SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 23 June 2021

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

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

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

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

## CRITICAL VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21777 | An information disclosure vulnerability exists in the Ethernet/IP UDP handler functionality of EIP Stack Group OpENer 2.3 and development commit 8c73bf3. A specially crafted network request can lead to an out-of-bounds read. | 10.0 | More Details |
| CVE-2021-34809 | Improper neutralization of special elements used in a command ('Command Injection') vulnerability in task management component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to execute arbitrary code via unspecified vectors. | 9.9 | More Details |
| CVE-2021-34810 | Improper privilege management vulnerability in cgi component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to execute arbitrary code via unspecified vectors. | 9.9 | More Details |
| CVE-2021-0516 | In p2p_process_prov_disc_req of p2p_pd.c, there is a possible out of bounds read and write due to a use after free. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181660448 | 9.8 | More Details |
| CVE-2021-21669 | Jenkins Generic Webhook Trigger Plugin 1.72 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. | 9.8 | More Details |
| CVE-2021-33576 | An issue was discovered in Cleo LexiCom 5.5.0.0. Within the AS2 message, the sender can specify a filename. This filename can include path-traversal characters, allowing the file to be written to an arbitrary location on disk. | 9.8 | More Details |
| CVE-2021-3604 | Secure 8 (Evalos) does not validate user input data correctly, allowing a remote attacker to perform a Blind SQL Injection. An attacker could exploit this vulnerability in order to extract information of users and administrator accounts stored in the database. | 9.8 | More Details |
| CVE-2021-31272 | SerenityOS before commit 3844e8569689dd476064a0759d704bc64fb3ca2c contains a directory traversal vulnerability in tar/unzip that may lead to command execution or privilege escalation. | 9.8 | More Details |
| CVE-2020-20466 | White Shark System (WSS) 1.3.2 is vulnerable to unauthorized access via user_edit_password.php, remote attackers can modify the password of any user. | 9.8 | More Details |
| CVE-2018-25016 | Greenbone Security Assistant (GSA) before 7.0.3 and Greenbone OS (GOS) before 5.0.0 allow Host Header Injection. | 9.8 | More Details |
| CVE-2021-32685 | tEnvoy contains the PGP, NaCl, and PBKDF2 in node.js and the browser (hashing, random, encryption, decryption, signatures, conversions), used by TogaTech.org. In versions prior to 7.0.3, the `verifyWithMessage` method of `tEnvoyNaClSigningKey` always returns `true` for any signature that has a SHA-512 hash matching the SHA-512 hash of the message even if the signature was invalid. This issue is patched in version 7.0.3. As a workaround: In `tenvoy.js` under the `verifyWithMessage` method definition within the `tEnvoyNaClSigningKey` class, ensure that the return statement call to `this.verify` ends in `.verified`. | 9.8 | More Details |
| CVE-2020-9493 | A deserialization flaw was found in Apache Chainsaw versions prior to 2.1.0 which could lead to malicious code execution. | 9.8 | More Details |
| CVE-2020-19510 | Textpattern 4.7.3 contains an aribtrary file load via the file_insert function in include/txp_file.php. | 9.8 | More Details |
| CVE-2021-24361 | In the Location Manager WordPress plugin before 2.1.0.10, the AJAX action gd_popular_location_list did not properly sanitise or validate some of its POST parameters, which are then used in a SQL statement, leading to unauthenticated SQL Injection issues. | 9.8 | More Details |
| CVE-2021-24370 | The Fancy Product Designer WordPress plugin before 4.6.9 allows unauthenticated attackers to upload arbitrary files, resulting in remote code execution. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-24376 | The Autoptimize WordPress plugin before 2.7.8 attempts to delete malicious files (such as .php) form the uploaded archive via the "Import Settings" feature, after its extraction. However, the extracted folders are not checked and it is possible to upload a zip which contained a directory with PHP file in it and then it is not removed from the disk. It is a bypass of CVE-2020-24948 which allows sending a PHP file via the "Import Settings" functionality to achieve Remote Code Execution. | 9.8 | More Details |
| CVE-2021-35066 | An XXE vulnerability exists in ConnectWise Automate before 2021.0.6.132. | 9.8 | More Details |
| CVE-2010-1433 | Joomla! Core is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly verify user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable. | 9.8 | More Details |
| CVE-2010-1435 | Joomla! Core is prone to a security bypass vulnerability. Exploiting this issue may allow attackers to perform otherwise restricted actions and subsequently retrieve password reset tokens from the database through an already existing SQL injection vector. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable. | 9.8 | More Details |
| CVE-2021-3044 | An improper authorization vulnerability in Palo Alto Networks Cortex XSOAR enables a remote unauthenticated attacker with network access to the Cortex XSOAR server to perform unauthorized actions through the REST API. This issue impacts: Cortex XSOAR 6.1.0 builds later than 1016923 and earlier than 1271064; Cortex XSOAR 6.2.0 builds earlier than 1271065. This issue does not impact Cortex XSOAR 5.5.0, Cortex XSOAR 6.0.0, Cortex XSOAR 6.0.1, or Cortex XSOAR 6.0.2 versions. All Cortex XSOAR instances hosted by Palo Alto Networks are upgraded to resolve this vulnerability. No additional action is required for these instances. | 9.8 | More Details |
| CVE-2021-26461 | Apache Nuttx Versions prior to 10.1.0 are vulnerable to integer wrap-around in functions malloc, realloc and memalign. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution. | 9.8 | More Details |
| CVE-2013-20002 | Elemin allows remote attackers to upload and execute arbitrary PHP code via the Themify framework (before 1.2.2) wp-content/themes/elemin/themify/themify-ajax.php file. | 9.8 | More Details |
| CVE-2020-25414 | A local file inclusion vulnerability was discovered in the captcha function in Monstra 3.0.4 which allows remote attackers to execute arbitrary PHP code. | 9.8 | More Details |
| CVE-2020-22205 | SQL Injection in ECShop 3.0 via the id parameter to admin/shophelp.php. | 9.8 | More Details |
| CVE-2021-32928 | The Sentinel LDK Run-Time Environment installer (Versions 7.6 and prior) adds a firewall rule named “Sentinel License Manager” that allows incoming connections from private networks using TCP Port 1947. While uninstalling, the uninstaller fails to close Port 1947. | 9.8 | More Details |
| CVE-2021-27610 | SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 804, does not create information about internal and external RFC user in consistent and distinguished format, which could lead to improper authentication and may be exploited by malicious users to obtain illegitimate access to the system. | 9.8 | More Details |
| CVE-2020-22198 | SQL Injection vulnerability in DedeCMS 5.7 via mdescription parameter to member/ajax_membergroup.php. | 9.8 | More Details |
| CVE-2020-35760 | bloofoxCMS 0.5.2.1 is infected with Unrestricted File Upload that allows attackers to upload malicious files (ex: php files). | 9.8 | More Details |
| CVE-2020-22199 | SQL Injection vulnerability in phpCMS 2007 SP6 build 0805 via the digg_mod parameter to digg_add.php. | 9.8 | More Details |
| CVE-2020-22203 | SQL Injection in phpCMS 2008 sp4 via the genre parameter to yp/job.php. | 9.8 | More Details |
| CVE-2020-25753 | An issue was discovered on Enphase Envoy R3.x and D4.x devices with v3 software. The default admin password is set to the last 6 digits of the serial number. The serial number can be retrieved by an unauthenticated user at /info.xml. | 9.8 | More Details |
| CVE-2020-22204 | SQL Injection in ECShop 2.7.6 via the goods_number parameter to flow.php. . | 9.8 | More Details |
| CVE-2020-22206 | SQL Injection in ECShop 3.0 via the aid parameter to admin/affiliate_ck.php. | 9.8 | More Details |
| CVE-2020-22208 | SQL Injection in 74cms 3.2.0 via the x parameter to plus/ajax_street.php. | 9.8 | More Details |
| CVE-2020-22209 | SQL Injection in 74cms 3.2.0 via the query parameter to plus/ajax_common.php. | 9.8 | More Details |
| CVE-2020-22210 | SQL Injection in 74cms 3.2.0 via the x parameter to ajax_officebuilding.php. | 9.8 | More Details |
| CVE-2020-22211 | SQL Injection in 74cms 3.2.0 via the key parameter to plus/ajax_street.php. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-22212 | SQL Injection in 74cms 3.2.0 via the id parameter to wap/wap-company-show.php. | 9.8 | More Details |
| CVE-2021-34813 | Matrix libolm before 3.2.3 allows a malicious Matrix homeserver to crash a client (while it is attempting to retrieve an Olm encrypted room key backup from the homeserver) because olm_pk_decrypt has a stack-based buffer overflow. Remote code execution might be possible for some nonstandard build configurations. | 9.8 | More Details |
| CVE-2021-20736 | NoSQL injection vulnerability in GROWI versions prior to v4.2.20 allows a remote attacker to obtain and/or alter the information stored in the database via unspecified vectors. | 9.1 | More Details |
| CVE-2021-20093 | A buffer over-read vulnerability exists in Wibu-Systems CodeMeter versions < 7.21a. An unauthenticated remote attacker can exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime Server. | 9.1 | More Details |
| CVE-2021-32700 | Ballerina is an open source programming language and platform for cloud application programmers. Ballerina versions 1.2.x and SL releases up to alpha 3 have a potential for a supply chain attack via MiTM against users. Http connections did not make use of TLS and certificate checking was ignored. The vulnerability allows an attacker to substitute or modify packages retrieved from BC thus allowing to inject malicious code into ballerina executables. This has been patched in Ballerina 1.2.14 and Ballerina SwanLake alpha4. | 9.1 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-0557 | In setRange of ABuffer.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179046129 | 8.8 | More Deta |
| CVE-2020-25755 | An issue was discovered on Enphase Envoy R3.x and D4.x (and other current) devices. The upgrade_start function in /installer/upgrade_start allows remote authenticated users to execute arbitrary commands via the force parameter. | 8.8 | More Deta |
| CVE-2020-22201 | phpCMS 2008 sp4 allowas remote malicious users to execute arbitrary php commands via the pagesize parameter to yp/product.php. | 8.8 | More Deta |
| CVE-2020-22390 | Akaunting <= 2.0.9 is vulnerable to CSV injection in the Item name field, export function. Attackers can inject arbitrary code into the name parameter and perform code execution when the crafted file is opened. | 8.8 | More Deta |
| CVE-2021-32691 | Apollos Apps is an open source platform for launching church-related apps. In Apollos Apps versions prior to 2.20.0, new user registrations are able to access anyone's account by only knowing their basic profile information (name, birthday, gender, etc). This includes all app functionality within the app, as well as any authenticated links to Rock-based webpages (such as giving and events). There is a patch in version 2.20.0. As a workaround, one can patch one's server by overriding the `create` data source method on the `People` class. | 8.8 | More Deta |
