SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 February 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-2021-21477	SAP Commerce Cloud, versions - 1808,1811,1905,2005,2011, enables certain users with required privileges to edit drools rules, an authenticated attacker with this privilege will be able to inject malicious code in the drools rules which when executed leads to Remote Code Execution vulnerability enabling the attacker to compromise the underlying host enabling him to impair confidentiality, integrity and availability of the application.	9.9	More Details
CVE-2020-28144	Certain Moxa Inc products are affected by an improper restriction of operations in EDR-G903 Series Firmware Version 5.5 or lower, EDR-G902 Series Firmware Version 5.5 or lower, and EDR-810 Series Firmware Version 5.6 or lower. Crafted requests sent to the device may allow remote arbitrary code execution.	9.8	More Details
CVE-2021-26918	The ProBot bot through 2021-02-08 for Discord might allow attackers to interfere with the intended purpose of the "Send an image when a user joins the server" feature (or possibly have unspecified other impact) because the uploader web service allows double extensions (such as .html.jpg) with the text/html content type. NOTE: there may not be cases in which an uploader web service is customer controlled; however, the nature of the issue has substantial interaction with customer controlled configuration. NOTE: the vendor states "This is just an uploader (like any other one) which uploads files to cloud storage and accepts various file types. There is no kind of vulnerability and it won't compromise either the client side or the server side.	9.8	More Details
CVE-2021-26754	wpDataTables before 3.4.1 mishandles order direction for server-side tables, aka admin-ajax.php?action=get_wdtable order[0][dir] SQL injection.	9.8	More Details
CVE-2020-11920	An issue was discovered in Svakom Siime Eye 14.1.00000001.3.330.0.0.3.14. A command injection vulnerability resides in the HOST/IP section of the NFS settings menu in the webserver running on the device. By injecting Bash commands via shell metacharacters here, the device executes arbitrary code with root privileges (all of the device's services are running as root).	9.8	More Details
CVE-2020-29165	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by incorrect access control, which can result in remotely gaining administrator privileges.	9.8	More Details
CVE-2020-16629	PhpOK 5.4.137 contains a SQL injection vulnerability that can inject an attachment data through SQL, and then call the attachment replacement function through api.php to write a PHP file to the target path.	9.8	More Details
CVE-2020-6649	An insufficient session expiration vulnerability in FortiNet's FortiIsolator version 2.0.1 and below may allow an attacker to reuse the unexpired admin user session IDs to gain admin privileges, should the attacker be able to obtain that session ID (via other, hypothetical attacks)	9.8	More Details
CVE-2021-26541	The gitlog function in src/index.ts in gitlog before 4.0.4 has a command injection vulnerability.	9.8	More Details
CVE-2020-7782	This affects all versions of package spritesheet-js. It depends on a vulnerable package platform-command. The injection point is located in line 32 in lib/generator.js, which is triggered by main entry of the package.	9.8	More Details
CVE-2020-7785	This affects all versions of package node-ps. The injection point is located in line 72 in lib/index.js.	9.8	More Details
CVE-2020-7786	This affects all versions of package macfromip. The injection point is located in line 66 in macfromip.js.	9.8	More Details
CVE-2021-22502	Remote Code execution vulnerability in Micro Focus Operation Bridge Reporter (OBR) product, affecting version 10.40. The vulnerability could be exploited to allow Remote Code Execution on the OBR server.	9.8	More Details
CVE-2021-25913	Prototype pollution vulnerability in 'set-or-get' version 1.0.0 through 1.2.10 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15798	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V16 Update 3a), SIMATIC HMI KTP Mobile Panels (All versions < V16 Update 3a), SINAMICS GH150 (All versions), SINAMICS GL150 (with option X30) (All versions), SINAMICS GM150 (with option X30) (All versions), SINAMICS SH150 (All versions), SINAMICS SL150 (All versions), SINAMICS SM120 (All versions), SINAMICS SM150 (All versions), SINAMICS SM150i (All versions). Affected devices with enabled telnet service do not require authentication for this service. This could allow a remote attacker to gain full access to the device. (ZDI-CAN-12046)	9.8	More Details
CVE-2020-10857	Zulip Desktop before 5.0.0 improperly uses shell.openExternal and shell.openItem with untrusted content, leading to remote code execution.	9.8	More Details
