulnerability.	9.8	More Details
CVE-2021-41418	AriaNg v0.1.0~v1.2.2 is affected by an incorrect access control vulnerability through not authenticating visitors' access rights.	9.8	More Details
CVE-2021-41403	flatCore-CMS version 2.0.8 calls dangerous functions, causing server-side request forgery vulnerabilities.	9.8	More Details
CVE-2022-30136	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41411	drools <=7.59.x is affected by an XML External Entity (XXE) vulnerability in KieModuleMarshaller.java. The Validator class is not used correctly, resulting in the XXE injection vulnerability.	9.8	More Details
CVE-2022-2098	Weak Password Requirements in GitHub repository kromitgmbh/titra prior to 0.78.1.	9.8	More Details
CVE-2021-41654	SQL injection vulnerabilities exist in Wuzhicms v4.1.0 which allows attackers to execute arbitrary SQL commands via the $keyValue parameter in /coreframe/app/pay/admin/index.php	9.8	More Details
CVE-2022-31382	Directory Management System v1.0 was discovered to contain a SQL injection vulnerability via the searchdata parameter in search-dirctory.php.	9.8	More Details
CVE-2022-31383	Directory Management System v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter in view-directory.php.	9.8	More Details
CVE-2022-31384	Directory Management System v1.0 was discovered to contain a SQL injection vulnerability via the fullname parameter in add-directory.php.	9.8	More Details
CVE-2021-41487	NOKIA VitalSuite SPM 2020 is affected by SQL injection through UserName'.	9.8	More Details
CVE-2022-25772	A cross-site scripting (XSS) vulnerability in the web tracking component of Mautic before 4.3.0 allows remote attackers to inject executable javascript	9.6	More Details
CVE-2022-32158	Splunk Enterprise deployment servers in versions before 8.1.10.1, 8.2.6.1, and 9.0 let clients deploy forwarder bundles to other deployment clients through the deployment server. An attacker that compromised a Universal Forwarder endpoint could use the vulnerability to execute arbitrary code on all other Universal Forwarder endpoints subscribed to the deployment server.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2019-12356	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /user/dls_download.php (when the attacker has dls_download authority) via the id parameter.
CVE-2022-32973	An authenticated attacker could create an audit file that bypasses PowerShell cmdlet checks and executes commands with administrator privileges.
CVE-2022-30165	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-26669	ASUS Control Center is vulnerable to SQL injection. An authenticated remote attacker with general user privilege can inject SQL command to specific API parameters t acquire database schema or access data.
CVE-2021-41402	flatCore-CMS v2.0.8 has a code execution vulnerability, which could let a remote malicious user execute arbitrary PHP code.
CVE-2022-30161	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2021-33036	In Apache Hadoop 2.2.0 to 2.10.1, 3.0.0-alpha1 to 3.1.4, 3.2.0 to 3.2.2, and 3.3.0 to 3.3.1, a user who can escalate to yarn user can possibly run arbitrary commands a root user. Users should upgrade to Apache Hadoop 2.10.2, 3.2.3, 3.3.2 or higher.
CVE-2022-33140	The optional ShellUserGroupProvider in Apache NiFi 1.10.0 to 1.16.2 and Apache NiFi Registry 0.6.0 to 1.16.2 does not neutralize arguments for group resolution commands, allowing injection of operating system commands on Linux and macOS platforms. The ShellUserGroupProvider is not included in the default configuration. Command injection requires ShellUserGroupProvider to be one of the enabled User Group Providers in the Authorizers configuration. Command injection also requires an authenticated user with elevated privileges. Apache NiFi requires an authenticated user with authorization to modify access policies in order to execute the comman Apache NiFi Registry requires an authenticated user with authorization to read user groups in order to execute the command. The resolution removes command formatting based on user-provided arguments.
CVE-2022-30158	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2019-12358	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /dl/dl_sendsms.php (when the attacker has dls_print authority) via a dlid cookie.

CVE Number	Description
CVE-2022-30157	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2022-30153	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-32299	YoudianCMS v9.5.0 was discovered to contain a SQL injection vulnerability via the id parameter at /App/Lib/Action/Admin/SiteAction.class.php.
CVE-2022-30023	Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1 is vulnerable to Command Injection via the Ping function.
CVE-2022-32300	YoudianCMS v9.5.0 was discovered to contain a SQL injection vulnerability via the MailSendID parameter at /App/Lib/Action/Admin/MailAction.class.php.
CVE-2022-32302	Theme Park Ticketing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at edit_ticket.php.
CVE-2022-31277	Xiaomi Lamp 1 v2.0.4_0066 was discovered to be vulnerable to replay attacks. This allows attackers to to bypass the expected access restrictions and gain control of the switch and other functions via a crafted POST request.
CVE-2022-30670	RoboHelp Server earlier versions than RHS 11 Update 3 are affected by an Improper Authorization vulnerability which could lead to privilege escalation. An authenticated attacker could leverage this vulnerability to achieve full administrator privileges. Exploitation of this issue does not require user interaction.
CVE-2022-32991	Web Based Quiz System v1.0 was discovered to contain a SQL injection vulnerability via the eid parameter at welcome.php.
CVE-2022-31849	MERCURY MIPC451-4 1.0.22 Build 220105 Rel.55642n was discovered to contain a remote code execution (RCE) vulnerability which is exploitable via a crafted POST request.
CVE-2022-1833	A flaw was found in AMQ Broker Operator 7.9.4 installed via UI using OperatorHub where a low-privilege user that has access to the namespace where the AMQ Operator is deployed has access to clusterwide edit rights by checking the secrets. The service account used for building the Operator gives more permission than expected and an attacker could benefit from it. This requires at least an already compromised low-privilege account or insider attack.
CVE-2022-26173	JForum v2.8.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via http://target_host:port/jforum-2.8.0/jforum.page, which allows attackers to arbitrarily add admin accounts.
CVE-2022-33753	CA Automic Automation 12.2 and 12.3 contain an insecure file creation and handling vulnerability in the Automic agent that could allow a user to potentially elevate privileges.
CVE-2022-2112	Improper Neutralization of Formula Elements in a CSV File in GitHub repository inventree/inventree prior to 0.7.2.
CVE-2022-2111	Unrestricted Upload of File with Dangerous Type in GitHub repository inventree/inventree prior to 0.7.2.
CVE-2022-30325	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The default pre-shared key for the Wi-Fi networks is the same for every router except for the last four digits. The device default pre-shared key for both 2.4 GHz and 5 GHz networks can be guessed or brute-forced by an attacker within range of the Wi-Fi network.
CVE-2020-36549	A vulnerability classified as critical was found in GE Voluson S8. Affected is the underlying Windows XP operating system. Missing patches might introduce an excessiv attack surface. Access to the local network is required for this attack to succeed.
CVE-2019-12352	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /dl/dl_sendmail.php (when the attacker has dls_print authority) via a dlid cookie.
CVE-2019-12355	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /user/dls_print.php (when the attacker has dls_print authority) via the id parameter.

CVE Number	Description
CVE-2020-35597	Victor CMS 1.0 is vulnerable to SQL injection via c_id parameter of admin_edit_comment.php, p_id parameter of admin_edit_post.php, u_id parameter of admin_edit_user.php, and edit parameter of admin_update_categories.php.
CVE-2022-21937	Under certain circumstances, a vulnerability in Metasys ADS/ADX/OAS 10 versions prior to 10.1.5 and Metasys ADS/ADX/OAS 11 versions prior to 11.0.2 could allow a user to inject malicious code into the web interface.
CVE-2022-31083	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 4.10.11 and 5.2.2, the certificate in the Parse Server Apple Game Center auth adapter not validated. As a result, authentication could potentially be bypassed by making a fake certificate accessible via certain Appl domains and providing the URL to that certificate in an authData object. Versions 4.0.11 and 5.2.2 prevent this by introducing a new `rootCertificateUrl` property to the Parse Server Apple Game Center auth adapter which takes the URL to the root certificate of Apple's Game Center authentication certificate. If no value is set, the `rootCertificateUrl` property defaults to the URL of the current root certificate as of May 27, 2022. Keep in mind that the root certificate can change at any time and that is the developer's responsibility to keep the root certificate URL up-to-date when using the Parse Server Apple Game Center auth adapter. There are no known workarounds for this issue.
CVE-2022-30163	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-22021	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2022-1665	A set of pre-production kernel packages of Red Hat Enterprise Linux for IBM Power architecture can be booted by the grub in Secure Boot mode even though it shouldn't. These kernel builds don't have the secure boot lockdown patches applied to it and can bypass the secure boot validations, allowing the attacker to load another non-trusted code.
CVE-2022-32156	In Splunk Enterprise and Universal Forwarder versions before 9.0, the Splunk command-line interface (CLI) did not validate TLS certificates while connecting to a remo Splunk platform instance by default. After updating to version 9.0, see Configure TLS host name validation for the Splunk CLI https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation#Configure_TLS_host_name_validation_for_the_Splunk_CLI to enab the remediation. The vulnerability does not affect the Splunk Cloud Platform. At the time of publishing, we have no evidence of exploitation of this vulnerability by external parties. The issue requires conditions beyond the control of a potential bad actor such as a machine-in-the-middle attack. Hence, Splunk rates the complexity o the attack as High.
CVE-2022-30141	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2021-46820	Arbitrary File Deletion vulnerability in XOS-Shop xos_shop_system 1.0.9 via current_manufacturer_image parameter to /shop/admin/categories.php
CVE-2022-27511	Corruption of the system by a remote, unauthenticated user. The impact of this can include the reset of the administrator password at the next device reboot, allowing a attacker with ssh access to connect with the default administrator credentials after the device has rebooted.
CVE-2022-31625	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to the parametrized query may lead to PHP attempting to free memory using uninitialized data as pointers. This could lead to RCE vulnerability or denial of service.
CVE-2022-21938	Under certain circumstances, a vulnerability in Metasys ADS/ADX/OAS 10 versions prior to 10.1.5 and Metasys ADS/ADX/OAS 11 versions prior to 11.0.2 could allow a user to inject malicious code into the MUI Graphics web interface.
CVE-2022-32153	Splunk Enterprise peers in Splunk Enterprise versions before 9.0 and Splunk Cloud Platform versions before 8.2.2203 did not validate the TLS certificates during Splun to-Splunk communications by default. Splunk peer communications configured properly with valid certificates were not vulnerable. However, an attacker with administrator credentials could add a peer without a valid certificate and connections from misconfigured nodes without valid certificates did not fail by default. For Splunk Enterprise, update to Splunk Enterprise version 9.0 and Configure TLS host name validation for Splunk-to-Splunk communications (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation) to enable the remediation.
CVE-2022-32152	Splunk Enterprise peers in Splunk Enterprise versions before 9.0 and Splunk Cloud Platform versions before 8.2.2203 did not validate the TLS certificates during Splun to-Splunk communications by default. Splunk peer communications configured properly with valid certificates were not vulnerable. However, an attacker with administrator credentials could add a peer without a valid certificate and connections from misconfigured nodes without valid certificates did not fail by default. For Splunk Enterprise, update to Splunk Enterprise version 9.0 and Configure TLS host name validation for Splunk-to-Splunk communications (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation) to enable the remediation.
CVE-2021-37764	Arbitrary File Deletion vulnerability in XOS-Shop xos_shop_system 1.0.9 via current_manufacturer_image parameter to /shop/admin/manufacturers.php.
CVE-2022-1824	An uncontrolled search path vulnerability in McAfee Consumer Product Removal Tool prior to version 10.4.128 could allow a local attacker to perform a sideloading attack by using a specific file name. This could result in the user gaining elevated permissions and being able to execute arbitrary code as there were insufficient check on the executable being signed by McAfee.