| CVE-2021-31769 | MyQ Server in MyQ X Smart before 8.2 allows remote code execution by unprivileged users because administrative session data can be read in the %PROGRAMFILES%\MyQ\PHP\Sessions directory. The "Select server file" feature is only intended for administrators but actually does not require authorization. An attacker can inject arbitrary OS commands (such as commands to create new .php files) via the Task Scheduler component. | 8.8 | More Deta |
| CVE-2020-20471 | White Shark System (WSS) 1.3.2 has an unauthorized access vulnerability in default_user_edit.php, remote attackers can exploit this vulnerability to escalate to admin privileges. | 8.8 | More Deta |
| CVE-2021-23846 | When using http protocol, the user password is transmitted as a clear text parameter for which it is possible to be obtained by an attacker through a MITM attack. This will be fixed starting from Firmware version 3.11.5, which will be released on the 30th of June, 2021. | 8.8 | More Deta |
| CVE-2021-32424 | In TrendNet TW100-S4W1CA 2.3.32, due to a lack of proper session controls, a threat actor could make unauthorized changes to an affected router via a specially crafted web page. If an authenticated user were to interact with a malicious web page it could allow for a complete takeover of the router. | 8.8 | More Deta |
| CVE-2020-36388 | In CiviCRM before 5.21.3 and 5.22.x through 5.24.x before 5.24.3, users may be able to upload and execute a crafted PHAR archive. | 8.8 | More Deta |
| CVE-2021-0507 | In handle_rc_metamsg_cmd of btif_rc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181860042 | 8.8 | More Deta |
| CVE-2020-18648 | Cross Site Request Forgery (CSRF) in JuQingCMS v1.0 allows remote attackers to gain local privileges via the component "JuQingCMS_v1.0/admin/index.php?c=administrator&a=add". | 8.8 | More Deta |
| CVE-2021-34244 | A cross site request forgery (CSRF) vulnerability was discovered in Ice Hrm 29.0.0.OS which allows attackers to create new admin accounts or change users' passwords. | 8.8 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-32243 | FOGProject v1.5.9 is affected by a File Upload RCE (Authenticated). | 8.8 | More Deta |
| CVE-2021-27489 | ZOLL Defibrillator Dashboard, v prior to 2.2, The web application allows a non-administrative user to upload a malicious file. This file could allow an attacker to remotely execute arbitrary commands. | 8.8 | More Deta |
| CVE-2021-21280 | Contiki-NG is an open-source, cross-platform operating system for internet of things devices. It is possible to cause an out-of-bounds write in versions of Contiki-NG prior to 4.6 when transmitting a 6LoWPAN packet with a chain of extension headers. Unfortunately, the written header is not checked to be within the available space, thereby making it possible to write outside the buffer. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround. | 8.6 | More Deta |
| CVE-2021-21282 | Contiki-NG is an open-source, cross-platform operating system for internet of things devices. In versions prior to 4.5, buffer overflow can be triggered by an input packet when using either of Contiki-NG's two RPL implementations in source-routing mode. The problem has been patched in Contiki-NG 4.5. Users can apply the patch for this vulnerability out-of-band as a workaround. | 8.6 | More Deta |
| CVE-2021-34372 | Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. | 8.2 | More Deta |
| CVE-2021-21410 | Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. An out-of-bounds read can be triggered by 6LoWPAN packets sent to devices running Contiki-NG 4.6 and prior. The IPv6 header decompression function (<code>uncompress_hdr_iphc</code>) does not perform proper boundary checks when reading from the packet buffer. Hence, it is possible to construct a compressed 6LoWPAN packet that will read more bytes than what is available from the packet buffer. As of time of publication, there is not a release with a patch available. Users can apply the patch for this vulnerability out-of-band as a workaround. | 8.2 | More Deta |
| CVE-2021-21257 | Contiki-NG is an open-source, cross-platform operating system for internet of things devices. The RPL-Classic and RPL-Lite implementations in the Contiki-NG operating system versions prior to 4.6 do not validate the address pointer in the RPL source routing header This makes it possible for an attacker to cause out-of-bounds writes with packets injected into the network stack. Specifically, the problem lies in the rpl_ext_header_srh_update function in the two rpl-ext-header.c modules for RPL-Classic and RPL-Lite respectively. The addr_ptr variable is calculated using an unvalidated CMPR field value from the source routing header. An out-of-bounds write can be triggered on line 151 in os/net/routing/rpl-lite/rpl-ext-header.c and line 261 in os/net/routing/rpl-classic/rpl-ext-header.c, which contain the following memcpy call with addr_ptr as destination. The problem has been patched in Contiki-NG 4.6. Users can apply a patch out-of-band as a workaround. | 8.2 | More Deta |
| CVE-2021-34203 | D-Link DIR-2640-US 1.01B04 is vulnerable to Incorrect Access Control. Router ac2600 (dir-2640-us), when setting PPPoE, will start quagga process in the way of whole network monitoring, and this function uses the original default password and port. An attacker can easily use telnet to log in, modify routing information, monitor the traffic of all devices under the router, hijack DNS and phishing attacks. In addition, this interface is likely to be questioned by customers as a backdoor, because the interface should not be exposed. | 8.1 | More Deta |
| CVE-2021-32612 | The VeryFitPro (com.veryfit2hr.second) application 3.2.8 for Android does all communication with the backend API over cleartext HTTP. This includes logins, registrations, and password change requests. This allows information theft and account takeover via network sniffing. | 8.1 | More Deta |
| CVE-2021-32623 | Opencast is a free and open source solution for automated video capture and distribution. Versions of Opencast prior to 9.6 are vulnerable to the billion laughs attack, which allows an attacker to easily execute a (seemingly permanent) denial of service attack, essentially taking down Opencast using a single HTTP request. To exploit this, users need to have ingest privileges, limiting the group of potential attackers The problem has been fixed in Opencast 9.6. There is no known workaround for this issue. | 8.1 | More Deta |
| CVE-2021-21422 | mongo-express is a web-based MongoDB admin interface, written with Node.js and express. 1: As mentioned in this issue: https://github.com/mongo-express/mongo-express/issues/577, when the content of a cell grows larger than supported size, clicking on a row will show full document unescaped, however this needs admin interaction on cell. 2: Data cells identified as media will be rendered as media, without being sanitized. Example of different renders: image, audio, video, etc. As an example of type 1 attack, an unauthorized user who only can send a large amount of data in a field of a document may use a payload with embedded javascript. This could send an export of a collection to the attacker without even an admin knowing. Other types of attacks such as dropping a database\collection are possible. | 8.1 | More Deta |
| CVE-2021-24377 | The Autoptimize WordPress plugin before 2.7.8 attempts to remove potential malicious files from the extracted archive uploaded via the 'Import Settings' feature, however this is not sufficient to protect against RCE as a race condition can be achieved in between the moment the file is extracted on the disk but not yet removed. It is a bypass of CVE-2020-24948. | 8.1 | More Deta |
| CVE-2021-3603 | PHPMailer 6.4.1 and earlier contain a vulnerability that can result in untrusted code being called (if such code is injected into the host project's scope by other means). If the $patternselect parameter to validateAddress() is set to 'php' (the default, defined by PHPMailer::$validator), and the global namespace contains a function called php, it will be called in preference to the built-in validator of the same name. Mitigated in PHPMailer 6.5.0 by denying the use of simple strings as validator function names. | 8.1 | More Deta |
| CVE-2021-34551 | PHPMailer before 6.5.0 on Windows allows remote code execution if lang_path is untrusted data and has a UNC pathname. | 8.1 | More Deta |
| CVE-2021-23845 | This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. | 8.0 | More Deta |
| CVE-2021-0478 | In updateDrawable of StatusBarIconView.java, there is a possible permission bypass due to an uncaught exception. This could lead to local escalation of privilege by running foreground services without notifying the user, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-169255797 | 7.8 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-32946 | An improper check for unusual or exceptional conditions issue exists within the parsing DGN files from Drawings SDK (Version 2022.4 and prior) resulting from the lack of proper validation of the user-supplied data. This may result in several of out-of-bounds problems and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. | 7.8 | More Deta |
| CVE-2021-29337 | MODAPI.sys in MSI Dragon Center 2.0.104.0 allows low-privileged users to access kernel memory and potentially escalate privileges via a crafted IOCTL 0x9c406104 call. This IOCTL provides the MmMapIoSpace feature for mapping physical memory. | 7.8 | More Deta |
| CVE-2021-0143 | Improper permissions in the installer for the Intel(R) Brand Verification Tool before version 11.0.0.1225 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.8 | More Deta |
| CVE-2021-32952 | An out-of-bounds write issue exists in the DGN file-reading procedure in the Drawings SDK (Version 2022.4 and prior) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. | 7.8 | More Deta |
| CVE-2021-32948 | An out-of-bounds write issue exists in the DWG file-reading procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. | 7.8 | More Deta |
| CVE-2021-32936 | An out-of-bounds write issue exists in the DXF file-recovering procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. | 7.8 | More Deta |
| CVE-2021-32944 | A use-after-free issue exists in the DGN file-reading procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a memory corruption or arbitrary code execution, allowing attackers to cause a denial-of-service condition or execute code in the context of the current process. | 7.8 | More Deta |
| CVE-2021-0512 | In __hidinput_change_resolution_multipliers of hid-input.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-173843328References: Upstream kernel | 7.8 | More Deta |
| CVE-2021-0505 | In the Settings app, there is a possible way to disable an always-on VPN 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-11Android ID: A-179975048 | 7.8 | More Deta |
| CVE-2021-0510 | In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-176444622 | 7.8 | More Deta |
| CVE-2021-0608 | In handleAppLaunch of AppLaunchActivity.java, there is a possible arbitrary activity launch due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174870704 | 7.8 | More Deta |