CVE-2021-25139	A potential security vulnerability has been identified in the HPE Moonshot Provisioning Manager v1.20. The HPE Moonshot Provisioning Manager is an application that is installed in a VMWare or Microsoft Hyper-V environment that is used to setup and configure an HPE Moonshot 1500 chassis. This vulnerability could be remotely exploited by an unauthenticated user to cause a stack based buffer overflow using user supplied input to the `khuploadfile.cgi` CGI ELF. The stack based buffer overflow could lead to Remote Code Execution, Denial of Service, and/or compromise system integrity. **Note:** HPE recommends that customers discontinue the use of the HPE Moonshot Provisioning Manager. The HPE Moonshot Provisioning Manager application is discontinued, no longer supported, is not available to download from the HPE Support Center, and no patch is available.	9.8	More Details
CVE-2021-25140	A potential security vulnerability has been identified in the HPE Moonshot Provisioning Manager v1.20. The HPE Moonshot Provisioning Manager is an application that is installed in a VMWare or Microsoft Hyper-V environment that is used to setup and configure an HPE Moonshot 1500 chassis. This vulnerability could be remotely exploited by an unauthenticated user to cause a directory traversal in user supplied input to the `khuploadfile.cgi` CGI ELF. The directory traversal could lead to Remote Code Execution, Denial of Service, and/or compromise system integrity. **Note:** HPE recommends that customers discontinue the use of the HPE Moonshot Provisioning Manager. The HPE Moonshot Provisioning Manager application is discontinued, no longer supported, is not available to download from the HPE Support Center, and no patch is available.	9.8	More Details
CVE-2019-17582	A use-after-free in the _zip_dirent_read function of zip_dirent.c in libzip 1.2.0 allows attackers to have an unspecified impact by attempting to unzip a malformed ZIP archive. NOTE: the discoverer states "This use-after-free is triggered prior to the double free reported in CVE-2017-12858."	9.8	More Details
CVE-2020-13117	Wavlink WN575A4 and WN579X3 devices through 2020-05-15 allow unauthenticated remote users to inject commands via the key parameter in a login request.	9.8	More Details
CVE-2021-26937	encoding.c in GNU Screen through 4.8.0 allows remote attackers to cause a denial of service (invalid write access and application crash) or possibly have unspecified other impact via a crafted UTF-8 character sequence.	9.8	More Details
CVE-2020-14343	A vulnerability was discovered in the PyYAML library in versions before 5.4, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. This flaw allows an attacker to execute arbitrary code on the system by abusing the python/object/new constructor. This flaw is due to an incomplete fix for CVE-2020-1747.	9.8	More Details
CVE-2021-21502	Dell PowerScale OneFS versions 8.1.0 – 9.1.0 contain a "use of SSH key past account expiration" vulnerability. A user on the network with the ISI_PRIV_AUTH_SSH RBAC privilege that has an expired account may potentially exploit this vulnerability, giving them access to the same things they had before account expiration. This may by a high privileged account and hence Dell recommends customers upgrade at the earliest opportunity.	9.8	More Details
CVE-2021-26951	An issue was discovered in the calamine crate before 0.17.0 for Rust. It allows attackers to overwrite heap-memory locations because Vec::set_len is used without proper memory claiming, and this uninitialized memory is used for a user-provided Read operation, as demonstrated by Sectors::get.	9.8	More Details
CVE-2021-26955	An issue was discovered in the xcb crate through 2021-02-04 for Rust. It has a soundness violation because xcb::xproto::GetAtomNameReply::name() calls std::str::from_utf8_unchecked() on unvalidated bytes from an X server.	9.8	More Details
CVE-2021-26956	An issue was discovered in the xcb crate through 2021-02-04 for Rust. It has a soundness violation because bytes from an X server can be interpreted as any data type returned by xcb::xproto::GetPropertyReply::value.	9.8	More Details
CVE-2021-3122	CMCAgent in NCR Command Center Agent 16.3 on Aloha POS/BOH servers permits the submission of a runCommand parameter (within an XML document sent to port 8089) that enables the remote, unauthenticated execution of an arbitrary command as SYSTEM, as exploited in the wild in 2020 and/or 2021. NOTE: the vendor's position is that exploitation occurs only on devices with a certain "misconfiguration."	9.8	More Details
CVE-2020-26051	College Management System Php 1.0 suffers from SQL injection vulnerabilities in the index.php page from POST parameters 'unametxt' and 'pwdtxt', which are not filtered before passing a SQL query.	9.8	More Details
CVE-2021-3311	An issue was discovered in October through build 471. It reactivates an old session ID (which had been invalid after a logout) once a new login occurs. NOTE: this violates the intended Auth/Manager.php authentication behavior but, admittedly, is only relevant if an old session ID is known to an attacker.	9.8	More Details