CVE Number	Description
CVE-2022-1823	Improper privilege management vulnerability in McAfee Consumer Product Removal Tool prior to version 10.4.128 could allow a local user to modify a configuration file and perform a LOLBin (Living off the land) attack. This could result in the user gaining elevated permissions and being able to execute arbitrary code, through not correctly checking the integrity of the configuration file.
CVE-2022-30132	Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2022-30131	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
CVE-2021-43756	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an Out-of-bounds Write vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2021-43754	Adobe Prelude version 22.1.1 (and earlier) is affected by an Out-of-bounds Write vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrar code execution in the context of the current user. User interaction is required to exploit this vulnerability.
CVE-2022-30135	Windows Media Center Elevation of Privilege Vulnerability
CVE-2022-27867	A maliciously crafted JT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead t code execution.
CVE-2022-20135	In writeToParcel of GateKeeperResponse.java, there is a possible parcel format mismatch. 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-12 Android-12LAndroid ID: A-220303465
CVE-2022-30147	Windows Installer Elevation of Privilege Vulnerability
CVE-2021-41683	There is a stack-overflow at ecma-helpers.c:326 in ecma_get_lex_env_type in JerryScript 2.4.0
CVE-2022-20134	In readArguments of CallSubjectDialog.java, there is a possible way to trick the user to call the wrong phone number due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-218341397
CVE-2021-39806	In closef of label_backends_android.c, there is a possible way to corrupt memory due to a double free. This could lead to local escalation of privilege during startup of servicemanager, if an attacker can trigger an initialization failure, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-215387420
CVE-2022-20138	In ACTION_MANAGED_PROFILE_PROVISIONED of DevicePolicyManagerService.java, there is a possible way for unprivileged app to send MANAGED_PROFILE_PROVISIONED intent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-210469972
CVE-2022-20142	In createFromParcel of GeofenceHardwareRequestParcelable.java, there is a possible arbitrary code execution due to parcel mismatch. 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-12 Android-12LAndroid ID: A-216631962
CVE-2022-30546	Out-of-bounds read vulnerability exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.
CVE-2022-27868	A maliciously crafted CAT file in Autodesk AutoCAD 2023 can be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead to code execution
CVE-2022-29149	Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability
CVE-2022-31218	Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist. The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.
CVE-2022-31216	Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist. The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.

CVE Number	Description
CVE-2021-43755	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an Out-of-bounds Write vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.
CVE-2022-28844	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28849	Adobe Bridge version 12.0.1 (and earlier versions) is affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-27532	A maliciously crafted TIF file in Autodesk 3ds Max 2022 and 2021 can be used to write beyond the allocated buffer while parsing TIF files. This vulnerability in conjunction with other vulnerabilities could lead to arbitrary code execution.
CVE-2022-27531	A maliciously crafted TIF file can be forced to read beyond allocated boundaries in Autodesk 3ds Max 2022, and 2021 when parsing the TIF files. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.
CVE-2022-20124	In deletePackageX of DeletePackageHelper.java, there is a possible way for a Guest user to reset pre-loaded applications for other users due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-170646036
CVE-2022-28226	Local privilege vulnerability in Yandex Browser for Windows prior to 22.3.3.801 allows a local, low privileged, attacker to execute arbitary code with the SYSTEM privileges through manipulating temporary files in directory with insecure permissions during Yandex Browser update process.
CVE-2022-28225	Local privilege vulnerability in Yandex Browser for Windows prior to 22.3.3.684 allows a local, low privileged, attacker to execute arbitary code with the SYSTEM privileges through manipulating symlinks to installation file during Yandex Browser update process.
CVE-2022-30659	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2021-41413	ok-file-formats master 2021-9-12 is affected by a buffer overflow in ok_jpg_convert_data_unit_grayscale and ok_jpg_convert_YCbCr_to_RGB.
CVE-2021-42735	Adobe Photoshop version 22.5.1 (and earlier versions) is affected by an Access of Memory Location After End of Buffer vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.
CVE-2022-31217	Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist. The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.
CVE-2022-33912	A permission issue affects users that deployed the shipped version of the Checkmk Debian package. Packages created by the agent bakery (enterprise editions only) were not affected. Using the shipped version of the agents, the maintainer scripts located at /var/lib/dpkg/info/ will be owned by the user and the group with ID 1001. If such a user exists on the system, they can change the content of these files (which are then executed by root). This leads to a local privilege escalation on the monitored host. Version 1.6 through 1.6.9p29, version 2.0 through 2.0.0p26, version 2.1 through 2.1.0p3, and version 2.2.0i1 are affected.
CVE-2022-30649	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2021-25261	Local privilege vulnerability in Yandex Browser for Windows prior to 22.5.0.862 allows a local, low privileged, attacker to execute arbitary code with the SYSTEM privileges through manipulating symlinks to installation file during Yandex Browser update process.
CVE-2022-20133	In setDiscoverableTimeout of AdapterService.java, there is a possible bypass of user interaction due to a missing permission check. This could lead to local escalation privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-206807679
CVE-2022-20203	In multiple locations of the nanopb library, there is a possible way to corrupt memory when decoding untrusted protobuf files. This could lead to local escalation of privilege,with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2022-22018	HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-29111	HEVC Video Extensions Remote Code Execution Vulnerability

CVE Number	Description
CVE-2022-29119	HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-40727	Access of Memory Location After End of Buffer (CWE-788
CVE-2021-42732	Access of Memory Location After End of Buffer (CWE-788)
CVE-2022-30549	Out-of-bounds read vulnerability exists in V-Server v4.0.11.0 and earlier and V-Server Lite v4.0.13.0 and earlier, which may allow an attacker to obtain information and/ execute arbitrary code by having a user to open a specially crafted image file.
CVE-2021-39820	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) is affected by an Out-of-bounds Write vulnerability due to insecure handling of a malicious TIFF file potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.
CVE-2022-20207	In static definitions of GattServiceConfig.java, there is a possible permission bypass due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-185513714
CVE-2022-20204	In registerRemoteBugreportReceivers of DevicePolicyManagerService.java, there is a possible reporting of falsified bug reports due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-171495100
CVE-2022-31464	Insecure permissions configuration in Adaware Protect v1.2.439.4251 allows attackers to escalate privileges via changing the service binary path.
CVE-2022-30656	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-20197	In recycle of Parcel.java, there is a possible way to start foreground activity from background due to a permissions bypass. This could lead to local escalation of privileg with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-208279300
CVE-2022-30166	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2022-20194	In onCreate of ChooseLockGeneric.java, there is a possible permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-222684510
CVE-2022-30167	AV1 Video Extension Remote Code Execution Vulnerability
CVE-2022-20192	In grantEmbeddedWindowFocus of WindowManagerService.java, there is a possible way to change an input channel for embedded hierarchy due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-215912712
CVE-2022-30168	Microsoft Photos App Remote Code Execution Vulnerability
CVE-2022-20186	In kbase_mem_alias of mali_kbase_mem_linux.c, there is a possible arbitrary code execution due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-215001024References: N/A
CVE-2022-30173	Microsoft Excel Remote Code Execution Vulnerability
CVE-2022-30174	Microsoft Office Remote Code Execution Vulnerability
CVE-2022-20156	In unflatten of GraphicBuffer.cpp, there is a possible arbitrary code execution due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-212803946References: N/A

CVE Number	Description
CVE-2022-30177	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30178	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30179	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30180	Azure RTOS GUIX Studio Information Disclosure Vulnerability
CVE-2022-32547	In ImageMagick, there is load of misaligned address for type 'double', which requires 8 byte alignment and for type 'float', which requires 4 byte alignment at MagickCore/property.c. Whenever crafted or untrusted input is processed by ImageMagick, this causes a negative impact to application availability or other problems related to undefined behavior.
CVE-2022-30188	HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-32546	A vulnerability was found in ImageMagick, causing an outside the range of representable values of type 'unsigned long' at coders/pcl.c, when crafted or untrusted input processed. This leads to a negative impact to application availability or other problems related to undefined behavior.
CVE-2022-30193	AV1 Video Extension Remote Code Execution Vulnerability
CVE-2022-32545	A vulnerability was found in ImageMagick, causing an outside the range of representable values of type 'unsigned char' at coders/psd.c, when crafted or untrusted inpu is processed. This leads to a negative impact to application availability or other problems related to undefined behavior.
CVE-2022-1720	Buffer Over-read in function grab_file_name in GitHub repository vim/vim prior to 8.2.4956. This vulnerability is capable of crashing the software, memory modification, and possible remote execution.
CVE-2022-30538	Out-of-bounds write vulnerability exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.
CVE-2022-34008	Comodo Antivirus 12.2.2.8012 has a quarantine flaw that allows privilege escalation. To escalate privilege, a low-privileged attacker can use an NTFS directory junctior to restore a malicious DLL from quarantine into the System32 folder.
CVE-2021-41682	There is a heap-use-after-free at ecma-helpers-string.c:1940 in ecma_compare_ecma_non_direct_strings in JerryScript 2.4.0
CVE-2022-30164	Kerberos AppContainer Security Feature Bypass Vulnerability
CVE-2022-27871	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code.
CVE-2022-27872	A maliciously crafted PDF file may be used to dereference a pointer for read or write operation while parsing PDF files in Autodesk Navisworks 2022. The vulnerability exists because the application fails to handle a crafted PDF file, which causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code.
CVE-2022-27869	A maliciously crafted TIFF file in Autodesk AutoCAD 2023 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability ca be exploited to execute arbitrary code.
CVE-2022-2124	Buffer Over-read in GitHub repository vim/vim prior to 8.2.
CVE-2022-20144	In multiple functions of AvatarPhotoController.java, there is a possible access to content owned by system content providers due to a confused deputy. This could lead local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Androic 11Android ID: A-250637906