| CVE-2021-0607 | In iaxxx_calc_i2s_div of iaxxx-codec.c, there is a possible hardware port write with user controlled data 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 kernelAndroid ID: A-180950209 | 7.8 | More Deta |
| CVE-2021-0550 | In onLoadFailed of AnnotateActivity.java, there is a possible way to gain WRITE_EXTERNAL_STORAGE permissions without user consent due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179688673 | 7.8 | More Deta |
| CVE-2021-0548 | In rw_i93_send_to_lower of rw_i93.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-11Android ID: A-157650357 | 7.8 | More Deta |
| CVE-2021-0547 | In onReceive of NetInitiatedActivity.java, there is a possible way to supply an attacker-controlled value to a GPS HAL handler due to a missing permission check. This could lead to local escalation of privilege that may result in undefined behavior in some HAL implementations with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174151048 | 7.8 | More Deta |
| CVE-2021-0539 | In archiveStoredConversation of MmsService.java, there is a possible way to archive message conversation without user consent 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-11Android ID: A-180419673 | 7.8 | More Deta |
| CVE-2021-0536 | In dropFile of WiFiInstaller, there is a way to delete files accessible to CertInstaller due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176756691 | 7.8 | More Deta |
| CVE-2010-2525 | A flaw was discovered in gfs2 file system's handling of acls (access control lists). An unprivileged local attacker could exploit this flaw to gain access or execute any file stored in the gfs2 file system. | 7.8 | More Deta |
| CVE-2021-0571 | In ActivityTaskManagerService.startActivity() and AppTaskImpl.startActivity() of ActivityTaskManagerService.java and AppTaskImpl.java, there is possible access to restricted activities 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-11Android ID: A-137395936 | 7.8 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-0570 | In sendBugreportNotification of BugreportProgressService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-178803845 | 7.8 | More Deta |
| CVE-2021-0568 | In onReceive of DevicePolicyManagerService.java, there is a possible enabling of disabled profiles 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-11Android ID: A-170121238 | 7.8 | More Deta |
| CVE-2021-0567 | In isRestricted of RemoteViews.java, there is a possible way to inject font files 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-11Android ID: A-179461812 | 7.8 | More Deta |
| CVE-2021-0534 | In permission declarations of DeviceAdminReceiver.java, there is a possible lack of broadcast protection 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-11Android ID: A-170639543 | 7.8 | More Deta |
| CVE-2021-35196 | Manuskript through 0.12.0 allows remote attackers to execute arbitrary code via a crafted settings.pickle file in a project file, because there is insecure deserialization via the pickle.load() function in settings.py. NOTE: the vendor's position is that the product is not intended for opening an untrusted project file | 7.8 | More Deta |
| CVE-2021-0531 | In memory management driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195272 | 7.8 | More Deta |
| CVE-2021-0530 | In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185196175 | 7.8 | More Deta |
| CVE-2021-0529 | In memory management driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195268 | 7.8 | More Deta |
| CVE-2021-0528 | In memory management driver, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195266 | 7.8 | More Deta |
| CVE-2021-0527 | In memory management driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193931 | 7.8 | More Deta |
| CVE-2021-0526 | In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195264 | 7.8 | More Deta |
| CVE-2021-0525 | In memory management driver, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193929 | 7.8 | More Deta |
| CVE-2021-0513 | In deleteNotificationChannel and related functions of NotificationManagerService.java, there is a possible permission bypass due to improper state validation. This could lead to local escalation of privilege via hidden services with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-156090809 | 7.8 | More Deta |
| CVE-2021-0511 | In Dex2oat of dex2oat.cc, there is a possible way to inject bytecode into an app 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-9 Android-10 Android-11Android ID: A-178055795 | 7.8 | More Deta |
| CVE-2021-31476 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA templates. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13531. | 7.8 | More Deta |
| CVE-2021-22361 | There is an improper authorization vulnerability in eCNS280 V100R005C00, V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200. A file access is not authorized correctly. Attacker with low access may launch privilege escalation in a specific scenario. This may compromise the normal service. | 7.8 | More Deta |
| CVE-2021-27483 | ZOLL Defibrillator Dashboard, v prior to 2.2,The affected products contain insecure filesystem permissions that could allow a lower privilege user to escalate privileges to an administrative level user. | 7.8 | More Deta |
| CVE-2021-34202 | There are multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640) 1.01B04. Ordinary permissions can be elevated to administrator permissions, resulting in local arbitrary code execution. An attacker can combine other vulnerabilities to further achieve the purpose of remote code execution. | 7.8 | More Deta |
| CVE-2021-34803 | TeamViewer before 14.7.48644 on Windows loads untrusted DLLs in certain situations. | 7.8 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2010-1432 | Joomla! Core is prone to an information disclosure vulnerability. Attackers can exploit this issue to obtain sensitive information that may help in launching further attacks. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable. | 7.5 | More Deta |
| CVE-2021-33186 | SerenityOS in test-crypto.cpp contains a stack buffer overflow which could allow attackers to obtain sensitive information. | 7.5 | More Deta |
| CVE-2021-27485 | ZOLL Defibrillator Dashboard, v prior to 2.2,The application allows users to store their passwords in a recoverable format, which could allow an attacker to retrieve the credentials from the web browser. | 7.5 | More Deta |
| CVE-2021-0517 | In updateCapabilities of ConnectivityService.java, there is a possible incorrect network state determination due to a logic error in the code. This could lead to biasing of networking tasks to occur on non-VPN networks, which could lead to remote information disclosure, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179053823 | 7.5 | More Deta |
| CVE-2021-0555 | In RenderStruct of protostream_objectsource.cc, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179161711 | 7.5 | More Deta |
| CVE-2021-22363 | There is a resource management error vulnerability in eCNS280_TD V100R005C10SPC650. An attacker needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices. | 7.5 | More Deta |
| CVE-2020-20469 | White Shark System (WSS) 1.3.2 has a SQL injection vulnerability. The vulnerability stems from the log_edit.php files failing to filter the csa_to_user parameter, remote attackers can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2010-1434 | Joomla! Core is prone to a session fixation vulnerability. An attacker may leverage this issue to hijack an arbitrary session and gain access to sensitive information, which may help in launching further attacks. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable. | 7.5 | More Deta |
| CVE-2021-29702 | Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1.4 and 11.5.5 is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200658. | 7.5 | More Deta |
| CVE-2021-0522 | In ConnectionHandler::SdpCb of connection_handler.cc, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-174182139 | 7.5 | More Deta |
| CVE-2021-29063 | A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Mpmath v1.0.0 through v1.2.1 when the mpmathify function is called. | 7.5 | More Deta |
| CVE-2021-29061 | A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Vfsjfilechooser2 version 0.2.9 and below which occurs when the application attempts to validate crafted URIs. | 7.5 | More Deta |
| CVE-2020-27511 | An issue was discovered in the stripTags and unescapeHTML components in Prototype 1.7.3 where an attacker can cause a Regular Expression Denial of Service (ReDOS) through stripping crafted HTML tags. | 7.5 | More Deta |
| CVE-2021-22914 | Citrix Cloud Connector before 6.31.0.62192 suffers from insecure storage of sensitive information due to sensitive information being stored in the Citrix Cloud Connector installation log files. Such information could be used by an malicious actor to access a Citrix Cloud environment. This issue affects all versions of Citrix Cloud Connector that were installed by passing secure client parameters for installation via the command line. The issue does not affect Citrix Cloud Connector if it was installed using the interactive installer or where a parameter file was used with the command-line installer. | 7.5 | More Deta |
| CVE-2021-31661 | RIOT-OS 2021.01 before commit 609c9ada34da5546cffb632a98b7ba157c112658 contains a buffer overflow that could allow attackers to obtain sensitive information. | 7.5 | More Deta |
| CVE-2021-33818 | An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. | 7.5 | More Deta |
| CVE-2021-33820 | An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67.Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service. | 7.5 | More Deta |
| CVE-2021-33822 | An issue was discovered on 4GEE ROUTER HH70VB Version HH70_E1_02.00_22. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. | 7.5 | More Deta |
| CVE-2021-33185 | SerenityOS contains a buffer overflow in the set_range test in TestBitmap which could allow attackers to obtain sensitive information. | 7.5 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2020-24939 | Prototype pollution in Stampit supermixer 1.0.3 allows an attacker to modify the prototype of a base object which can vary in severity depending on the implementation. | 7.5 | More Deta |
| CVE-2021-33823 | An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service. | 7.5 | More Deta |
| CVE-2021-33824 | An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. | 7.5 | More Deta |
| CVE-2021-21279 | Contiki-NG is an open-source, cross-platform operating system for internet of things devices. In verions prior to 4.6, an attacker can perform a denial-of-service attack by triggering an infinite loop in the processing of IPv6 neighbor solicitation (NS) messages. This type of attack can effectively shut down the operation of the system because of the cooperative scheduling used for the main parts of Contiki-NG and its communication stack. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround. | 7.5 | More Deta |
| CVE-2021-31664 | RIOT-OS 2021.01 before commit 44741ff99f7a71df45420635b238b9c22093647a contains a buffer overflow which could allow attackers to obtain sensitive information. | 7.5 | More Deta |
| CVE-2021-31663 | RIOT-OS 2021.01 before commit bc59d60be60dfc0a05def57d74985371e4f22d79 contains a buffer overflow which could allow attackers to obtain sensitive information. | 7.5 | More Deta |
| CVE-2021-31662 | RIOT-OS 2021.01 before commit 07f1254d8537497552e7dce80364aaead9266bbe contains a buffer overflow which could allow attackers to obtain sensitive information. | 7.5 | More Deta |