CVE-2021-1290	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2020-28653	Zoho ManageEngine OpManager Stable build before 125203 (and Released build before 125233) allows Remote Code Execution via the Smart Update Manager (SUM) servlet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2507	The vulnerability have been reported to affect earlier versions of QTS. If exploited, this command injection vulnerability could allow remote attackers to run arbitrary commands. This issue affects: QNAP Systems Inc. Helpdesk versions prior to 3.0.3.	9.8	More Details
CVE-2020-35481	SolarWinds Serv-U before 15.2.2 allows Unauthenticated Macro Injection.	9.8	More Details
CVE-2021-25770	In JetBrains YouTrack before 2020.5.3123, server-side template injection (SSTI) was possible, which could lead to code execution.	9.8	More Details
CVE-2020-17523	Apache Shiro before 1.7.1, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.	9.8	More Details
CVE-2021-25274	The Collector Service in SolarWinds Orion Platform before 2020.2.4 uses MSMQ (Microsoft Message Queue) and doesn't set permissions on its private queues. As a result, remote unauthenticated clients can send messages to TCP port 1801 that the Collector Service will process. Additionally, upon processing of such messages, the service deserializes them in insecure manner, allowing remote arbitrary code execution as LocalSystem.	9.8	More Details
CVE-2021-3401	Bitcoin Core before 0.19.0 might allow remote attackers to execute arbitrary code when another application unsafely passes the -platformpluginpath argument to the bitcoin-qt program, as demonstrated by an x-scheme-handler/bitcoin handler for a .desktop file or a web browser. NOTE: the discoverer states "I believe that this vulnerability cannot actually be exploited."	9.8	More Details
CVE-2021-20016	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x.	9.8	More Details
CVE-2021-26687	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. In preloaded applications, the HostnameVerified default is mishandled. The LG ID is LVE-SMP-200029 (February 2021).	9.8	More Details
CVE-2021-26688	An issue was discovered on LG Wing mobile devices with Android OS 10 software. The biometric sensor has weak security properties. The LG ID is LVE-SMP-200030 (February 2021).	9.8	More Details
CVE-2021-26689	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. The USB laf gadget has a use-after-free. The LG ID is LVE-SMP-200031 (February 2021).	9.8	More Details
CVE-2020-14245	HCL OneTest UI V9.5, V10.0, and V10.1 does not perform authentication for functionality that either requires a provable user identity or consumes a significant amount of resources.	9.8	More Details
CVE-2021-1289	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2021-26957	An issue was discovered in the xcb crate through 2021-02-04 for Rust. It has a soundness violation because there is an out-of-bounds read in xcb::xproto::change_property(), as demonstrated by a format=32 T=u8 situation where out-of-bounds bytes are sent to an X server.	9.8	More Details
CVE-2021-1291	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2021-1293	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2021-20623	Video Insight VMS versions prior to 7.8 allows a remote attacker to execute arbitrary code with the system user privilege by sending a specially crafted request.	9.8	More Details
CVE-2020-18717	SQL Injection in ZZZCMS zzzphp 1.7.1 allows remote attackers to execute arbitrary code due to a lack of parameter filtering in inc/zzz_template.php.	9.8	More Details
CVE-2020-18716	SQL Injection in Rockoa v1.8.7 allows remote attackers to gain privileges due to loose filtering of parameters in wordAction.php.	9.8	More Details
CVE-2020-18714	SQL Injection in Rockoa v1.8.7 allows remote attackers to gain privileges due to loose filtering of parameters in wordModel.php's getdata function.	9.8	More Details
CVE-2020-18713	SQL Injection in Rockoa v1.8.7 allows remote attackers to gain privileges due to loose filtering of parameters in customerAction.php	9.8	More Details
CVE-2020-10539	An issue was discovered in Epikur before 20.1.1. The Epikur server contains the checkPassword() function that, upon user login, checks the submitted password against the user password's MD5 hash stored in the database. It is also compared to a second MD5 hash, which is the same for every user (aka a "Backdoor Password" of 3p1kursupport). If the submitted password matches either one, access is granted.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1295	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2021-1294	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2021-1292	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	9.8	More Details