CVE Number	Description
CVE-2022-27870	A maliciously crafted TGA file in Autodesk AutoCAD 2023 may be used to write beyond the allocated buffer while parsing TGA file. This vulnerability may be exploited t execute arbitrary code.
CVE-2022-2125	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-2129	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.
CVE-2022-20147	In nfa_dm_check_set_config of nfa_dm_main.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221216105
CVE-2022-2126	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.
CVE-2022-30160	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2022-34006	An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. When installing, Microsoft SQL Express 2019 installs by default with an SQL instance running as SYSTEM with BUILTIN\Users as sysadmin, thus enabling unprivileged Windows users to execute commands locally as NT AUTHORITY\SYSTEM, aka NX-I674 (sub-issue 2). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation.
CVE-2022-20664	A vulnerability in the web management interface of Cisco Secure Email and Web Manager, formerly Cisco Security Management Appliance (SMA), and Cisco Email Security Appliance (ESA) could allow an authenticated, remote attacker to retrieve sensitive information from a Lightweight Directory Access Protocol (LDAP) external authentication server connected to an affected device. This vulnerability is due to a lack of proper input sanitization while querying the external authentication server. An attacker could exploit this vulnerability by sending a crafted query through an external authentication web page. A successful exploit could allow the attacker to gain access to sensitive information, including user credentials from the external authentication server. To exploit this vulnerability, an attacker would need valid operator-lev (or higher) credentials.
CVE-2022-30142	Windows File History Remote Code Execution Vulnerability
CVE-2022-31372	Wiris Mathtype v7.28.0 was discovered to contain a path traversal vulnerability in the resourceFile parameter. This vulnerability is exploited via a crafted request to the resource handler.
CVE-2022-30140	Windows iSCSI Discovery Service Remote Code Execution Vulnerability
CVE-2022-31295	An issue in the delete_post() function of Online Discussion Forum Site 1 allows unauthenticated attackers to arbitrarily delete posts.
CVE-2022-30152	Windows Network Address Translation (NAT) Denial of Service Vulnerability
CVE-2022-30150	Windows Defender Remote Credential Guard Elevation of Privilege Vulnerability
CVE-2022-24946	Improper Resource Locking vulnerability in Mitsubishi Electric MELSEC iQ-R Series R12CCPU-V firmware versions "16" and prior, Mitsubishi Electric MELSEC-Q Serie Q03UDECPU the first 5 digits of serial No. "24061" and prior, Mitsubishi Electric MELSEC-Q Series Q04/06/10/13/20/26/50/100UDEHCPU the first 5 digits of serial No. "24061" and prior, Mitsubishi Electric MELSEC-Q Series Q03/04/06/13/26UDVCPU the first 5 digits of serial number "24051" and prior, Mitsubishi Electric MELSEC-Q Series Q04/06/13/26UDPVCPU the first 5 digits of serial number "24051" and prior, Mitsubishi Electric MELSEC-Q Series Q12DCCPU-V all versions, Mitsubishi Electri MELSEC-Q Series Q24DHCCPU-V(G) all versions, Mitsubishi Electric MELSEC-Q Series Q24/26DHCCPU-LS all versions, Mitsubishi Electric MELSEC-L series L02/06/26CPU(-P) the first 5 digits of serial number "24051" and prior, Mitsubishi Electric MELSEC-L series L26CPU-(P)BT the first 5 digits of serial number "24051" ar prior and Mitsubishi Electric MELIPC Series MI5122-VW firmware versions "05" and prior allows a remote unauthenticated attacker to cause a denial of service (DoS) condition in Ethernet communications by sending specially crafted packets. A system reset of the products is required for recovery.
CVE-2022-30149	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2020-28865	An issue was discovered in PowerJob through 3.2.2, allows attackers to change arbitrary user passwords via the id parameter to /appinfo/save.

CVE Number	Description
CVE-2022-29862	An infinite loop in OPC UA .NET Standard Stack 1.04.368 allows a remote attackers to cause the application to hang via a crafted message.
CVE-2022-29865	OPC UA .NET Standard Stack allows a remote attacker to bypass the application authentication check via crafted fake credentials.
CVE-2022-33756	CA Automic Automation 12.2 and 12.3 contain an entropy weakness vulnerability in the Automic AutomationEngine that could allow a remote attacker to potentially access sensitive data.
CVE-2022-29863	OPC UA .NET Standard Stack 1.04.368 allows remote attacker to cause a crash via a crafted message that triggers excessive memory allocation.
CVE-2022-30143	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2020-25459	An issue was discovered in function sync_tree in hetero_decision_tree_guest.py in WeBank FATE (Federated AI Technology Enabler) 0.1 through 1.4.2 allows attacke to read sensitive information during the training process of machine learning joint modeling.
CVE-2022-29143	Microsoft SQL Server Remote Code Execution Vulnerability
CVE-2022-29864	OPC UA .NET Standard Stack 1.04.368 allows a remote attacker to cause a server to crash via a large number of messages that trigger Uncontrolled Resource Consumption.
CVE-2022-29866	OPC UA .NET Standard Stack 1.04.368 allows a remote attacker to exhaust the memory resources of a server via a crafted request that triggers Uncontrolled Resourc Consumption.
CVE-2022-33913	In Mahara 21.04 before 21.04.6, 21.10 before 21.10.4, and 22.04.2, files can sometimes be downloaded through thumb.php with no permission check.
CVE-2022-31626	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd driver, if the third party is allowed to supply hos to connect to and the password for the connection, password of excessive length can trigger a buffer overflow in PHP, which can lead to a remote code execution vulnerability.
CVE-2022-33751	CA Automic Automation 12.2 and 12.3 contain an insecure memory handling vulnerability in the Automic agent that could allow a remote attacker to potentially access sensitive data.
CVE-2022-33739	CA Clarity 15.8 and below and 15.9.0 contain an insecure XML parsing vulnerability that could allow a remote attacker to potentially view the contents of any file on the system.
CVE-2018-18907	An issue was discovered on D-Link DIR-850L 1.21WW devices. A partially completed WPA handshake is sufficient for obtaining full access to the wireless network. A client can access the network by sending packets on Data Frames to the AP without encryption.
CVE-2022-30146	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30145	Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
CVE-2022-30139	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-31291	An issue in dlt_config_file_parser.c of dlt-daemon v2.18.8 allows attackers to cause a double free via crafted TCP packets.
CVE-2022-20177	Product: AndroidVersions: Android kernelAndroid ID: A-209906686References: N/A

CVE Number	Description
CVE-2022-22138	All versions of package fast-string-search are vulnerable to Denial of Service (DoS) when computations are incorrect for non-string inputs. One can cause the V8 to attempt reading from non-permitted locations and cause a segmentation fault due to the violation.
CVE-2022-20169	Product: AndroidVersions: Android kernelAndroid ID: A-211162353References: N/A
CVE-2022-33995	A path traversal issue in entry attachments in Devolutions Remote Desktop Manager before 2022.2 allows attackers to create or overwrite files in an arbitrary location.
CVE-2022-20175	Product: AndroidVersions: Android kernelAndroid ID: A-209252491References: N/A
CVE-2022-20179	Product: AndroidVersions: Android kernelAndroid ID: A-211683760References: N/A
CVE-2022-20181	Product: AndroidVersions: Android kernelAndroid ID: A-210936609References: N/A
CVE-2022-20184	Product: AndroidVersions: Android kernelAndroid ID: A-209153114References: N/A
CVE-2022-21213	This affects all versions of package mout. The deepFillIn function can be used to 'fill missing properties recursively', while the deepMixIn mixes objects into the target object, recursively mixing existing child objects as well. In both cases, the key used to access the target object recursively is not checked, leading to exploiting this vulnerability. **Note:** This vulnerability derives from an incomplete fix of [CVE-2020-7792](https://security.snyk.io/vuln/SNYK-JS-MOUT-1014544).
CVE-2022-31044	Rundeck is an open source automation service with a web console, command line tools and a WebAPI. The Key Storage converter plugin mechanism was not enabled correctly in Rundeck 4.2.0 and 4.2.1, resulting in use of the encryption layer for Key Storage possibly not working. Any credentials created or overwritten using Rundecl 4.2.0 or 4.2.1 might result in them being written in plaintext to the backend storage. This affects those using any `Storage Converter` plugin. Rundeck 4.3.1 and 4.2.2 have fixed the code and upon upgrade will re-encrypt any plain text values. Version 4.3.0 does not have the vulnerability, but does not include the patch to re-encrypt plain text values if 4.2.0 or 4.2.1 were used. To prevent plaintext credentials from being stored in Rundeck 4.2.0/4.2.1, write access to key storage can be disabled via ACLs. After upgrading to 4.3.1 or later, write access can be restored.
CVE-2022-20188	Product: AndroidVersions: Android kernelAndroid ID: A-207254598References: N/A
CVE-2022-20151	Product: AndroidVersions: Android kernelAndroid ID: A-210712565References: N/A
CVE-2022-20190	Product: AndroidVersions: Android kernelAndroid ID: A-208744915References: N/A
CVE-2022-25345	All versions of package @discordjs/opus are vulnerable to Denial of Service (DoS) when trying to encode using an encoder with zero channels, or a non-initialized buffer. This leads to a hard crash.
CVE-2022-25852	All versions of package pg-native; all versions of package libpq are vulnerable to Denial of Service (DoS) when the addons attempt to cast the second argument to an array and fail. This happens for every non-array argument passed. **Note:** pg-native is a mere binding to npm's libpq library, which in turn has the addons and binding to the actual C libpq library. This means that problems found in pg-native may transitively impact npm's libpq.
CVE-2022-25856	The package github.com/argoproj/argo-events/sensors/artifacts before 1.7.1 are vulnerable to Directory Traversal in the (g *GitArtifactReader).Read() API in git.go. This could allow arbitrary file reads if the GitArtifactReader is provided a pathname containing a symbolic link or an implicit directory name such as ...
CVE-2022-22979	In Spring Cloud Function versions prior to 3.2.6, it is possible for a user who directly interacts with framework provided lookup functionality to cause a denial-of-service condition due to the caching issue in the Function Catalog component of the framework.
CVE-2022-32157	Splunk Enterprise deployment servers in versions before 9.0 allow unauthenticated downloading of forwarder bundles. Remediation requires you to update the deployment server to version 9.0 and Configure authentication for deployment servers and clients (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/ConfigDSDCAuthEnhancements#Configure_authentication_for_deployment_servers_and_clients). Once enabled, deployment servers can manage only Universal Forwarder versions 9.0 and higher. Though the vulnerability does not directly affect Universal Forwarders, remediation requires updating all Universal Forwarders that the deployment server manages to version 9.0 or higher prior to enabling the remediation.