| CVE-2021-33813 | An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to cause a denial of service via a crafted HTTP request. | 7.5 | More Deta |
| CVE-2021-30468 | A vulnerability in the JsonMapObjectReaderWriter of Apache CXF allows an attacker to submit malformed JSON to a web service, which results in the thread getting stuck in an infinite loop, consuming CPU indefinitely. This issue affects Apache CXF versions prior to 3.4.4; Apache CXF versions prior to 3.3.11. | 7.5 | More Deta |
| CVE-2021-31660 | RIOT-OS 2021.01 before commit 85da504d2dc30188b89f44c3276fc5a25b31251f contains a buffer overflow which could allow attackers to obtain sensitive information. | 7.5 | More Deta |
| CVE-2020-22170 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\get_doctor.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2021-32701 | ORY Oathkeeper is an Identity & Access Proxy (IAP) and Access Control Decision API that authorizes HTTP requests based on sets of Access Rules. When you make a request to an endpoint that requires the scope `foo` using an access token granted with that `foo` scope, introspection will be valid and that token will be cached. The problem comes when a second requests to an endpoint that requires the scope `bar` is made before the cache has expired. Whether the token is granted or not to the `bar` scope, introspection will be valid. A patch will be released with `v0.38.12-beta.1`. Per default, caching is disabled for the `oauth2_introspection` authenticator. When caching is disabled, this vulnerability does not exist. The cache is checked in [`func (a *AuthenticatorOAuth2Introspection) Authenticate(...)`] (https://github.com/ory/oathkeeper/blob/6a31df1c3779425e05db1c2a381166b087cb29a4/pipeline/authn/authenticator_oauth2_introspection.go#L152). From [`tokenFromCache()`] (https://github.com/ory/oathkeeper/blob/6a31df1c3779425e05db1c2a381166b087cb29a4/pipeline/authn/authenticator_oauth2_introspection.go#L97) it seems that it only validates the token expiration date, but ignores whether the token has or not the proper scopes. The vulnerability was introduced in PR #424. During review, we failed to require appropriate test coverage by the submitter which is the primary reason that the vulnerability passed the review process. | 7.5 | More Deta |
| CVE-2021-29059 | A vulnerability was discovered in IS-SVG version 2.1.0 to 4.2.2 and below where a Regular Expression Denial of Service (ReDOS) occurs if the application is provided and checks a crafted invalid SVG string. | 7.5 | More Deta |
| CVE-2021-20566 | IBM Resilient SOAR V38.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 199238. | 7.5 | More Deta |
| CVE-2020-22173 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\edit-profile.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-25754 | An issue was discovered on Enphase Envoy R3.x and D4.x devices. There is a custom PAM module for user authentication that circumvents traditional user authentication. This module uses a password derived from the MD5 hash of the username and serial number. The serial number can be retrieved by an unauthenticated user at /info.xml. Attempts to change the user password via passwd or other tools have no effect. | 7.5 | More Deta |
| CVE-2021-32582 | An issue was discovered in ConnectWise Automate before 2021.5. A blind SQL injection vulnerability exists in core agent inventory communication that can enable an attacker to extract database information or administrative credentials from an instance via crafted monitor status responses. | 7.5 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2020-22172 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\get_doctor.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22171 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\registration.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2021-34825 | Quassel through 0.13.1, when --require-ssl is enabled, launches without SSL or TLS support if a usable X.509 certificate is not found on the local system. | 7.5 | More Deta |
| CVE-2021-20094 | A denial of service vulnerability exists in Wibu-Systems CodeMeter versions < 7.21a. An unauthenticated remote attacker can exploit this issue to crash the CodeMeter Runtime Server. | 7.5 | More Deta |
| CVE-2020-20474 | White Shark System (WSS) 1.3.2 has a SQL injection vulnerability. The vulnerability stems from the default_task_edituser.php files failing to filter the csa_to_user parameter. Remote attackers can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22169 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\appointment-history.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-20473 | White Shark System (WSS) 1.3.2 has a SQL injection vulnerability. The vulnerability stems from the control_task.php, control_project.php, default_user.php files failing to filter the sort parameter. Remote attackers can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22168 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\change-emaild.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22166 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\forgot-password.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22175 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\admin\betweendates-detailsreports.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22165 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\user-login.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-22164 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\check_availability.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2020-18647 | Information Disclosure in NoneCMS v1.3 allows remote attackers to obtain sensitive information via the component "/nonecms/vendor". | 7.5 | More Deta |
| CVE-2020-18646 | Information Disclosure in NoneCMS v1.3 allows remote attackers to obtain sensitive information via the component "/public/index.php". | 7.5 | More Deta |
| CVE-2010-4816 | It was found in FreeBSD 8.0, 6.3 and 4.9, and OpenBSD 4.6 that a null pointer dereference in ftpd/popen.c may lead to remote denial of service of the ftpd service. | 7.5 | More Deta |
| CVE-2021-21441 | There is a XSS vulnerability in the ticket overview screens. It's possible to collect various information by having an e-mail shown in the overview screen. Attack can be performed by sending specially crafted e-mail to the system and it doesn't require any user intraction. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.26 and prior versions. | 7.5 | More Deta |
| CVE-2020-22176 | PHPGurukul Hospital Management System in PHP v4.0 has a sensitive information disclosure vulnerability in multiple areas. Remote unauthenticated users can exploit the vulnerability to obtain user sensitive information. | 7.5 | More Deta |
| CVE-2020-22174 | PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\book-appointment.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information. | 7.5 | More Deta |
| CVE-2021-1566 | A vulnerability in the Cisco Advanced Malware Protection (AMP) for Endpoints integration of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to intercept traffic between an affected device and the AMP servers. This vulnerability is due to improper certificate validation when an affected device establishes TLS connections. A man-in-the-middle attacker could exploit this vulnerability by sending a crafted TLS packet to an affected device. A successful exploit could allow the attacker to spoof a trusted host and then extract sensitive information or alter certain API requests. | 7.4 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-31477 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of GE Reason RPV311 14A03. Authentication is not required to exploit this vulnerability. The specific flaw exists within the firmware and filesystem of the device. The firmware and filesystem contain hard-coded default credentials. An attacker can leverage this vulnerability to execute code in the context of the download user. Was ZDI-CAN-11852. | 7.3 | More Deta |
| CVE-2021-0553 | In onBindViewHolder of AppSwitchPreference.java, there is a possible bypass of device admin setttings due to unclear UI. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169936038 | 7.3 | More Deta |
| CVE-2021-0506 | In ActivityPicker.java, there is a possible bypass of user interaction in intent resolution due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-181962311 | 7.3 | More Deta |
| CVE-2021-0537 | In onCreate of WiFiInstaller.java, there is a possible way to install a malicious Hotspot 2.0 configuration due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176756141 | 7.3 | More Deta |
| CVE-2021-0538 | In onCreate of EmergencyCallbackModeExitDialog.java, there is a possible exit of emergency callback mode due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-178821491 | 7.3 | More Deta |
| CVE-2021-0523 | In onCreate of WifiScanModeActivity.java, there is a possible way to enable Wi-Fi scanning without user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-174047492 | 7.3 | More Deta |
| CVE-2021-1541 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. | 7.2 | More Deta |
| CVE-2020-20444 | Jact OpenClinic 0.8.20160412 allows the attacker to read server files after login to the the admin account by an infected 'file' GET parameter in '/shared/view_source.php' which "could" lead to RCE vulnerability . | 7.2 | More Deta |
| CVE-2021-1542 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. | 7.2 | More Deta |
| CVE-2021-22377 | There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. | 7.2 | More Deta |
| CVE-2021-1571 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. | 7.2 | More Deta |
| CVE-2021-1543 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. | 7.2 | More Deta |
| CVE-2021-29706 | IBM AIX 7.1 could allow a non-privileged local user to exploit a vulnerability in the trace facility to expose sensitive information or cause a denial of service. IBM X-Force ID: 200663. | 7.1 | More Deta |
| CVE-2021-34201 | D-Link DIR-2640-US 1.01B04 is vulnerable to Buffer Overflow. There are multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640). Local ordinary users can overwrite the global variables in the .bss section, causing the process crashes or changes. | 7.1 | More Deta |
| CVE-2021-32938 | Drawings SDK (All versions prior to 2022.4) are vulnerable to an out-of-bounds read due to parsing of DWG files resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allows attackers to cause a denial-of service condition or read sensitive information from memory. | 7.1 | More Deta |
| CVE-2021-32940 | An out-of-bounds read issue exists in the DWG file-recovering procedure in the Drawings SDK (All versions prior to 2022.5) resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or read sensitive information from memory locations. | 7.1 | More Deta |
| CVE-2021-32950 | An out-of-bounds read issue exists within the parsing of DXF files in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allows attackers to cause a denial-of-service condition or read sensitive information from memory locations. | 7.1 | More Deta |
| CVE-2021-32078 | An Out-of-Bounds Read was discovered in arch/arm/mach-footbridge/personal-pci.c in the Linux kernel through 5.12.11 because of the lack of a check for a value that shouldn't be negative, e.g., access to element -2 of an array, aka CID-298a58e165e4. | 7.1 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-1567 | A vulnerability in the DLL loading mechanism of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for DLL files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with SYSTEM privileges. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. | 7.0 | More Deta |