CVE-2021-21146	Use after free in Navigation in Google Chrome prior to 88.0.4324.146 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-35125	A cross-site scripting (XSS) vulnerability in the forms component of Mautic before 3.2.4 allows remote attackers to inject executable JavaScript via mautic[return] (a different attack method than CVE-2020-35124, but also related to the Referer concept).	9.6	More Details
CVE-2021-21142	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21132	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2021-21121	Use after free in Omnibox in Google Chrome on Linux prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21124	Potential user after free in Speech Recognizer in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-26530	The mg_tls_init function in Cesanta Mongoose HTTPS server 7.0 (compiled with OpenSSL support) is vulnerable to remote OOB write attack via connection request after exhausting memory pool.	9.1	More Details
CVE-2020-28645	Deleting users with certain names caused system files to be deleted. Risk is higher for systems which allow users to register themselves and have the data directory in the web root. This affects ownCloud/core versions < 10.6.	9.1	More Details
CVE-2021-26528	The mg_http_serve_file function in Cesanta Mongoose HTTP server 7.0 is vulnerable to remote OOB write attack via connection request after exhausting memory pool.	9.1	More Details
CVE-2021-26529	The mg_tls_init function in Cesanta Mongoose HTTPS server 7.0 and 6.7-6.18 (compiled with mbedTLS support) is vulnerable to remote OOB write attack via connection request after exhausting memory pool.	9.1	More Details
CVE-2021-21479	In SCIMono before 0.0.19, it is possible for an attacker to inject and execute java expression compromising the availability and integrity of the system.	9.1	More Details
CVE-2020-36242	In the cryptography package before 3.3.2 for Python, certain sequences of update calls to symmetrically encrypt multi-GB values could result in an integer overflow and buffer overflow, as demonstrated by the Fernet class.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	
CVE-2021-21119	Use after free in Media in Google Chrome prior to 88.0.4324.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corru
CVE-2021-3394	Millennium Millewin (also known as "Cartella clinica") 13.39.028, 13.39.28.3342, and 13.39.146.1 has insecure folder permissions allowing a malicious user for a local p
CVE-2021-21122	Use after free in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-3191	Idelji Web ViewPoint Suite, as used in conjunction with HPE NonStop, allows Remote Unauthorized Access for T0320L01^ABY and T0320L01^ACD, T0952L01^AAR t

CVE Number	
CVE-2020-35942	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload and Local File Inclusion via settings modifica
CVE-2021-26675	A stack-based buffer overflow in dnsproxy in ConnMan before 1.39 could be used by network adjacent attackers to execute code.
CVE-2021-21148	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21127	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass content security policy via a crafted Chrome
CVE-2021-26958	An issue was discovered in the xcb crate through 2021-02-04 for Rust. It has a soundness violation because transmutation to the wrong type can happen after xcb::bas
CVE-2021-21128	Heap buffer overflow in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-20652	Cross-site request forgery (CSRF) vulnerability in Name Directory 1.17.4 and earlier allows remote attackers to hijack the authentication of administrators via unspecifie
CVE-2020-35765	doFilter in com.adventnet.appmanager.filter.UriCollector in Zoho ManageEngine Applications Manager through 14930 allows an authenticated SQL Injection via the res
CVE-2020-27259	The Omron CX-One Version 4.60 and prior may allow an attacker to supply a pointer to arbitrary memory locations, which may allow an attacker to remotely execute ar
CVE-2020-27261	The Omron CX-One Version 4.60 and prior is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.
CVE-2021-21143	Heap buffer overflow in Extensions in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially ex
CVE-2021-25765	In JetBrains YouTrack before 2020.4.4701, CSRF via attachment upload was possible.
CVE-2021-21144	Heap buffer overflow in Tab Groups in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially e:
CVE-2021-21120	Use after free in WebSQL in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21145	Use after free in Fonts in Google Chrome prior to 88.0.4324.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-18215	Multiple SQL Injection vulnerabilities in PHPSHE 1.7 in phpshe/admin.php via the (1) ad_id, (2) menu_id, and (3) cashout_id parameters, which could let a remote mali
CVE-2020-36152	Buffer overflow in readDataVar in hdf/dataobject.c in Symonics libmysofa 0.5 - 1.1 allows attackers to execute arbitrary code via a crafted SOFA.
CVE-2020-16044	Use after free in WebRTC in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.