CVE Number	Description
CVE-2022-32155	In universal forwarder versions before 9.0, management services are available remotely by default. When not required, it introduces a potential exposure, but it is not a vulnerability. If exposed, we recommend each customer assess the potential severity specific to your environment. In 9.0, the universal forwarder now binds the management port to localhost preventing remote logins by default. If management services are not required in versions before 9.0, set disableDefaultPort = true in server.conf OR allowRemoteLogin = never in server.conf OR mgmtHostPort = localhost in web.conf. See Configure universal forwarder management security (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation#Configure_universal_forwarder_management_security) for more information on disabling the remote management services.
CVE-2021-45918	NHI's health insurance web service component has insufficient validation for input string length, which can result in heap-based buffer overflow attack. A remote attacke can exploit this vulnerability to flood the memory space reserved for the program, in order to terminate service without authentication, which requires a system restart to recover service.
CVE-2022-20168	Product: AndroidVersions: Android kernelAndroid ID: A-210594998References: N/A
CVE-2022-20209	In hme_add_new_node_to_a_sorted_array of hme_utils.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-2075023
CVE-2022-20131	In nci_proc_rf_management_ntf of nci_hrcv.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221856662
CVE-2021-41490	Memory leaks in LazyPRM.cpp of OMPL v1.5.0 can cause unexpected behavior.
CVE-2022-1642	A program using swift-corelibs-foundation is vulnerable to a denial of service attack caused by a potentially malicious source producing a JSON document containing a type mismatch. This vulnerability is caused by the interaction between a deserialization mechanism offered by the Swift standard library, the Codable protocol; and the JSONDecoder class offered by swift-corelibs-foundation, which can deserialize types that adopt the Codable protocol based on the content of a provided JSON document. When a type that adopts Codable requests the initialization of a field with an integer value, the JSONDecoder class uses a type-erased container with different accessor methods to attempt and coerce a corresponding JSON value and produce an integer. In the case the JSON value was a numeric literal with a floating point portion, JSONDecoder used different type-eraser methods during validation than it did during the final casting of the value. The checked casting produces a deterministic crash due to this mismatch. The JSONDecoder class is often wrapped by popular Swift-based web frameworks to parse the body of HTTP requests and perform basic type validation. This makes the attack low-effort: sending a specifically crafted JSON document during a request to these endpoints will cause them to crash. The attack does not have any confidentiality or integrity risks in and of itself; the crash is produced deterministically by an abort function that ensures that execution does not continue in the face of this violation of assumptions. However, unexpected crashes can lead to violations of invariants in services, so it's possible tha this attack can be used to trigger error conditions that escalate the risk. Producing a denial of service may also be the goal of an attacker in itself. This issue is solved in Swift 5.6.2 for Linux and Windows. This issue was solved by ensuring that the same methods are invoked both when validating and during casting, so that no type mismatch occurs. Swift for Linux and Windows versions are not ABI-interchangeable. To upgrade a service, its owner must update to this version of the Swift toolchain, then recompile and redeploy their software. The new version of Swift includes an updated swift-corelibs-foundation package. Versions of Swift running on Darwin-based operating systems are not affected.
CVE-2021-40511	OBDA systems' Mastro 1.0 is vulnerable to XML Entity Expansion (aka "billion laughs") attack allowing denial of service.
CVE-2021-40510	XML eXternal Entity (XXE) in OBDA systems' Mastro 1.0 allows remote attackers to read system files via custom DTDs.
CVE-2022-1801	The Very Simple Contact Form WordPress plugin before 11.6 exposes the solution to the captcha in the rendered contact form, both as hidden input fields and as plain text in the page, making it very easy for bots to bypass the captcha check, rendering the page a likely target for spam bots.
CVE-2022-1614	The WP-EMail WordPress plugin before 2.69.0 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based anti-spamming restrictions.
CVE-2022-20123	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221852424
CVE-2021-45025	ASG technologies (A Rocket Software Company) ASG-Zena Cross Platform Server Enterprise Edition 4.2.1 is vulnerable to Cleartext Storage of Sensitive Information a Cookie.
CVE-2022-20149	Product: AndroidVersions: Android kernelAndroid ID: A-211685939References: N/A
CVE-2022-21935	A vulnerability in Metasys ADS/ADX/OAS 10 versions prior to 10.1.5 and Metasys ADS/ADX/OAS 11 versions prior to 11.0.2 allows unverified password change.

CVE Number	Description
CVE-2022-32276	Grafana 8.4.3 allows unauthenticated access via (for example) a /dashboard/snapshot/*?orgId=0 URI. NOTE: the vendor considers this a UI bug, not a vulnerability
CVE-2022-20817	A vulnerability in Cisco Unified IP Phones could allow an unauthenticated, remote attacker to impersonate another user's phone if the Cisco Unified Communications Manager (CUCM) is in secure mode. This vulnerability is due to improper key generation during the manufacturing process that could result in duplicated manufactured keys installed on multiple devices. An attacker could exploit this vulnerability by performing a machine-in-the-middle attack on the secure communication between the phone and the CUCM. A successful exploit could allow the attacker to impersonate another user's phone. This vulnerability cannot be addressed with software updates There is a workaround that addresses this vulnerability.
CVE-2022-32151	The httplib and urllib Python libraries that Splunk shipped with Splunk Enterprise did not validate certificates using the certificate authority (CA) certificate stores by default in Splunk Enterprise versions before 9.0 and Splunk Cloud Platform versions before 8.2.2203. Python 3 client libraries now verify server certificates by default and use the appropriate CA certificate stores for each library. Apps and add-ons that include their own HTTP libraries are not affected. For Splunk Enterprise, update to Splunk Enterprise version 9.0 and Configure TLS host name validation for Splunk-to-Splunk communications (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation) to enable the remediation.
CVE-2021-39691	In WindowManager, there is a possible tapjacking attack due to an incorrect window flag when processing user input. This could lead to local escalation of privilege witl no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-157929241
CVE-2014-125020	A vulnerability has been found in FFmpeg 2.0 and classified as critical. This vulnerability affects the function decode_update_thread_context. The manipulation leads to memory corruption. The attack can be initiated remotely. It is recommended to apply a patch to fix this issue.
CVE-2017-20067	A vulnerability was found in Hindu Matrimonial Script. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/. The manipulation of the argument username/password with the input 'or''=' leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-31219	Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist. The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.
CVE-2014-125015	A vulnerability classified as critical has been found in FFmpeg 2.0. Affected is the function read_var_block_data. The manipulation leads to memory corruption. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125024	A vulnerability was found in FFmpeg 2.0. It has been rated as critical. Affected by this issue is the function lag_decode_frame. The manipulation leads to memory corruption. The attack may be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125017	A vulnerability classified as critical was found in FFmpeg 2.0. This vulnerability affects the function rpza_decode_stream. The manipulation leads to memory corruption. The attack can be initiated remotely. The name of the patch is Fixes Invalid Writes. It is recommended to apply a patch to fix this issue.
CVE-2022-20193	In getUniqueUsagesWithLabels of PermissionUsageHelper.java, there is a possible incorrect permission attribution due to a logic error in the code. This could lead to local escalation of privilege by conflating apps with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-212434116
CVE-2022-26668	ASUS Control Center API has a broken access control vulnerability. An unauthenticated remote attacker can call privileged API functions to perform partial system operations or cause partial disrupt of service.
CVE-2022-20126	In setScanMode of AdapterService.java, there is a possible way to enable Bluetooth discovery mode without user interaction due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-203431023
CVE-2022-20137	In onCreateContextMenu of NetworkProviderSettings.java, there is a possible way for non-owner users to change WiFi settings due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-206986392
CVE-2022-1939	The Allow svg files WordPress plugin before 1.1 does not properly validate uploaded files, which could allow high privilege users such as admin to upload PHP files eve when they are not allowed to
CVE-2022-1472	The Better Find and Replace WordPress plugin before 1.3.6 does not properly sanitise, validate and escape various parameters before using them in an SQL statemer leading to an SQL Injection
CVE-2022-31912	Online Tutor Portal Site v1.0 is vulnerable to SQL Injection via /otps/classes/Master.php?f=delete_team.
CVE-2022-31911	Online Discussion Forum Site v1.0 is vulnerable to SQL Injection via /odfs/classes/Master.php?f=delete_team.

CVE Number	Description
CVE-2022-31908	Student Registration and Fee Payment System v1.0 is vulnerable to SQL Injection via /scms/student.php.
CVE-2019-12359	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /admin/ztliuyan_sendmail.php (when the attacker has admin authority) via the id parameter.
CVE-2019-12357	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /admin/deluser.php (when the attacker has admin authority) via the id parameter.
CVE-2022-32433	itsourcecode Advanced School Management System v1.0 is vulnerable to Arbitrary code execution via ip/school/view/all_teacher.php.
CVE-2022-32380	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_student_subject.php?index=.
CVE-2022-32375	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_timetable.php?id=.
CVE-2022-32381	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_admin_profile.php?my_index=.
CVE-2022-32370	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_classroom.php?id=.
CVE-2022-32371	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_teacher.php?id=.
CVE-2022-32372	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_subject.php?id=.
CVE-2022-32379	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_parents_profile.php?my_index=.
CVE-2022-33056	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/schedules/manage_schedule.php.
CVE-2022-32378	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_teacher_profile.php?my_index=.
CVE-2022-33055	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/trains/manage_train.php.
CVE-2022-32377	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_exam_timetable.php?id=.
CVE-2022-32374	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_subject_routing.php?id=.
CVE-2022-32376	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_events.php?event_id=.
CVE-2022-32373	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_exam.php?id=.
CVE-2022-32368	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via /school/model/get_grade.php?id=.

CVE Number	Description
CVE-2019-12353	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /admin/dl_sendmail.php (when the attacker has admin authority) via the id parameter.
CVE-2019-12354	An issue was discovered in zzcms 2019. There is a SQL injection Vulnerability in /admin/showbad.php (when the attacker has admin authority) via the id parameter.
CVE-2022-33049	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/?page=user/manage_user.
CVE-2022-32992	Online Tours And Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the tname parameter at /admin/operations/tax.php.
CVE-2022-33048	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/reservations/view_details.php.
CVE-2022-22788	The Zoom Opener installer is downloaded by a user from the Launch meeting page, when attempting to join a meeting without having the Zoom Meeting Client installed The Zoom Opener installer for Zoom Client for Meetings before version 5.10.3 and Zoom Rooms for Conference Room for Windows before version 5.10.3 are susceptible to a DLL injection attack. This vulnerability could be used to run arbitrary code on the victims host.
CVE-2022-20141	In ip_check_mc_rcu of igmp.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege when opening and closing inet sockets with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-112551163References: Upstream kernel
CVE-2022-30151	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2022-33915	Versions of the Amazon AWS Apache Log4j hotpatch package before log4j-cve-2021-44228-hotpatch-1.3.5 are affected by a race condition that could lead to a local privilege escalation. This Hotpatch package is not a replacement for updating to a log4j version that mitigates CVE-2021-44228 or CVE-2021-45046; it provides a temporary mitigation to CVE-2021-44228 by hotpatching the local Java virtual machines. To do so, it iterates through all running Java processes, performs several checks, and executes the Java virtual machine with the same permissions and capabilities as the running process to load the hotpatch. A local user could cause the hotpatch script to execute a binary with elevated privileges by running a custom java process that performs exec() of an SUID binary after the hotpatch has observed th process path and before it has observed its effective user ID.
CVE-2022-20155	In ipu_core_jqs_msg_transport_kernel_write_sync of ipu-core-jqs-msg-transport.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID A-176754369References: N/A
CVE-2022-20125	In GBoard, there is a possible way to bypass factory reset protections due to a sandbox escape. This could lead to local escalation of privilege if an attacker has physic access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-194402515
CVE-2022-32154	Dashboards in Splunk Enterprise versions before 9.0 might let an attacker inject risky search commands into a form token when the token is used in a query in a cross-origin request. The result bypasses SPL safeguards for risky commands. See New capabilities can limit access to some custom and potentially risky commands (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/SPLsafeguards#New_capabilities_can_limit_access_to_some_custom_and_potentially_risky_command for more information. Note that the attack is browser-based and an attacker cannot exploit it at will.
CVE-2022-20153	In rcu_cblist_dequeue of rcu_segcblist.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222091980References: Upstream kernel
CVE-2022-20152	In the TitanM chip, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privilege needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-202006198References: N/A
CVE-2022-20233	In param_find_digests_internal and related functions of the Titan-M source, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID A-222472803References: N/A
CVE-2022-20201	In getAppSize of InstalldNativeService.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-220733817
CVE-2022-20166	In various methods of kernel base drivers, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-182388481References: Upstream kernel
CVE-2022-30137	Executive Summary An Elevation of Privilege (EOP) vulnerability has been identified within Service Fabric clusters that run Docker containers. Exploitation of this EOP vulnerability requires an attacker to gain remote code execution within a container. All Service Fabric and Docker versions are impacted.