| CVE-2021-0508 | In various functions of DrmPlugin.cpp, 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-8.1 Android-9 Android-10 Android-11Android ID: A-176444154 | 7.0 | More Deta |
| CVE-2021-0509 | In various functions of CryptoPlugin.cpp, 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-9 Android-10 Android-11 Android-8.1Android ID: A-176444161 | 7.0 | More Deta |
| CVE-2021-0532 | In memory management driver, there is a possible memory corruption 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 SoCAndroid ID: A-185196177 | 7.0 | More Deta |
| CVE-2021-21281 | Contiki-NG is an open-source, cross-platform operating system for internet of things devices. A buffer overflow vulnerability exists in Contiki-NG versions prior to 4.6. After establishing a TCP socket using the tcp-socket library, it is possible for the remote end to send a packet with a data offset that is unvalidated. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround. | 7.0 | More Deta |
| CVE-2021-0565 | In wrapUserThread of AudioStream.cpp, 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-11Android ID: A-174801970 | 7.0 | More Deta |
| CVE-2021-0520 | In several functions of MemoryFileSystem.cpp and related files, 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-11 Android-10Android ID: A-176237595 | 7.0 | More Deta |
| CVE-2021-0533 | In memory management driver, there is a possible memory corruption 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 SoCAndroid ID: A-185193932 | 7.0 | More Deta |
| CVE-2020-36394 | pam_setquota.c in the pam_setquota module before 2020-05-29 for Linux-PAM allows local attackers to set their quota on an arbitrary filesystem, in certain situations where the attacker's home directory is a FUSE filesystem mounted under /home. | 7.0 | More Deta |
| CVE-2021-32698 | eLabFTW is an open source electronic lab notebook for research labs. This vulnerability allows an attacker to make GET requests on behalf of the server. It is "blind" because the attacker cannot see the result of the request. Issue has been patched in eLabFTW 4.0.0. | 6.8 | More Deta |
| CVE-2021-32690 | Helm is a tool for managing Charts (packages of pre-configured Kubernetes resources). In versions of helm prior to 3.6.1, a vulnerability exists where the username and password credentials associated with a Helm repository could be passed on to another domain referenced by that Helm repository. This issue has been resolved in 3.6.1. There is a workaround through which one may check for improperly passed credentials. One may use a username and password for a Helm repository and may audit the Helm repository in order to check for another domain being used that could have received the credentials. In the `index.yaml` file for that repository, one may look for another domain in the `urls` list for the chart versions. If there is another domain found and that chart version was pulled or installed, the credentials would be passed on. | 6.8 | More Deta |
| CVE-2021-32693 | Symfony is a PHP framework for web and console applications and a set of reusable PHP components. A vulnerability related to firewall authentication is in Symfony starting with version 5.3.0 and prior to 5.3.2. When an application defines multiple firewalls, the token authenticated by one of the firewalls was available for all other firewalls. This could be abused when the application defines different providers for each part of the application, in such a situation, a user authenticated on a part of the application could be considered authenticated on the rest of the application. Starting in version 5.3.2, a patch ensures that the authenticated token is only available for the firewall that generates it. | 6.8 | More Deta |
| CVE-2021-34204 | D-Link DIR-2640-US 1.01B04 is affected by Insufficiently Protected Credentials. D-Link AC2600(DIR-2640) stores the device system account password in plain text. It does not use linux user management. In addition, the passwords of all devices are the same, and they cannot be modified by normal users. An attacker can easily log in to the target router through the serial port and obtain root privileges. | 6.8 | More Deta |
| CVE-2021-0535 | In wpas_ctrl_msg_queue_timeout of ctrl_iface_unix.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168314741 | 6.7 | More Deta |
| CVE-2021-0544 | In phNxpNciHal_print_res_status of phNxpNciHal.cc, 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-11Android ID: A-169257710 | 6.7 | More Deta |
| CVE-2021-0540 | In halWrapperDataCallback of hal_wrapper.cc, 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-11Android ID: A-169328517 | 6.7 | More Deta |
| CVE-2021-0543 | In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, 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-11Android ID: A-169258743 | 6.7 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-0606 | In drm_syncobj_handle_to_fd of drm_syncobj.c, there is a possible use after free due to incorrect refcounting. 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-168034487 | 6.7 | More Deta |
| CVE-2020-27339 | In the kernel in Insyde InsydeH2O 5.x, certain SMM drivers did not correctly validate the CommBuffer and CommBufferSize parameters, allowing callers to corrupt either the firmware or the OS memory. The fixed versions for this issue in the AhciBusDxe, IdeBusDxe, NvmExpressDxe, SdHostDriverDxe, and SdMmcDeviceDxe drivers are 05.16.25, 05.26.25, 05.35.25, 05.43.25, and 05.51.25 (for Kernel 5.1 through 5.5). | 6.7 | More Deta |
| CVE-2021-0545 | In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258884 | 6.7 | More Deta |
| CVE-2021-0546 | In phNxpNciHal_print_res_status of phNxpNciHal.cc, 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-11Android ID: A-169258733 | 6.7 | More Deta |
| CVE-2020-20468 | White Shark System (WSS) 1.3.2 is vulnerable to CSRF. Attackers can use the user_edit_password.php file to modify the user password. | 6.5 | More Deta |
| CVE-2020-20467 | White Shark System (WSS) 1.3.2 is vulnerable to sensitive information disclosure via default_task_add.php, remote attackers can exploit the vulnerability to create a task. | 6.5 | More Deta |
| CVE-2020-15732 | Improper Certificate Validation vulnerability in the Online Threat Prevention module as used in Bitdefender Total Security allows an attacker to potentially bypass HTTP Strict Transport Security (HSTS) checks. This issue affects: Bitdefender Total Security versions prior to 25.0.7.29. Bitdefender Internet Security versions prior to 25.0.7.29. Bitdefender Antivirus Plus versions prior to 25.0.7.29. | 6.5 | More Deta |
| CVE-2021-32954 | Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to a directory traversal, which may allow an attacker to remotely read arbitrary files on the file system. | 6.5 | More Deta |
| CVE-2021-32575 | HashiCorp Nomad and Nomad Enterprise up to version 1.0.4 bridge networking mode allows ARP spoofing from other bridged tasks on the same node. Fixed in 0.12.12, 1.0.5, and 1.1.0 RC1. | 6.5 | More Deta |
| CVE-2021-0558 | In fillMainDataBuf of pvmp3_framedecoder.cpp, 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-11Android ID: A-173473906 | 6.5 | More Deta |
| CVE-2021-32697 | neos/forms is an open source framework to build web forms. By crafting a special `GET` request containing a valid form state, a form can be submitted without invoking any validators. Form state is secured with an HMAC that is still verified. That means that this issue can only be exploited if Form Finishers cause side effects even if no form values have been sent. Form Finishers can be adjusted in a way that they only execute an action if the submitted form contains some expected data. Alternatively a custom Finisher can be added as first finisher. This regression was introduced with https://github.com/neos/form/commit/049d415295be8d4a0478ccba97dba1bb81649567 | 6.5 | More Deta |
| CVE-2021-28979 | SafeNet KeySecure Management Console 8.12.0 is vulnerable to HTTP response splitting attacks. A remote attacker could exploit this vulnerability using specially-crafted URL to cause the server to return a split response, once the URL is clicked. | 6.5 | More Deta |
| CVE-2021-1569 | Multiple vulnerabilities in Cisco Jabber for Windows, Cisco Jabber for Mac, and Cisco Jabber for mobile platforms could allow an attacker to access sensitive information or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. | 6.5 | More Deta |
| CVE-2021-0559 | In Lag_max of p_ol_wgh.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 needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172312730 | 6.5 | More Deta |
| CVE-2021-1570 | Multiple vulnerabilities in Cisco Jabber for Windows, Cisco Jabber for Mac, and Cisco Jabber for mobile platforms could allow an attacker to access sensitive information or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. | 6.5 | More Deta |
| CVE-2020-35759 | bloofoxCMS 0.5.2.1 is infected with a CSRF Attack that leads to an attacker editing any file content (Locally/Remotely). | 6.5 | More Deta |
| CVE-2020-8299 | Citrix ADC and Citrix/NetScaler Gateway 13.0 before 13.0-76.29, 12.1-61.18, 11.1-65.20, Citrix ADC 12.1-FIPS before 12.1-55.238, and Citrix SD-WAN WANOP Edition before 11.4.0, 11.3.2, 11.3.1a, 11.2.3a, 11.1.2c, 10.2.9a suffers from uncontrolled resource consumption by way of a network-based denial-of-service from within the same Layer 2 network segment. Note that the attacker must be in the same Layer 2 network segment as the vulnerable appliance. | 6.5 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-32659 | Matrix-appservice-bridge is the bridging service for the Matrix communication program's application services. In versions 2.6.0 and earlier, if a bridge has room upgrade handling turned on in the configuration (the `roomUpgradeOpts` key when instantiating a new `Bridge` instance.), any `m.room.tombstone` event it encounters will be used to unbridge the current room and bridge into the target room. However, the target room `m.room.create` event is not checked to verify if the `predecessor` field contains the previous room. This means that any malicious admin of a bridged room can repoint the traffic to a different room without the new room being aware. Versions 2.6.1 and greater are patched. As a workaround, disabling the automatic room upgrade handling can be done by removing the `roomUpgradeOpts` key from the `Bridge` class options. | 6.5 | More Deta |
| CVE-2021-20488 | IBM Security Identity Manager 6.0.2 could allow an authenticated malicious user to change the passwords of other users in the Windows AD environment when IBM Security Identity Manager Windows Password Synch Plug-in is deployed and configured. IBM X-Force ID: 197789. | 6.5 | More Deta |
| CVE-2021-0551 | In bind of MediaControlPanel.java, there is a possible way to lock up the system UI using a malicious media file due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-180518039 | 6.5 | More Deta |
| CVE-2021-32699 | Wings is the control plane software for the open source Pterodactyl game management system. All versions of Pterodactyl Wings prior to `1.4.4` are vulnerable to system resource exhaustion due to improper container process limits being defined. A malicious user can consume more resources than intended and cause downstream impacts to other clients on the same hardware, eventually causing the physical server to stop responding. Users should upgrade to `1.4.4` to mitigate the issue. There is no non-code based workaround for impacted versions of the software. Users running customized versions of this software can manually set a PID limit for containers created. | 6.5 | More Deta |