CVE Number	Description
CVE-2022-26057	Vulnerabilities in the Mint WorkBench allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist. The Mint WorkBench installer file allows a low-privileged user to run a "repair" operation on the product
CVE-2022-20185	In TBD of TBD, there is a possible use after free bug. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-208842348References: N/A
CVE-2022-20183	In hypx_create_blob_dmabuf of faceauth_hypx.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-188911154References N/A
CVE-2022-20178	In ioctl_dpm_qos_update and ioctl_event_control_set of (TBD), there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-224932775References: N/A
CVE-2022-2134	Allocation of Resources Without Limits or Throttling in GitHub repository inventree/inventree prior to 0.8.0.
CVE-2022-30328	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The username and password setup for the web interface does not require entering the existing password. A malicious user can change the username and password of the interface.
CVE-2022-1832	The CaPa Protect WordPress plugin through 0.5.8.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and disable the applied protection.
CVE-2021-25121	The Rating by BestWebSoft WordPress plugin before 1.6 does not validate the submitted rating, allowing submission of long integer, causing a Denial of Service on the post/page when a user submit such rating
CVE-2021-46823	python-ldap before 3.4.0 is vulnerable to a denial of service when ldap.schema is used for untrusted schema definitions, because of a regular expression denial of service (ReDoS) flaw in the LDAP schema parser. By sending crafted regex input, a remote authenticated attacker could exploit this vulnerability to cause a denial of service condition.
CVE-2022-1831	The WPlite WordPress plugin through 1.3.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack
CVE-2022-1610	The Seamless Donations WordPress plugin before 5.1.9 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged admin change them via a CSRF attack
CVE-2022-1830	The Amazon Einzeltitellinks WordPress plugin through 1.3.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping
CVE-2022-31294	An issue in the save_users() function of Online Discussion Forum Site 1 allows unauthenticated attackers to arbitrarily create or update user accounts.
CVE-2022-1828	The PDF24 Articles To PDF WordPress plugin through 4.2.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack
CVE-2022-1630	The WP-EMail WordPress plugin before 2.69.0 does not protect its log deletion functionality with nonce checks, allowing attacker to make a logged in admin delete logs via a CSRF attack
CVE-2022-30327	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The web interface is vulnerable to CSRF. An attacker can change the pre-shared key of th Wi-Fi router if the interface's IP address is known.
CVE-2022-30607	IBM Robotic Process Automation 20.10.0, 20.12.5, 21.0.0, 21.0.1, and 21.0.2 contains a vulnerability that could allow a user to obtain sensitive information due to information properly masked in the control center UI. IBM X-Force ID: 227294.
CVE-2022-23071	In Recipes, versions 0.9.1 through 1.2.5 are vulnerable to Server Side Request Forgery (SSRF), in the “Import Recipe” functionality. When an attacker enters the localhost URL, a low privileged attacker can access/read the internal file system to access sensitive information.
CVE-2022-1829	The Inline Google Maps WordPress plugin through 5.11 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged i admin change them via a CSRF attack, and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping

CVE Number	Description
CVE-2022-34000	libjxl 0.6.1 has an assertion failure in LowMemoryRenderPipeline::Init() in render_pipeline/low_memory_render_pipeline.cc.
CVE-2022-1826	The Cross-Linker WordPress plugin through 3.0.1.9 does not have CSRF check in place when creating Cross-Links, which could allow attackers to make a logged in admin perform such action via a CSRF attack
CVE-2022-20819	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability exists because administrative privilege levels for sensitive data are not properly enforced. An attacker with read-only privileges for the web-based management interface on an affected device could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information about the system configuration.
CVE-2022-1827	The PDF24 Article To PDF WordPress plugin through 4.2.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack
CVE-2022-23823	A potential vulnerability in some AMD processors using frequency scaling may allow an authenticated attacker to execute a timing attack to potentially enable informati disclosure.
CVE-2022-22953	VMware HCX update addresses an information disclosure vulnerability. A malicious actor with network user access to the VMware HCX appliance may be able to gain access to sensitive information.
CVE-2022-1596	Incorrect Permission Assignment for Critical Resource vulnerability in ABB REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch ar attack against the user database file and try to take control of an affected system node.
CVE-2022-32974	An authenticated attacker could read arbitrary files from the underlying operating system of the scanner using a custom crafted compliance audit file without providing any valid SSH credentials.
CVE-2022-30189	Windows Autopilot Device Management and Enrollment Client Spoofing Vulnerability
CVE-2022-24436	Observable behavioral in power management throttling for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via network access.
CVE-2022-28749	Zooms On-Premise Meeting Connector MMR before version 4.8.113.20220526 fails to properly check the permissions of a Zoom meeting attendee. As a result, a threa actor in the Zooms waiting room can join the meeting without the consent of the host.
CVE-2022-20202	In ih264_resi_trans_quant_4x4_sse42 of ih264_resi_trans_quant_sse42.c, there is a possible out of bounds read 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-12LAndroid ID: A-204704614
CVE-2021-41672	PEEL Shopping CMS 9.4.0 is vulnerable to authenticated SQL injection in utilisateurs.php. A user that belongs to the administrator group can inject a malicious SQL query in order to affect the execution logic of the application and retrive information from the database.
CVE-2022-20154	In lock_sock_nested of sock.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174846563References: Upstream kernel
CVE-2022-20148	In TBD of TBD, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-219513976References: Upstream kernel
CVE-2017-20064	A vulnerability was found in Elefant CMS 1.3.12-RC. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /designer/add/layout. The manipulation leads to code injection. The attack can be launched remotely. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20081	A vulnerability, which was classified as critical, was found in Hindu Matrimonial Script. This affects an unknown part of the file /admin/reports.php. The manipulation leads to improper privilege management. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2018-25040	A vulnerability was found in uTorrent Web. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component HTTP RPC Serve The manipulation leads to privilege escalation. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.
CVE-2017-20051	A vulnerability was found in InnoSetup Installer. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads t uncontrolled search path. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.

CVE Number	Description
CVE-2018-25041	A vulnerability was found in uTorrent. It has been rated as critical. Affected by this issue is some unknown functionality of the component JSON RPC Server. The manipulation leads to privilege escalation. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.
CVE-2018-25044	A vulnerability, which was classified as critical, has been found in uTorrent. This issue affects some unknown processing of the component Guest Account. The manipulation leads to privilege escalation. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.
CVE-2022-1958	A vulnerability classified as critical has been found in FileCloud. Affected is an unknown function of the component NTFS Handler. The manipulation leads to improper access controls. It is possible to launch the attack remotely. Upgrading to version 21.3.5.18513 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-201960.
CVE-2017-20063	A vulnerability was found in Elefant CMS 1.3.12-RC. It has been classified as critical. Affected is an unknown function of the file /filemanager/upload/drop of the component File Upload. The manipulation leads to improper privilege management. It is possible to launch the attack remotely. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20069	A vulnerability classified as critical has been found in Hindu Matrimonial Script. This affects an unknown part of the file /admin/countrymanagement.php. The manipulation leads to improper privilege management. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20070	A vulnerability classified as critical was found in Hindu Matrimonial Script. This vulnerability affects unknown code of the file /admin/communitymanagement.php. The manipulation leads to improper privilege management. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20076	A vulnerability was found in Hindu Matrimonial Script. It has been declared as critical. This vulnerability affects unknown code of the file /admin/searchview.php. The manipulation leads to improper privilege management. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20074	A vulnerability was found in Hindu Matrimonial Script and classified as critical. Affected by this issue is some unknown functionality of the file /admin/newsletter1.php. The manipulation leads to improper privilege management. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20072	A vulnerability, which was classified as critical, was found in Hindu Matrimonial Script. Affected is an unknown function of the file /admin/generalsettings.php. The manipulation leads to improper privilege management. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20071	A vulnerability, which was classified as critical, has been found in Hindu Matrimonial Script. This issue affects some unknown processing of the file /admin/renewaldue.php. The manipulation leads to improper privilege management. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-2086	A vulnerability, which was classified as critical, has been found in SourceCodester Bank Management System 1.0. Affected by this issue is login.php. The manipulation of the argument password with the input 1'and 1=2 union select 1,sleep(10),3,4,5 --+ leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20077	A vulnerability was found in Hindu Matrimonial Script. It has been rated as critical. This issue affects some unknown processing of the file /admin/success_story.php. Th manipulation leads to improper privilege management. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20068	A vulnerability was found in Hindu Matrimonial Script. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/usermanagement.php. The manipulation leads to improper privilege management. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20075	A vulnerability was found in Hindu Matrimonial Script. It has been classified as critical. This affects an unknown part of the file /admin/payment.php. The manipulation leads to improper privilege management. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20078	A vulnerability classified as critical has been found in Hindu Matrimonial Script. Affected is an unknown function of the file /admin/featured.php. The manipulation leads improper privilege management. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20079	A vulnerability classified as critical was found in Hindu Matrimonial Script. Affected by this vulnerability is an unknown functionality of the file /admin/photo.php. The manipulation leads to improper privilege management. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20073	A vulnerability has been found in Hindu Matrimonial Script and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/cms.php. The manipulation leads to improper privilege management. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20080	A vulnerability, which was classified as critical, has been found in Hindu Matrimonial Script. Affected by this issue is some unknown functionality of the file /admin/googleads.php. The manipulation leads to improper privilege management. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-21742	Realtek USB driver has a buffer overflow vulnerability due to insufficient parameter length verification in the API function. An unauthenticated LAN attacker can exploit this vulnerability to disrupt services.

CVE Number	Description
CVE-2022-31873	Trendnet IP-110wn camera fw_tv-ip110wn_v2(1.2.2.68) has an XSS vulnerability via the prefix parameter in /admin/general.cgi.
CVE-2022-31299	Haraj v3.7 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in the User Upgrade Form.
CVE-2022-32442	u5cms version 8.3.5 is vulnerable to Cross Site Scripting (XSS). When a user accesses the default home page if the parameter passed in is http://127.0.0.1/?"Onmouseover=%27tzgl (96502)%27bad=", it can cause html injection.
CVE-2021-40776	Adobe Lightroom Classic 10.3 (and earlier) are affected by a privilege escalation vulnerability in the Offline Lightroom Classic installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User interaction is required before product installation to abuse this vulnerability.
CVE-2021-41415	Subscription-Manager v1.0 /main.js has a cross-site scripting (XSS) vulnerability in the machineDetail parameter.
CVE-2022-31875	Trendnet IP-110wn camera fw_tv-ip110wn_v2(1.2.2.68) has an xss vulnerability via the proname parameter in /admin/scheprofile.cgi
CVE-2021-40910	There is a reflective cross-site scripting (XSS) vulnerability in the PHPCMS V9.6.3 management side.
CVE-2022-31373	SolarView Compact v6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component Solar_AiConf.php.
CVE-2021-45026	ASG technologies ASG-Zena Cross Platform Server Enterprise Edition 4.2.1 is vulnerable to Cross Site Scripting (XSS).
CVE-2022-33119	NUUO Network Video Recorder NVRsolo v03.06.02 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via login.php.
CVE-2021-36901	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability in Phil Baker's Age Gate plugin <= 2.17.0 at WordPress.
CVE-2022-31786	IdeaLMS 2022 allows reflected Cross Site Scripting (XSS) via the IdeaLMS/Class/Assessment/ PATH_INFO.
CVE-2022-2130	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.17.
CVE-2022-31734	Cisco Catalyst 2940 Series Switches provided by Cisco Systems, Inc. contain a reflected cross-site scripting vulnerability regarding error page generation. An arbitrary script may be executed on the web browser of the user who is using the product. The affected firmware is prior to 12.2(50)SY released in 2011, and Cisco Catalyst 294 Series Switches have been retired since January 2015
CVE-2021-25104	The Ocean Extra WordPress plugin before 1.9.5 does not escape generated links which are then used when the OceanWP is active, leading to a Reflected Cross-Site Scripting issue
CVE-2021-41924	Webkul krayin crm before 1.2.2 is vulnerable to Cross Site Scripting (XSS).
CVE-2022-32444	An issue was discovered in u5cms verion 8.3.5 There is a URL redirection vulnerability that can cause a user's browser to be redirected to another site via /loginsave.php.
CVE-2020-36547	A vulnerability was found in GE Voluson S8. It has been rated as critical. This issue affects the Service Browser which itroduces hard-coded credentials. Attacking local is a requirement. It is recommended to change the configuration settings.
CVE-2022-21184	An information disclosure vulnerability exists in the License registration functionality of Bachmann Visutec GmbH Atvise 3.5.4, 3.6 and 3.7. A plaintext HTTP request ca lead to a disclosure of login credentials. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.

CVE Number	Description
CVE-2022-25871	All versions of package querymen are vulnerable to Prototype Pollution if the parameters of exported function handler(type, name, fn) can be controlled by users withou any sanitization. Note: This vulnerability derives from an incomplete fix of [CVE-2020-7600](https://security.snyk.io/vuln/SNYK-JS-QUERYMEN-559867).
CVE-2022-23171	AtlasVPN - Privilege Escalation Lack of proper security controls on named pipe messages can allow an attacker with low privileges to send a malicious payload and ga SYSTEM permissions on a windows computer where the AtlasVPN client is installed.
CVE-2020-36548	A vulnerability classified as problematic has been found in GE Voluson S8. Affected is the file /uscgi-bin/users.cgi of the Service Browser. The manipulation leads to improper authentication and elevated access possibilities. It is possible to launch the attack on the local host.
CVE-2022-31069	NestJS Proxy is a NestJS module to decorate and proxy calls. Prior to version 0.7.0, the nestjs-proxy library did not have a way to control when Authorization headers should should be forwarded for specific backend services configured by the application developer. This could have resulted in sensitive information such as OAuth bearer access tokens being inadvertently exposed to such services that should not see them. A new feature has been introduced in the patched version of nestjs-proxy that allows application developers to opt out of forwarding the Authorization headers on a per service basis using the `forwardToken` config setting. Developers are advised to review the README for this library on Github or NPM for further details on how this configuration can be applied. This issue has been fixed in version 0.7.0 o `@finastra/nestjs-proxy`. Users of `@ffdc/nestjs-proxy` are advised that this package has been deprecated and is no longer being maintained or receiving updates. Suc users should update their package.json file to use `@finastra/nestjs-proxy` instead.
CVE-2022-31070	NestJS Proxy is a NestJS module to decorate and proxy calls. Prior to version 0.7.0, the nestjs-proxy library did not have a way to block sensitive cookies (e.g. session cookies) from being forwarded to backend services configured by the application developer. This could have led to sensitive cookies being inadvertently exposed to suc services that should not see them. The patched version now blocks cookies from being forwarded by default. However developers can configure an allow-list of cookie names by using the `allowedCookies` config setting. This issue has been fixed in version 0.7.0 of `@finastra/nestjs-proxy`. Users of `@ffdc/nestjs-proxy` are advised th this package has been deprecated and is no longer being maintained or receiving updates. Such users should update their package.json file to use `@finastra/nestjs-proxy` instead.
CVE-2022-20206	In setPackageOrComponentEnabled of NotificationManagerService.java, there is a missing permission check. This could lead to local information disclosure about enabled notification listeners with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A 220737634
CVE-2022-20172	In onbind of ShannonRcsService.java, there is a possible access to protect data 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 kernelAndroid ID: A-206987222References N/A
CVE-2022-20200	In updateApState of SoftApManager.java, there is a possible leak of hotspot state due to a missing permission check. This could lead to local information disclosure wit no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-212695058
CVE-2022-20205	In isFileUri of FileUtil.java, there is a possible way to bypass the check for a file:// scheme due to improper input validation. This could lead to local information disclosur with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-215212561
CVE-2022-21127	Incomplete cleanup in specific special register read operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosur via local access.
CVE-2022-21123	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21125	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-20129	In registerPhoneAccount of PhoneAccountRegistrar.java, there is a possible way to prevent the user from selecting a phone account due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-217934478
CVE-2022-22444	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a local user to exploit a vulnerability in the lpd daemon to cause a denial of service. IBM X-Force ID: 224444.
CVE-2021-46822	The PPM reader in libjpeg-turbo through 2.0.90 mishandles use of tjLoadImage for loading a 16-bit binary PPM file into a grayscale buffer and loading a 16-bit binary PGM file into an RGB buffer. This is related to a heap-based buffer overflow in the get_word_rgb_row function in rdppm.c.
CVE-2022-20143	In addAutomaticZenRule of ZenModeHelper.java, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-220735360
CVE-2022-20146	In uploadFile of FileUploadServiceImpl.java, there is a possible incorrect file access due to a confused deputy. This could lead to local information disclosure of private files with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-211757677References: N/A

CVE Number	Description
CVE-2021-3675	Improper Input Validation vulnerability in synaTEE.signed.dll of Synaptics Fingerprint Driver allows a local authorized attacker to overwrite a heap tag, with potential los of confidentiality. This issue affects: Synaptics Synaptics Fingerprint Driver 5.1.xxx.26 versions prior to xxx=340 on x86/64; 5.2.xxxx.26 versions prior to xxxx=3541 on x86/64; 5.2.2xx.26 versions prior to xx=29 on x86/64; 5.2.3xx.26 versions prior to xx=25 on x86/64; 5.3.xxxx.26 versions prior to xxxx=3543 on x86/64; 5.5.xx.1058 versions prior to xx=44 on x86/64; 5.5.xx.1102 versions prior to xx=34 on x86/64; 5.5.xx.1116 versions prior to xx=14 on x86/64; 6.0.xx.1104 versions prior to xx=50 on x86/64; 6.0.xx.1108 versions prior to xx=31 on x86/64; 6.0.xx.1111 versions prior to xx=58 on x86/64.
CVE-2022-31246	paymentrequest.py in Electrum before 4.2.2 allows a file:// URL in the r parameter of a payment request (e.g., within QR code data). On Windows, this can lead to capture of credentials over SMB. On Linux and UNIX, it can lead to a denial of service by specifying the /dev/zero filename.
CVE-2022-31307	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_string_offset at src/njs_string.c.
CVE-2022-30155	Windows Kernel Denial of Service Vulnerability
CVE-2022-30159	Microsoft Office Information Disclosure Vulnerability
CVE-2022-30162	Windows Kernel Information Disclosure Vulnerability
CVE-2022-30171	Microsoft Office Information Disclosure Vulnerability
CVE-2022-30669	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open malicious file.
CVE-2022-30668	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open malicious file.
CVE-2022-30172	Microsoft Office Information Disclosure Vulnerability
CVE-2022-30667	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open malicious file.
CVE-2022-30666	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open malicious file.
CVE-2022-30148	Windows Desired State Configuration (DSC) Information Disclosure Vulnerability
CVE-2022-31306	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_array_convert_to_slow_array at src/njs_array.c.
CVE-2022-30184	.NET and Visual Studio Information Disclosure Vulnerability
CVE-2022-28850	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker coul leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-21180	Improper input validation for some Intel(R) Processors may allow an authenticated user to potentially cause a denial of service via local access.
CVE-2021-41458	In GPAC MP4Box v1.1.0, there is a stack buffer overflow at src/utils/error.c:1769 which leads to a denial of service vulnerability.
CVE-2022-22414	IBM Robotic Process Automation 21.0.2 could allow a local user to obtain sensitive web service configuration credentials from system memory. IBM X-Force ID: 22302

CVE Number	Description
CVE-2022-2085	A NULL pointer dereference vulnerability was found in Ghostscript, which occurs when it tries to render a large number of bits in memory. When allocating a buffer device, it relies on an init_device_procs defined for the device that uses it as a prototype that depends upon the number of bits per pixel. For bpp > 64, mem_x_device i used and does not have an init_device_procs defined. This flaw allows an attacker to parse a large number of bits (more than 64 bits per pixel), which triggers a NULL pointer dereference flaw, causing an application to crash.
CVE-2022-21166	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosu via local access.
CVE-2022-32414	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_vmcode_interpreter at src/njs_vmcode.c.
CVE-2021-33295	Cross Site Scripting (XSS) vulnerability in Joplin Desktop App before 1.8.5 allows attackers to execute aribrary code due to improper sanitizing of html.
CVE-2022-28612	Improper Access Control vulnerability leading to multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in Muneeb's Custom Popup Builder plugin <= 1.3.1 at WordPress.
CVE-2022-29453	Cross-Site Request Forgery (CSRF) vulnerability in API KEY for Google Maps plugin <= 1.2.1 at WordPress leading to Google Maps API key update.
CVE-2022-29442	Authenticated (subscriber or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Messages For WordPress <= 2.1.10 at WordPress.
CVE-2022-29440	Multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in Promotion Slider plugin <= 3.3.4 at WordPress.
CVE-2022-29439	Cross-Site Request Forgery (CSRF) vulnerability in Image Slider by NextCode plugin <= 1.1.2 at WordPress allows deleting slides.
CVE-2022-29437	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Image Slider by NextCode plugin <= 1.1.2 at WordPress.
CVE-2021-36608	Cross Site Scripting (XSS) vulnerability in webTareas 2.2p1 via the Name field to /projects/editproject.php.
CVE-2022-30533	Cross-site scripting vulnerability in Modern Events Calendar Lite versions prior to 6.3.0 allows remote an authenticated attacker to inject an arbitrary script via unspecified vectors.
CVE-2022-31914	Zoo Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via zms/admin/public_html/save_animal?an_id=24.
CVE-2022-30874	There is a Cross Site Scripting Stored (XSS) vulnerability in NukeViet CMS before 4.5.02.
CVE-2022-31302	maccms8 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Server Group text field.
CVE-2022-31300	A cross-site scripting vulnerability in the DM Section component of Haraj v3.7 allows attackers to execute arbitrary web scripts or HTML via a crafted POST request.
CVE-2022-1818	The Multi-page Toolkit WordPress plugin through 2.6 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping as well
CVE-2022-31298	A cross-site scripting vulnerability in the ads comment section of Haraj v3.7 allows attackers to execute arbitrary web scripts or HTML via a crafted POST request.
CVE-2022-31303	maccms10 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Server Group text field.