| CVE-2021-22382 | Huawei LTE USB Dongle products have an improper permission assignment vulnerability. An attacker can locally access and log in to a PC to induce a user to install a specially crafted application. After successfully exploiting this vulnerability, the attacker can perform unauthenticated operations. Affected product versions include:E3372 E3372h-153TCPU-V200R002B333D01SP00C00. | 6.5 | More Deta |
| CVE-2021-32676 | Nextcloud Talk is a fully on-premises audio/video and chat communication service. Password protected shared chats in Talk before version 9.0.10, 10.0.8 and 11.2.2 did not rotate the session cookie after a successful authentication event. It is recommended that the Nextcloud Talk App is upgraded to 9.0.10, 10.0.8 or 11.2.2. No workarounds for this vulnerability are known to exist. | 6.5 | More Deta |
| CVE-2021-0504 | In avrc_pars_browse_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179162665 | 6.5 | More Deta |
| CVE-2020-8300 | Citrix ADC and Citrix/NetScaler Gateway before 13.0-82.41, 12.1-62.23, 11.1-65.20 and Citrix ADC 12.1-FIPS before 12.1-55.238 suffer from improper access control allowing SAML authentication hijack through a phishing attack to steal a valid user session. Note that Citrix ADC or Citrix Gateway must be configured as a SAML SP or a SAML IdP for this to be possible. | 6.5 | More Deta |
| CVE-2021-20737 | Improper authentication vulnerability in GROWI versions prior to v4.2.20 allows a remote attacker to view the unauthorized pages without access privileges via unspecified vectors. | 6.5 | More Deta |
| CVE-2021-20483 | IBM Security Identity Manager 6.0.2 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197591. | 6.5 | More Deta |
| CVE-2021-32644 | Ampache is an open source web based audio/video streaming application and file manager. Due to a lack of input filtering versions 4.x.y are vulnerable to code injection in random.php. The attack requires user authentication to access the random.php page unless the site is running in demo mode. This issue has been resolved in 4.4.3. | 6.4 | More Deta |
| CVE-2021-0564 | In decrypt of CryptoPlugin.cpp, 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-11Android ID: A-176495665 | 6.4 | More Deta |
| CVE-2021-34388 | Bootloader contains a vulnerability in NVIDIA TegraBoot where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. | 6.3 | More Deta |
| CVE-2021-34387 | The ARM TrustZone Technology on which Trusty is based on contains a vulnerability in access permission settings where the portion of the DRAM reserved for TrustZone is identity-mapped by TLK with read, write, and execute permissions, which gives write access to kernel code and data that is otherwise mapped read only. | 6.3 | More Deta |
| CVE-2021-34386 | Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the calloc size calculation can cause the multiplication of count and size can overflow, which might lead to heap overflows. | 6.3 | More Deta |
| CVE-2010-4266 | It was found in vanilla forums before 2.0.10 a potential linkbait vulnerability in dispatcher. | 6.1 | More Deta |
| CVE-2021-24373 | The WP Hardening – Fix Your WordPress Security WordPress plugin before 1.2.2 did not sanitise or escape the historyvalue GET parameter before outputting it in a Javascript block, leading to a reflected Cross-Site Scripting issue. | 6.1 | More Deta |
| CVE-2021-28833 | Increments Qiita::Markdown before 0.34.0 allows XSS via a crafted gist link, a different vulnerability than CVE-2021-28796. | 6.1 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-20734 | Cross-site scripting vulnerability in Welcart e-Commerce versions prior to 2.2.4 allows remote attackers to inject arbitrary script or HTML via unspecified vectors. | 6.1 | More Deta |
| CVE-2021-20744 | Cross-site scripting vulnerability in EC-CUBE Category contents plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation. | 6.1 | More Deta |
| CVE-2021-20735 | Cross-site scripting vulnerability in ETUNA EC-CUBE plugins (Delivery slip number plugin (3.0 series) 1.0.10 and earlier, Delivery slip number csv bulk registration plugin (3.0 series) 1.0.8 and earlier, and Delivery slip number mail plugin (3.0 series) 1.0.8 and earlier) allows remote attackers to inject an arbitrary script by executing a specific operation on the management page of EC-CUBE. | 6.1 | More Deta |
| CVE-2021-20743 | Cross-site scripting vulnerability in EC-CUBE Email newsletters management plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.4 allows a remote attacker to inject an arbitrary script by leading a user to a specially crafted page and to perform a specific operation. | 6.1 | More Deta |
| CVE-2021-20742 | Cross-site scripting vulnerability in EC-CUBE Business form output plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script via unspecified vector. | 6.1 | More Deta |
| CVE-2021-20741 | Cross-site scripting vulnerability in Hitachi Application Server Help (Hitachi Application Server V10 Manual (Windows) version 10-11-01 and earlier and Hitachi Application Server V10 Manual (UNIX) version 10-11-01 and earlier) allows a remote attacker to inject an arbitrary script via unspecified vectors. | 6.1 | More Deta |
| CVE-2010-4264 | It was found in vanilla forums before 2.0.10 a cross-site scripting vulnerability where a filename could contain arbitrary code to execute on the client side. | 6.1 | More Deta |
| CVE-2021-32426 | In TrendNet TW100-S4W1CA 2.3.32, it is possible to inject arbitrary JavaScript into the router's web interface via the "echo" command. | 6.1 | More Deta |
| CVE-2021-20733 | Improper authorization in handler for custom URL scheme vulnerability in あすけんダイエット (asken diet) for Android versions from v.3.0.0 to v.4.2.x allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App. | 6.1 | More Deta |
| CVE-2021-26835 | No filtering of cross-site scripting (XSS) payloads in the markdown-editor in Zettlr 1.8.7 allows attackers to perform remote code execution via a crafted file. | 6.1 | More Deta |
| CVE-2021-32536 | The login page in the MCUsystem does not filter with special characters, which allows remote attackers can inject JavaScript without privilege and thus perform reflected XSS attacks. | 6.1 | More Deta |
| CVE-2021-33557 | An XSS issue was discovered in manage_custom_field_edit_page.php in MantisBT before 2.25.2. Unescaped output of the return parameter allows an attacker to inject code into a hidden input field. | 6.1 | More Deta |
| CVE-2020-18654 | Cross Site Scripting (XSS) in Wuzhi CMS v4.1.0 allows remote attackers to execute arbitrary code via the "Title" parameter in the component "/coreframe/app/guestbook/myissue.php". | 6.1 | More Deta |
| CVE-2019-25047 | Greenbone Security Assistant (GSA) before 8.0.2 and Greenbone OS (GOS) before 5.0.10 allow XSS during 404 URL handling in gsad. | 6.1 | More Deta |
| CVE-2020-21517 | Cross Site Scripting (XSS) vulnerability in MetInfo 7.0.0 via the gourl parameter in login.php. | 6.1 | More Deta |
| CVE-2021-24364 | The Jannah WordPress theme before 5.4.4 did not properly sanitize the options JSON parameter in its tie_get_user_weather AJAX action before outputting it back in the page, leading to a Reflected Cross-Site Scripting (XSS) vulnerability. | 6.1 | More Deta |
| CVE-2020-21130 | Cross Site Scripting (XSS) vulnerability in HisiPHP 2.0.8 via the group name in addgroup.html. | 6.1 | More Deta |
| CVE-2020-35373 | In Fiyo CMS 2.0.6.1, the 'tag' parameter results in an unauthenticated XSS attack. | 6.1 | More Deta |
| CVE-2020-19511 | Cross Site Scriptiong vulnerability in Typesetter 5.1 via the !1) className and !2) Description fields in index.php/Admin/Classes, | 6.1 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-32956 | Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to redirection, which may allow an attacker to send a maliciously crafted URL that could result in redirecting a user to a malicious webpage. | 6.1 | More Deta |
| CVE-2021-35045 | Cross site scripting (XSS) vulnerability in Ice Hrm 29.0.0.OS, allows attackers to execute arbitrary code via the parameters to the /app/ endpoint. | 6.1 | More Deta |
| CVE-2021-35046 | A session fixation vulnerability was discovered in Ice Hrm 29.0.0 OS which allows an attacker to hijack a valid user session via a crafted session cookie. | 6.1 | More Deta |
| CVE-2021-35206 | Gitpod before 0.6.0 allows unvalidated redirects. | 6.1 | More Deta |
| CVE-2021-24368 | The Quiz And Survey Master – Best Quiz, Exam and Survey Plugin WordPress plugin before 7.1.18 did not sanitise or escape its result_id parameter when displaying an existing quiz result page, leading to a reflected Cross-Site Scripting issue. This could allow for privilege escalation by inducing a logged in admin to open a malicious link | 6.1 | More Deta |
| CVE-2021-24372 | The WP Hardening – Fix Your WordPress Security WordPress plugin before 1.2.2 did not sanitise or escape the $_SERVER['REQUEST_URI'] before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue. | 6.1 | More Deta |
| CVE-2021-28815 | Insecure storage of sensitive information has been reported to affect QNAP NAS running myQNAPcloud Link. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism. This issue affects: QNAP Systems Inc. myQNAPcloud Link versions prior to 2.2.21 on QTS 4.5.3; versions prior to 2.2.21 on QuTS hero h4.5.2; versions prior to 2.2.21 on QuTScloud c4.5.4. | 6.0 | More Deta |
| CVE-2010-3300 | It was found that all OWASP ESAPI for Java up to version 2.0 RC2 are vulnerable to padding oracle attacks. | 5.9 | More Deta |
| CVE-2021-31857 | In Zoho ManageEngine Password Manager Pro before 11.1 build 11104, attackers are able to retrieve credentials via a browser extension for non-website resource types. | 5.9 | More Deta |
| CVE-2021-34812 | Use of hard-coded credentials vulnerability in php component in Synology Calendar before 2.4.0-0761 allows remote attackers to obtain sensitive information via unspecified vectors. | 5.8 | More Deta |
| CVE-2021-34808 | Server-Side Request Forgery (SSRF) vulnerability in cgi component in Synology Media Server before 1.8.3-2881 allows remote attackers to access intranet resources via unspecified vectors. | 5.8 | More Deta |
| CVE-2021-23396 | All versions of package lutils are vulnerable to Prototype Pollution via the main (merge) function. | 5.6 | More Deta |
| CVE-2021-0556 | In getBlockSum of fastcodemb.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172716941 | 5.5 | More Deta |
| CVE-2021-22366 | There is an out-of-bounds read vulnerability in eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a function that handles an internal message contains an out-of-bounds read vulnerability. An attacker could crafted messages between system process, successful exploit could cause Denial of Service (DoS). | 5.5 | More Deta |
| CVE-2021-27487 | ZOLL Defibrillator Dashboard, v prior to 2.2, The affected products contain credentials stored in plaintext. This could allow an attacker to gain access to sensitive information. | 5.5 | More Deta |
| CVE-2021-0563 | In ih264e_fmt_conv_422i_to_420sp of ih264e_fmt_conv.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172908358 | 5.5 | More Deta |
| CVE-2021-0562 | In RasterIntraUpdate of motion_est.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176084648 | 5.5 | More Deta |