CVE Number	Description
CVE-2022-31301	Haraj v3.7 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Post Ads component.
CVE-2021-36609	Cross Site Scripting (XSS) vulnerability in webTareas 2.2p1 via the Name field to /linkedcontent/editfolder.php.
CVE-2022-25585	Unioncms v1.0.13 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Default settings.
CVE-2022-32280	Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Xakuro's XO Slider plugin <= 3.3.2 at WordPress.
CVE-2022-2113	Cross-site Scripting (XSS) - Stored in GitHub repository inventree/inventree prior to 0.7.2.
CVE-2021-36891	Cross-Site Request Forgery (CSRF) vulnerability in Photo Gallery by Supsystic plugin <= 1.15.5 at WordPress allows changing the plugin settings.
CVE-2021-41420	A stored XSS vulnerability in MaianAffiliate v.1.0 allows an authenticated attacker for arbitrary JavaScript code execution in the context of authenticated and unauthenticated users through the MaianAffiliate admin panel.
CVE-2022-24004	A Stored Cross-Site Scripting (XSS) vulnerability was discovered in Messenger/messenger_ajax.php in REDCap 12.0.11. This issue allows any authenticated user to inject arbitrary code into the messenger title (aka new_title) field when editing an existing conversation. The payload executes in the browser of any conversation participant with the sidebar shown.
CVE-2022-24127	A Stored Cross-Site Scripting (XSS) vulnerability was discovered in ProjectGeneral/edit_project_settings.php in REDCap 12.0.11. This issue allows any user with proje management permissions to inject arbitrary code into the project title (app_title) field when editing an existing project. The payload is then reflected within the title tag of the page.
CVE-2022-29450	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Admin Management Xtended plugin <= 2.4.4 at WordPress.
CVE-2022-30326	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The network pre-shared key field on the web interface is vulnerable to XSS. An attacker can use a simple XSS payload to crash the basic.config page of the web interface.
CVE-2014-125014	A vulnerability classified as problematic was found in FFmpeg 2.0. Affected by this vulnerability is an unknown functionality of the component HEVC Video Decoder. Th manipulation leads to memory corruption. The attack can be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2022-33755	CA Automic Automation 12.2 and 12.3 contain an insecure input handling vulnerability in the Automic Agent that could allow a remote attacker to potentially enumerate users.
CVE-2022-27512	Temporary disruption of the ADM license service. The impact of this includes preventing new licenses from being issued or renewed by Citrix ADM.
CVE-2022-31876	netgear wnap320 router WNAP320_V2.0.3_firmware is vulnerable to Incorrect Access Control via /recreate.php, which can leak all users cookies.
CVE-2022-25872	All versions of package fast-string-search are vulnerable to Out-of-bounds Read due to incorrect memory freeing and length calculation for any non-string input as the source. This allows the attacker to read previously allocated memory.
CVE-2021-39006	IBM QRadar WinCollect Agent 10.0 and 10.0.1 could allow an attacker to obtain sensitive information due to missing best practices. IBM X-Force ID: 213549.
CVE-2022-32983	Knot Resolver through 5.5.1 may allow DNS cache poisoning when there is an attempt to limit forwarding actions by filters.
CVE-2014-125002	A vulnerability was found in FFmpeg 2.0. It has been classified as problematic. Affected is the function dnxhd_init_rc of the file libavcodec/dnxhdenc.c. The manipulatio leads to memory corruption. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue.

CVE Number	Description
CVE-2021-36761	The GeoAnalytics feature in Qlik Sense April 2020 patch 4 allows SSRF.
CVE-2017-20066	A vulnerability has been found in Adminer Login 1.4.4 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to improper acces controls. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.
CVE-2022-31062	### Impact A plugin public script can be used to read content of system files. ### Patches Upgrade to version 1.0.2. ### Workarounds `b/deploy/index.php` file can be deleted if deploy feature is not used.
CVE-2022-23342	The Hyland Onbase Application Server releases prior to 20.3.58.1000 and OnBase releases 21.1.1.1000 through 21.1.15.1000 are vulnerable to a username enumeration vulnerability. An attacker can obtain valid users based on the response returned for invalid and valid users by sending a POST login request to the /mobilebroker/ServiceToBroker.svc/Json/Connect endpoint. This can lead to user enumeration against the underlying Active Directory integrated systems.
CVE-2014-125016	A vulnerability was found in FFmpeg 2.0. It has been rated as problematic. This issue affects the function ff_init_buffer_info of the file utils.c. The manipulation leads to memory corruption. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue.
CVE-2022-33987	The got package before 12.1.0 (also fixed in 11.8.5) for Node.js allows a redirect to a UNIX socket.
CVE-2014-125003	A vulnerability was found in FFmpeg 2.0 and classified as problematic. This issue affects the function get_siz of the file libavcodec/jpeg2000dec.c. The manipulation leads to memory corruption. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125009	A vulnerability classified as problematic has been found in FFmpeg 2.0. This affects the function add_yblock of the file libavcodec/snow.h. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125019	A vulnerability, which was classified as problematic, was found in FFmpeg 2.0. This affects the function decode_nal_unit of the component Slice Segment Handler. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125022	A vulnerability was found in FFmpeg 2.0. It has been classified as problematic. Affected is the function shorten_decode_frame of the component Bitstream Buffer. The manipulation leads to memory corruption. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125018	A vulnerability, which was classified as problematic, has been found in FFmpeg 2.0. Affected by this issue is the function decode_slice_header. The manipulation leads to memory corruption. The attack may be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125012	A vulnerability was found in FFmpeg 2.0. It has been classified as problematic. Affected is an unknown function of the file libavcodec/dxtroy.c. The manipulation leads t integer coercion error. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125013	A vulnerability was found in FFmpeg 2.0 and classified as problematic. This issue affects the function msrle_decode_frame of the file libavcodec/msrle.c. The manipulation leads to memory corruption. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125023	A vulnerability was found in FFmpeg 2.0. It has been declared as problematic. Affected by this vulnerability is the function truemotion1_decode_header of the compone Truemotion1 Handler. The manipulation leads to memory corruption. The attack can be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125010	A vulnerability was found in FFmpeg 2.0. It has been rated as critical. Affected by this issue is the function decode_slice_header of the file libavcodec/h64.c. The manipulation leads to memory corruption. The attack may be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125025	A vulnerability classified as problematic has been found in FFmpeg 2.0. This affects the function decode_pulses. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125008	A vulnerability classified as problematic has been found in FFmpeg 2.0. Affected is the function vorbis_header of the file libavformat/oggparsevorbis.c. The manipulatio leads to memory corruption. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125011	A vulnerability was found in FFmpeg 2.0. It has been declared as problematic. Affected by this vulnerability is the function decode_frame of the file libavcodec/ansi.c. The manipulation leads to integer coercion error. The attack can be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125007	A vulnerability classified as problematic was found in FFmpeg 2.0. Affected by this vulnerability is the function intra_pred of the file libavcodec/hevcpred_template.c. Th manipulation leads to memory corruption. The attack can be launched remotely. It is recommended to apply a patch to fix this issue.

CVE Number	Description
CVE-2014-125006	A vulnerability, which was classified as problematic, has been found in FFmpeg 2.0. Affected by this issue is the function output_frame of the file libavcodec/h264.c. Th manipulation leads to memory corruption. The attack may be launched remotely. It is recommended to apply a patch to fix this issue.
CVE-2014-125005	A vulnerability, which was classified as problematic, was found in FFmpeg 2.0. This affects the function decode_vol_header of the file libavcodec/mpeg4videodec.c. Th manipulation leads to memory corruption. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue.
CVE-2022-20733	A vulnerability in the login page of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to log in without credentials and access all role without any restrictions. This vulnerability is due to exposed sensitive Security Assertion Markup Language (SAML) metadata. An attacker could exploit this vulnerabilit by using the exposed SAML metadata to bypass authentication to the user portal. A successful exploit could allow the attacker to access all roles without any restrictions.
CVE-2014-125004	A vulnerability has been found in FFmpeg 2.0 and classified as problematic. This vulnerability affects the function decode_hextile of the file libavcodec/vmnc.c. The manipulation leads to memory corruption. The attack can be initiated remotely. It is recommended to apply a patch to fix this issue.
CVE-2022-30154	Microsoft File Server Shadow Copy Agent Service (RVSS) Elevation of Privilege Vulnerability
CVE-2022-20736	A vulnerability in the web-based management interface of Cisco AppDynamics Controller Software could allow an unauthenticated, remote attacker to access a configuration file and the login page for an administrative console that they would not normally have authorization to access. This vulnerability is due to improper authorization checking for HTTP requests that are submitted to the affected web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected instance of AppDynamics Controller. A successful exploit could allow the attacker to access the login page for an administrative console. AppDynamics has released software updates that address this vulnerability.
CVE-2014-125021	A vulnerability was found in FFmpeg 2.0 and classified as problematic. This issue affects the function cmv_process_header. The manipulation leads to memory corruption. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue.
CVE-2018-25043	A vulnerability classified as critical was found in uTorrent. This vulnerability affects unknown code of the component PRNG. The manipulation leads to weak authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.
CVE-2022-20196	In gallery3d and photos, there is a possible permission bypass due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-201535148
CVE-2018-25042	A vulnerability classified as critical has been found in uTorrent. This affects an unknown part. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. It is recommended to upgrade the affected component.
CVE-2022-20195	In the keystore library, there is a possible prevention of access to system Settings due to unsafe deserialization. This could lead to local denial of service with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-213172664
CVE-2017-20052	A vulnerability classified as problematic was found in Python 2.7.13. This vulnerability affects unknown code of the component pgAdmin4. The manipulation leads to uncontrolled search path. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20062	A vulnerability was found in Elefant CMS 1.3.12-RC and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2022-21503	Vulnerability in the Oracle Cloud Infrastructure product of Oracle Cloud Services. Easily exploitable vulnerability allows high privileged attacker with network access to compromise Oracle Cloud Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to Oracle Cloud Infrastructure accessible data. All affected customers were notified of CVE-2022-21503 by Oracle. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N)
CVE-2022-1945	The Coming Soon & Maintenance Mode by Colorlib WordPress plugin before 1.0.99 does not sanitize and escape some settings, allowing high privilege users such as admin to perform Stored Cross-Site Scripting when unfiltered_html is disallowed (for example in multisite setup)
CVE-2022-1889	The Newsletter WordPress plugin before 7.4.6 does not escape and sanitise the preheader_text setting, which could allow high privilege users to perform Stored Cross Site Scripting attacks when the unfilteredhtml is disallowed
CVE-2022-1915	The WP Zillow Review Slider WordPress plugin before 2.4 does not escape a settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite)
CVE-2022-1896	The underConstruction WordPress plugin before 1.21 does not sanitise or escape the "Display a custom page using your own HTML" setting before outputting it, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiletred_html capability is disallowed.