| CVE-2021-27481 | ZOLL Defibrillator Dashboard, v prior to 2.2, The affected products utilize an encryption key in the data exchange process, which is hardcoded. This could allow an attacker to gain access to sensitive information. | 5.5 | More Deta |
| CVE-2021-0561 | In append_to_verify_fifo_interleaved_ of stream_encoder.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174302683 | 5.5 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-0572 | In doNotification of AccountManagerService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-177931355 | 5.5 | More Deta |
| CVE-2021-0542 | In updateNotification of BeamTransferManager.java, there is a missing permission check. This could lead to local information disclosure of paired Bluetooth addresses with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168712890 | 5.5 | More Deta |
| CVE-2021-0552 | In getEndItemSliceAction of MediaOutputSlice.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-175124820 | 5.5 | More Deta |
| CVE-2021-21997 | VMware Tools for Windows (11.x.y prior to 11.3.0) contains a denial-of-service vulnerability in the VM3DMP driver. A malicious actor with local user privileges in the Windows guest operating system, where VMware Tools is installed, can trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest operating system. | 5.5 | More Deta |
| CVE-2021-1568 | A vulnerability in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. This vulnerability is due to uncontrolled memory allocation. An attacker could exploit this vulnerability by copying a crafted file to a specific folder on the system. A successful exploit could allow the attacker to crash the VPN Agent service when the affected application is launched, causing it to be unavailable to all users of the system. To exploit this vulnerability, the attacker must have valid credentials on a multiuser Windows system. | 5.5 | More Deta |
| CVE-2021-0521 | In getAllPackages of PackageManagerService, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of cross-user permissions with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174661955 | 5.5 | More Deta |
| CVE-2021-0554 | In isBackupServiceActive of BackupManagerService.java, there is 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-11Android ID: A-158482162 | 5.5 | More Deta |
| CVE-2021-26834 | A cross-site scripting (XSS) vulnerability exists in Znote 0.5.2. An attacker can insert payloads, and the code execution will happen immediately on markdown view mode. | 5.4 | More Deta |
| CVE-2021-27479 | ZOLL Defibrillator Dashboard, v prior to 2.2,The affected product's web application could allow a low privilege user to inject parameters to contain malicious scripts to be executed by higher privilege users. | 5.4 | More Deta |
| CVE-2021-32244 | Cross Site Scripting (XSS) in Moodle 3.10.3 allows remote attackers to execute arbitrary web script or HTML via the "Description" field. | 5.4 | More Deta |
| CVE-2021-31521 | Trend Micro InterScan Web Security Virtual Appliance version 6.5 was found to have a reflected cross-site scripting (XSS) vulnerability in the product's Captive Portal. | 5.4 | More Deta |
| CVE-2020-19202 | An authenticated Stored XSS (Cross-site Scripting) exists in the "captive.cgi" Captive Portal via the "Title of Login Page" text box or "TITLE" parameter in IPFire 2.21 (x86_64) - Core Update 130. It allows an authenticated WebGUI user with privileges to execute Stored Cross-site Scripting in the Captive Portal page. | 5.4 | More Deta |
| CVE-2020-22167 | PHPGurukul Hospital Management System in PHP v4.0 has a Persistent Cross-Site Scripting vulnerability in \hms\admin\appointment-history.php. Remote registered users can exploit the vulnerability to obtain user cookie data. | 5.4 | More Deta |
| CVE-2021-32681 | Wagtail is an open source content management system built on Django. A cross-site scripting vulnerability exists in versions 2.13-2.13.1, versions 2.12-2.12.4, and versions prior to 2.11.8. When the `{% include_block %}` template tag is used to output the value of a plain-text StreamField block (`CharBlock`, `TextBlock` or a similar user-defined block derived from `FieldBlock`), and that block does not specify a template for rendering, the tag output is not properly escaped as HTML. This could allow users to insert arbitrary HTML or scripting. This vulnerability is only exploitable by users with the ability to author StreamField content (i.e. users with 'editor' access to the Wagtail admin). Patched versions have been released as Wagtail 2.11.8 (for the LTS 2.11 branch), Wagtail 2.12.5, and Wagtail 2.13.2 (for the current 2.13 branch). As a workaround, site implementors who are unable to upgrade to a current supported version should audit their use of `{% include_block %}` to ensure it is not used to output `CharBlock` / `TextBlock` values with no associated template. Note that this only applies where `{% include_block %}` is used directly on that block (uses of `include_block` on a block _containing_ a CharBlock / TextBlock, such as a StructBlock, are unaffected). In these cases, the tag can be replaced with Django's `{{ ... }}` syntax - e.g. `{% include_block my_title_block %}` becomes `{{ my_title_block }}`. | 5.4 | More Deta |
| CVE-2020-35761 | bloofoxCMS 0.5.2.1 is infected with XSS that allows remote attackers to execute arbitrary JS/HTML Code. | 5.4 | More Deta |
| CVE-2021-32245 | In PageKit v1.0.18, a user can upload SVG files in the file upload portion of the CMS. These SVG files can contain malicious scripts. This file will be uploaded to the system and it will not be stripped or filtered. The user can create a link on the website pointing to "/storage/exp.svg" that will point to http://localhost/pagekit/storage/exp.svg. When a user comes along to click that link, it will trigger a XSS attack. | 5.4 | More Deta |
| CVE-2021-21667 | Jenkins Scriptler Plugin 3.2 and earlier does not escape parameter names shown in job configuration forms, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Scriptler/Configure permission. | 5.4 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-21668 | Jenkins Scriptler Plugin 3.1 and earlier does not escape script content, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Scriptler/Configure permission. | 5.4 | More Deta |
| CVE-2021-33347 | An issue was discovered in JPress v3.3.0 and below. There are XSS vulnerabilities in the template module and tag management module. If you log in to the background by means of weak password, the storage XSS vulnerability can occur. | 5.4 | More Deta |
| CVE-2021-24338 | The Pods – Custom Content Types and Fields WordPress plugin before 2.7.27 was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) security vulnerability within the 'Singular Label' field parameter. | 5.4 | More Deta |
| CVE-2021-24339 | The Pods – Custom Content Types and Fields WordPress plugin before 2.7.27 was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) security vulnerability within the 'Menu Label' field parameter. | 5.4 | More Deta |
| CVE-2021-24366 | The Admin Columns WordPress plugin before 4.3 and Admin Columns Pro WordPress plugin before 5.5.1 do not sanitise and escape its Label settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | 5.4 | More Deta |
| CVE-2021-24367 | The WP Config File Editor WordPress plugin through 1.7.1 was affected by an Authenticated Stored Cross-Site Scripting (XSS) vulnerability. | 5.4 | More Deta |
| CVE-2021-24369 | In the GetPaid WordPress plugin before 2.3.4, users with the contributor role and above can create a new Payment Form, however the Label and Help Text input fields were not getting sanitized properly. So it was possible to inject malicious content such as img tags, leading to a Stored Cross-Site Scripting issue which is triggered when the form will be edited, for example when an admin reviews it and could lead to privilege escalation. | 5.4 | More Deta |
| CVE-2021-24383 | The WP Google Maps WordPress plugin before 8.1.12 did not sanitise, validate of escape the Map Name when output in the Map List of the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue | 5.4 | More Deta |
| CVE-2021-34243 | A stored cross site scripting (XSS) vulnerability was discovered in Ice Hrm 29.0.0.OS which allows attackers to execute arbitrary web scripts or HTML via a crafted file uploaded into the Document Management tab. The exploit is triggered when a user visits the upload location of the crafted file. | 5.4 | More Deta |
| CVE-2020-25752 | An issue was discovered on Enphase Envoy R3.x and D4.x devices. There are hardcoded web-panel login passwords for the installer and Enphase accounts. The passwords for these accounts are hardcoded values derived from the MD5 hash of the username and serial number mixed with some static strings. The serial number can be retrieved by an unauthenticated user at /info.xml. These passwords can be easily calculated by an attacker; users are unable to change these passwords. | 5.3 | More Deta |
| CVE-2021-34390 | Trusty contains a vulnerability in the NVIDIA TLK kernel function where a lack of checks allows the exploitation of an integer overflow through a specific SMC call that is triggered by the user, which may lead to denial of service. | 5.3 | More Deta |
| CVE-2021-22378 | There is a race condition vulnerability in eCNS280_TD V100R005C00 and V100R005C10. There is a timing window exists in which the database can be operated by another thread that is operating concurrently. Successful exploit may cause the affected device abnormal. | 5.3 | More Deta |
| CVE-2021-31159 | Zoho ManageEngine ServiceDesk Plus MSP before 10519 is vulnerable to a User Enumeration bug due to improper error-message generation in the Forgot Password functionality, aka SDPMSP-15732. | 5.3 | More Deta |
| CVE-2020-22200 | Directory Traversal vulnerability in phpCMS 9.1.13 via the q parameter to public_get_suggest_keyword. | 5.3 | More Deta |
| CVE-2020-20470 | White Shark System (WSS) 1.3.2 has web site physical path leakage vulnerability. | 5.3 | More Deta |
| CVE-2021-29060 | A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Color-String version 1.5.5 and below which occurs when the application is provided and checks a crafted invalid HWB string. | 5.3 | More Deta |
| CVE-2021-34801 | Valine 1.4.14 allows remote attackers to cause a denial of service (application outage) by supplying a ua (aka User-Agent) value that only specifies the product and version. | 5.3 | More Deta |
| CVE-2021-24374 | The Jetpack Carousel module of the JetPack WordPress plugin before 9.8 allows users to create a "carousel" type image gallery and allows users to comment on the images. A security vulnerability was found within the Jetpack Carousel module by nguyenhg_vcs that allowed the comments of non-published page/posts to be leaked. | 5.3 | More Deta |
| CVE-2021-24379 | The Comments Like Dislike WordPress plugin before 1.1.4 allows users to like/dislike posted comments, however does not prevent them from replaying the AJAX request to add a like. This allows any user (even unauthenticated) to add unlimited like/dislike to any comment. The plugin appears to have some Restriction modes, such as Cookie Restriction, IP Restrictions, Logged In User Restriction, however, they do not prevent such attack as they only check client side | 5.3 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-34391 | Trusty contains a vulnerability in the NVIDIA TLK kernel function where a lack of checks allows the exploitation of an integer overflow through a specific SMC call that is triggered by the user, which may lead to denial of service. | 5.3 | More Deta |
| CVE-2020-20472 | White Shark System (WSS) 1.3.2 has a sensitive information disclosure vulnerability. The if_get_addbook.php file does not have an authentication operation. Remote attackers can obtain username information for all users of the current site. | 5.3 | More Deta |
| CVE-2021-34683 | An issue was discovered in EXCELLENT INFOTEK CORPORATION (EIC) E-document System 3.0. A remote attacker can use kw/auth/bbs/asp/get_user_email_info_bbs.asp to obtain the contact information (name and e-mail address) of everyone in the entire organization. This information can allow remote attackers to perform social engineering or brute force attacks against the system login page. | 5.3 | More Deta |
| CVE-2021-33577 | An issue was discovered in Cleo LexiCom 5.5.0.0. The requirement for the sender of an AS2 message to identify themselves (via encryption and signing of the message) can be bypassed by changing the Content-Type of the message to text/plain. | 5.3 | More Deta |
| CVE-2021-0569 | In onStart of ContactsDumpActivity.java, there is possible access to contacts due to a tapjacking/overlay attack. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174045870 | 5.0 | More Deta |
| CVE-2021-34811 | Server-Side Request Forgery (SSRF) vulnerability in task management component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to access intranet resources via unspecified vectors. | 5.0 | More Deta |
| CVE-2021-34389 | Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check can allow a local user through a malicious client to access memory from the heap in the TrustZone, which may lead to information disclosure. | 5.0 | More Deta |
| CVE-2021-22342 | There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. | 4.9 | More Deta |
| CVE-2021-22383 | There is an out-of-bounds read vulnerability in eCNS280_TD V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a message-handling function that contains an out-of-bounds read vulnerability. An attacker can exploit this vulnerability by sending a specific message to the target device, which could cause a Denial of Service (DoS). | 4.9 | More Deta |
| CVE-2021-24378 | The Autoptimize WordPress plugin before 2.7.8 does not check for malicious files such as .html in the archive uploaded via the 'Import Settings' feature. As a result, it is possible for a high privilege user to upload a malicious file containing JavaScript code inside an archive which will execute when a victim visits index.html inside the plugin directory. | 4.8 | More Deta |
| CVE-2021-34815 | CheckSec Canopy before 3.5.2 allows XSS attacks against the login page via the LOGIN_PAGE_DISCLAIMER parameter. | 4.8 | More Deta |
| CVE-2021-1395 | A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. | 4.7 | More Deta |
| CVE-2021-32033 | Protectimus SLIM NFC 70 10.01 devices allow a Time Traveler attack in which attackers can predict TOTP passwords in certain situations. The time value used by the device can be set independently from the used seed value for generating time-based one-time passwords, without authentication. Thus, an attacker with short-time physical access to a device can set the internal real-time clock (RTC) to the future, generate one-time passwords, and reset the clock to the current time. This allows the generation of valid future time-based one-time passwords without having further access to the hardware token. | 4.6 | More Deta |
| CVE-2021-34392 | Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the tz_map_shared_mem function can bypass boundary checks, which might lead to denial of service. | 4.4 | More Deta |
| CVE-2021-0566 | In accessAudioHalPidscpp of TimeCheck.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-175894436 | 4.4 | More Deta |
| CVE-2021-20567 | IBM Resilient SOAR V38.0 could allow a local privileged attacker to obtain sensitive information due to improper or nonexisting encryption.IBM X-Force ID: 199239. | 4.4 | More Deta |
| CVE-2021-0549 | In sspRequestCallback of BondStateMachine.java, there is a possible leak of Bluetooth MAC addresses due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-183961896 | 4.4 | More Deta |
| CVE-2021-0605 | In pfkey_dump of af_key.c, there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-110373476 | 4.4 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2021-0541 | In phNxpNciHal_ext_process_nfc_init_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258455 | 4.4 | More Deta |
| CVE-2021-34553 | Sonatype Nexus Repository Manager 3.x before 3.31.0 allows a remote authenticated attacker to get a list of blob files and read the content of a blob file (via a GET request) without having been granted access. | 4.3 | More Deta |
| CVE-2021-1524 | A vulnerability in the API of Cisco Meeting Server could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because requests that are sent to the API are not properly validated. An attacker could exploit this vulnerability by sending a malicious request to the API. A successful exploit could allow the attacker to cause all participants on a call to be disconnected, resulting in a DoS condition. | 4.3 | More Deta |
| CVE-2021-31818 | Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API because user supplied data in the API request isn't parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables. | 4.3 | More Deta |
| CVE-2021-3535 | Rapid7 Nexpose is vulnerable to a non-persistent cross-site scripting vulnerability affecting the Security Console's Filtered Asset Search feature. A specific search criterion and operator combination in Filtered Asset Search could have allowed a user to pass code through the provided search field. This issue affects version 6.6.80 and prior, and is fixed in 6.6.81. If your Security Console currently falls on or within this affected version range, ensure that you update your Security Console to the latest version. | 4.3 | More Deta |
| CVE-2020-36389 | In CiviCRM before 5.28.1 and CiviCRM ESR before 5.27.5 ESR, the CKEditor configuration form allows CSRF. | 4.3 | More Deta |
| CVE-2021-28684 | The XML parser used in ConeXware PowerArchiver before 20.10.02 allows processing of external entities, which might lead to exfiltration of local files over the network (via an XXE attack). | 4.3 | More Deta |
| CVE-2021-34393 | Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. | 4.2 | More Deta |
| CVE-2021-34394 | Trusty contains a vulnerability in the NVIDIA OTE protocol that is present in all TAs. An incorrect message stream deserialization allows an attacker to use the malicious CA that is run by the user to cause the buffer overflow, which may lead to information disclosure and data modification. | 4.2 | More Deta |
| CVE-2021-32694 | Nextcloud Android app is the Android client for Nextcloud. In versions prior to 3.15.1, a malicious application on the same device is possible to crash the Nextcloud Android Client due to an uncaught exception. The vulnerability is patched in version 3.15.1. | 4.1 | More Deta |
| CVE-2021-32695 | Nextcloud Android app is the Android client for Nextcloud. In versions prior to 3.16.1, a malicious app on the same device could have gotten access to the shared preferences of the Nextcloud Android application. This required user-interaction as a victim had to initiate the sharing flow and choose the malicious app. The shared preferences contain some limited private data such as push tokens and the account name. The vulnerability is patched in version 3.16.1. | 3.9 | More Deta |
| CVE-2021-34395 | Trusty TLK contains a vulnerability in its access permission settings where it does not properly restrict access to a resource from a user with local privileges, which might lead to limited information disclosure, a low risk of modifcations to data, and limited denial of service. | 3.9 | More Deta |
| CVE-2021-32696 | The npm package "striptags" is an implementation of PHP's strip_tags in Typescript. In striptags before version 3.2.0, a type-confusion vulnerability can cause `striptags` to concatenate unsanitized strings when an array-like object is passed in as the `html` parameter. This can be abused by an attacker who can control the shape of their input, e.g. if query parameters are passed directly into the function. This can lead to a XSS. | 3.7 | More Deta |
| CVE-2021-33572 | A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the FSAVD component used in certain F-Secure products can crash while scanning larger packages/fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. | 3.5 | More Deta |
| CVE-2020-18442 | Infinite Loop in zziplib v0.13.69 allows remote attackers to cause a denial of service via the return value "zzip_file_read" in the function "unzzip_cat_file". | 3.3 | More Deta |
| CVE-2021-22365 | There is an out of bounds read vulnerability in eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. A local attacker can exploit this vulnerability by sending specific message to the target device. Due to insufficient validation of internal message, successful exploit may cause the process and the service abnormal. | 3.3 | More Deta |
| CVE-2021-34396 | Bootloader contains a vulnerability in access permission settings where unauthorized software may be able to overwrite NVIDIA MB2 code, which would result in limited denial of service. | 3.0 | More Deta |
| CVE-2021-34428 | For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, if an exception is thrown from the SessionListener#sessionDestroyed() method, then the session ID is not invalidated in the session ID manager. On deployments with clustered sessions and multiple contexts this can result in a session not being invalidated. This can result in an application used on a shared computer being left logged in. | 2.9 | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2020-35762 | bloofoxCMS 0.5.2.1 is infected with Path traversal in the 'fileurl' parameter that allows attackers to read local files. | 2.7 | More Deta |
| CVE-2021-34397 | Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. | 1.9 | More Deta |
| CVE-2010-3446 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none | N/A | More Deta |
| CVE-2010-2804 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2005-0394 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2007-3733 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2018-14639 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2005-2795 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2019-7002 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2020-7031 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2006-0016 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2006-0017 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2006-0740 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2006-0849 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2006-1053 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2007-1857 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2021-20248 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Deta |
| CVE-2010-0413 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2010-2475 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |

| CVE Number | Description | Base Score | Refe |
|---|---|---|---|
| CVE-2010-2485 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2010-2486 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Deta |
| CVE-2021-20249 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none | N/A | More Deta |