CVE Number	Description
CVE-2022-31906	Online Fire Reporting System v1.0 is vulnerable to Cross Site Scripting (XSS) via /ofrs/classes/Master.php.
CVE-2022-1717	The Custom Share Buttons with Floating Sidebar WordPress plugin before 4.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed
CVE-2021-41421	A PHP code injection vulnerability in MaianAffiliate v.1.0 allows an authenticated attacker to gain RCE through the MaianAffiliate admin panel.
CVE-2021-36827	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Saturday Drive's Ninja Forms Contact Form plugin <= 3.6.9 at WordPress via "label".
CVE-2022-31910	Online Tutor Portal Site v1.0 is vulnerable to Cross Site Scripting (XSS). via /otps/classes/Master.php.
CVE-2022-32550	An issue was discovered in AgileBits 1Password, involving the method various 1Password apps and integrations used to create connections to the 1Password service. In specific circumstances, this issue allowed a malicious server to convince a 1Password app or integration it is communicating with the 1Password service.
CVE-2022-29438	Authenticated (author or higher user role) Persistent Cross-Site Scripting (XSS) vulnerability in Image Slider by NextCode plugin <= 1.1.2 at WordPress.
CVE-2022-31913	Online Discussion Forum Site v1.0 is vulnerable to Cross Site Scripting (XSS) via /odfs/classes/Master.php?f=save_category, name.
CVE-2022-1266	The Post Grid, Slider & Carousel Ultimate WordPress plugin before 1.5.0 does not sanitise and escape the Header Title, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-0663	The Print, PDF, Email by PrintFriendly WordPress plugin before 5.2.3 does not sanitise and escape the Custom Button Text settings, which could allow high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed
CVE-2021-25088	The XML Sitemaps WordPress plugin before 4.1.3 does not sanitise and escape a settings before outputting it in the Debug page, which could allow high privilege user to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)
CVE-2022-20132	In lg_probe and related functions of hid-lg.c and other USB HID files, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure if a malicious USB HID device were plugged in, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-188677105References: Upstream kernel
CVE-2022-1342	A lack of password masking in Devolutions Remote Desktop Manager allows physically proximate attackers to observe sensitive data. A caching issue can cause sensitive fields to sometimes stay revealed when closing and reopening a panel, which could lead to involuntarily disclosing sensitive information. This issue affects: Devolutions Remote Desktop Manager 2022.1.24 version and prior versions.
CVE-2022-20162	In asn1_p256_int of crypto/asn1.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-223492713References: N/A
CVE-2022-20165	In asn1_parse of asn1.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-220868345References: N/A
CVE-2022-20198	In llcp_dlc_proc_connect_pdu of llcp_dlc.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure from the NFC stack with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-22185187
CVE-2022-20208	In parseRecursively of cppbor_parse.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-192743373
CVE-2022-20159	In asn1_ec_pkey_parse of acropora/crypto/asn1_common.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-210971465References: N/A
CVE-2022-20182	In handle_ramdump of pixel_loader.c, there is a possible way to create a ramdump of non-secure memory due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222348453References: N/A

CVE Number	Description
CVE-2022-20176	In auth_store of sjtag-driver.c, there is a possible read of uninitialized memory due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-197787879References: N/A
CVE-2022-20174	In exynos_secEnv_init of mach-gs101.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-210847407References: N/A
CVE-2022-31478	The UserTakeOver plugin before 4.0.1 for ILIAS allows an attacker to list all users via the search function.
CVE-2022-1603	The Mail Subscribe List WordPress plugin before 2.1.4 does not have CSRF check in place when deleting subscribed users, which could allow attackers to make a logged in admin perform such action and delete arbitrary users from the subscribed list
CVE-2017-20053	A vulnerability was found in XYZScripts Contact Form Manager Plugin. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-29441	Cross-Site Request Forgery (CSRF) vulnerability in Private Messages For WordPress plugin <= 2.1.10 at WordPress allows attackers to send messages.
CVE-2022-31095	discourse-chat is a chat plugin for the Discourse application. Versions prior to 0.4 are vulnerable to an exposure of sensitive information, where an attacker who knows the message ID for a channel they do not have access to can view that message using the chat message lookup endpoint, primarily affecting direct message channels. There are no known workarounds for this issue, and users are advised to update the plugin.
CVE-2017-20061	A vulnerability has been found in Elefant CMS 1.3.12-RC and classified as problematic. This vulnerability affects unknown code of the file /admin/extended. The manipulation of the argument name with the input %3Cimg%20src=no%20onerror=alert(1)%3E leads to basic cross site scripting (Reflected). The attack can be initiate remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2022-1895	The underConstruction WordPress plugin before 1.20 does not have CSRF check in place when deactivating the construction mode, which could allow attackers to make a logged in admin perform such action via a CSRF attack
CVE-2017-20058	A vulnerability classified as problematic was found in Elefant CMS 1.3.12-RC. Affected by this vulnerability is an unknown functionality of the component Version Comparison. The manipulation leads to basic cross site scripting (Persistent). The attack can be launched remotely. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20057	A vulnerability classified as problematic has been found in Elefant CMS 1.3.12-RC. Affected is an unknown function. The manipulation of the argument username leads to basic cross site scripting (Persistent). It is possible to launch the attack remotely. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20065	A vulnerability was found in Supsystic Popup Plugin 1.7.6 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-29443	Multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in Nicdark's Hotel Booking plugin <= 3.0 at WordPress.
CVE-2022-27859	Multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in Nicdark d.o.o. Travel Management plugin <= 2.0 at WordPress.
CVE-2022-29406	Multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in DynamicWebLab's WordPress Team Manager plugin <= 1.6. at WordPress.
CVE-2022-2087	A vulnerability, which was classified as problematic, was found in SourceCodester Bank Management System 1.0. This affects the file /mnotice.php?id=2. The manipulation of the argument notice with the input <script>alert(1)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has beer disclosed to the public and may be used.
CVE-2017-20060	A vulnerability, which was classified as problematic, was found in Elefant CMS 1.3.12-RC. This affects an unknown part of the component Blog Post Handler. The manipulation leads to basic cross site scripting (Persistent). It is possible to initiate the attack remotely. Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20059	A vulnerability, which was classified as problematic, has been found in Elefant CMS 1.3.12-RC. Affected by this issue is some unknown functionality of the component Title Handler. The manipulation with the input </title><img src=no onerror=alert(1)> leads to basic cross site scripting (Persistent). The attack may be launched remotel Upgrading to version 1.3.13 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20056	A vulnerability was found in weblizar User Login Log Plugin 2.2.1. It has been classified as problematic. Affected is an unknown function. The manipulation leads to bas cross site scripting (Stored). It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

CVE Number	Description
CVE-2017-20055	A vulnerability classified as problematic has been found in BestWebSoft Contact Form Plugin 4.0.0. This affects an unknown part. The manipulation leads to basic cros site scripting (Stored). It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.0.2 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20054	A vulnerability was found in XYZScripts Contact Form Manager Plugin. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-29452	Authenticated (editor or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Export All URLs plugin <= 4.1 at WordPress.
CVE-2022-33981	drivers/block/floppy.c in the Linux kernel before 5.17.6 is vulnerable to a denial of service, because of a concurrency use-after-free flaw after deallocating raw_cmd in th raw_cmd_ioctl function.
CVE-2022-31072	Octokit is a Ruby toolkit for the GitHub API. Versions 4.23.0 and 4.24.0 of the octokit gem were published containing world-writeable files. Specifically, the gem was packed with files having their permissions set to `-rw-rw-rw-` (i.e. 0666) instead of `rw-r--r--` (i.e. 0644). This means everyone who is not the owner (Group and Public) with access to the instance where this release had been installed could modify the world-writable files from this gem. This issue is patched in Octokit 4.25.0. Two workarounds are available. Users can use the previous version of the gem, v4.22.0. Alternatively, users can modify the file permissions manually until they are able to upgrade to the latest version.
CVE-2022-31071	Octopoller is a micro gem for polling and retrying. Version 0.2.0 of the octopoller gem was published containing world-writeable files. Specifically, the gem was packed with files having their permissions set to `-rw-rw-rw-` (i.e. 0666) instead of `rw-r--r--` (i.e. 0644). This means everyone who is not the owner (Group and Public) with access to the instance where this release had been installed could modify the world-writable files from this gem. This issue is patched in Octopoller 0.3.0. Two workarounds are available. Users can use the previous version of the gem, v0.1.0. Alternatively, users can modify the file permissions manually until they are able to upgrade to the latest version.
CVE-2022-30664	Adobe Animate version 22.0.5 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30653	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30657	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the conte of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30655	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the conte of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30654	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code executio in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-1836	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-33981. Reason: This candidate is a reservation duplicate of CVE-2022-33981. Notes: All CVE users should reference CVE-2022-33981 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage
CVE-2017-20046	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This CVE has been rejected since it is out of scope in accordance to the Vulnerability Policy of Axis: https://www.axis.com/dam/public/76/fe/26/axis-vulnerability-management-policy-en-US-375421.pdf. Notes: none
CVE-2017-20047	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This CVE has been rejected as out of scope in accordance to the Vulnerabili Policy of Axis: https://www.axis.com/dam/public/76/fe/26/axis-vulnerability-management-policy-en-US-375421.pdf. Notes: none
CVE-2017-20048	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This CVE has been rejected since it is out of scope in accordance to the Vulnerability Policy of Axis: https://www.axis.com/dam/public/76/fe/26/axis-vulnerability-management-policy-en-US-375421.pdf. Notes: none
CVE-2017-20050	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This CVE has been rejected due to lack of sufficient information on how to reproduce the vulnerability. Notes: none
CVE-2022-30662	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28842	Adobe Bridge version 12.0.1 (and earlier versions) is affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE Number	Description
CVE-2022-28839	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30652	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30660	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30658	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30663	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30665	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30650	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code executio in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30651	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-23072	In Recipes, versions 1.0.5 through 1.2.5 are vulnerable to Stored Cross-Site Scripting (XSS), in “Add to Cart” functionality. When a victim accesses the food list page, then adds a new Food with a malicious javascript payload in the ‘Name’ parameter and clicks on the Add to Shopping Cart icon, an XSS payload will trigger. A low privileged attacker will have the victim's API key and can lead to admin's account takeover.
CVE-2022-23073	In Recipes, versions 1.0.5 through 1.2.5 are vulnerable to Stored Cross-Site Scripting (XSS), in copy to clipboard functionality. When a victim accesses the food list page, then adds a new Food with a malicious javascript payload in the ‘Name’ parameter and clicks on the clipboard icon, an XSS payload will trigger. A low privileged attacker will have the victim's API key and can lead to admin's account takeover.
CVE-2022-30648	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28840	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30647	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28848	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28847	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28846	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28845	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-28843	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-30661	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE Number	Description
CVE-2022-28841	Adobe Bridge version 12.0.1 (and earlier versions) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-23074	In Recipes, versions 0.17.0 through 1.2.5 are vulnerable to Stored Cross-Site Scripting (XSS), in the ‘Name’ field of Keyword, Food and Unit components. When a victi accesses the Keyword/Food/Unit endpoints, the XSS payload will trigger. A low privileged attacker will have the victim's API key and can lead to admin's account takeover.