CVE-2020-29163	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by SQL injection.

CVE Number	
CVE-2020-13460	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities were present in Tufin SecureTrack, affecting all versions prior to R20-2 GA.
CVE-2020-36243	The Patient Portal of OpenEMR 5.0.2.1 is affected by a Command Injection vulnerability in /interface/main/backup.php. To exploit the vulnerability, an authenticated att
CVE-2020-35700	A second-order SQL injection issue in Widgets/TopDevicesController.php (aka the Top Devices dashboard widget) of LibreNMS before 21.1.0 allows remote authentica
CVE-2021-21472	SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1) does not have an option to set password during its installation, this all
CVE-2021-26551	An issue was discovered in SmartFoxServer 2.17.0. An attacker can execute arbitrary Python code, and bypass the javashell.py protection mechanism, by creating /co
CVE-2021-21118	Insufficient data validation in V8 in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform out of bounds memory access via a crafted H
CVE-2020-27872	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R7450 1.2.0.62_1.0.1 routers. Authentication is not execute code in the context of root. Was ZDI-CAN-11365.
CVE-2020-28449	This affects all versions of package decal. The vulnerability is in the set function.
CVE-2020-28450	This affects all versions of package decal. The vulnerability is in the extend function.
CVE-2021-1288	Multiple vulnerabilities in the ingress packet processing function of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service
CVE-2021-21138	Use after free in DevTools in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform a sandbox escape via a crafted file.
CVE-2021-1313	Multiple vulnerabilities in the ingress packet processing function of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service
CVE-2020-24685	An unauthenticated specially crafted packet sent by an attacker over the network will cause a denial-of-service (DoS) vulnerability. Vulnerability allows attacker to stop t
CVE-2020-4795	IBM Security Identity Governance and Intelligence 5.2.6 could disclose sensitive information to an unauthorized user using a specially crafted HTTP request. IBM X-For
CVE-2020-25856	The function DecWPA2KeyData() in the Realtek RTL8195A Wi-Fi Module prior to versions released in April 2020 (up to and excluding 2.08) does not validate the size p handshake. The attacker needs to know the network's PSK in order to exploit this.
CVE-2020-25237	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP1 Update 1), SINEMA Server (All versions < V14.0 SP2 Update 2). When uploading files to an as 'Zip-Slip'. (ZDI-CAN-12054)
CVE-2021-21125	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a
CVE-2020-10552	An issue was discovered in Psyprax before 3.2.2. The Firebird database is accessible with the default user sysdba and password masterke after installation. This allows
CVE-2020-25854	The function DecWPA2KeyData() in the Realtek RTL8195A Wi-Fi Module prior to versions released in April 2020 (up to and excluding 2.08) does not validate the size p injecting a crafted packet into the WPA2 handshake. The attacker needs to know the network's PSK in order to exploit this.

CVE Number	
CVE-2021-26915	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization
CVE-2021-26914	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization
CVE-2021-26913	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization
CVE-2021-26220	The ezxml_toxml function in ezxml 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.
CVE-2021-26221	The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.
CVE-2021-26222	The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.
CVE-2020-25855	The function AES_UnWRAP() in the Realtek RTL8195A Wi-Fi Module prior to versions released in April 2020 (up to and excluding 2.08) does not validate the size para attacker needs to know the network's PSK in order to exploit this.
CVE-2021-26912	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization
CVE-2020-12122	In Max Secure Max Spyware Detector 1.0.0.044, the driver file (MaxProc64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified otl
CVE-2021-21117	Insufficient policy enforcement in Cryptohome in Google Chrome prior to 88.0.4324.96 allowed a local attacker to perform OS-level privilege escalation via a crafted file
CVE-2021-25171	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetlicensecfg funct
CVE-2021-25170	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetremoteimageint
CVE-2020-27001	A vulnerability has been identified in JT2Go (All versions < V13.1.0.2), Teamcenter Visualization (All versions < V13.1.0.2). Affected applications lack proper validation
CVE-2020-27000	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2021-25169	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetservicecfg func
CVE-2021-25168	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webupdatecomponent
CVE-2020-25238	A vulnerability has been identified in PCS neo (Administration Console) (All versions < V3.1), TIA Portal (V15, V15.1 and V16). Manipulating certain files in specific fold
CVE-2020-25245	A vulnerability has been identified in DIGSI 4 (All versions < V4.94 SP1 HF 1). Several folders in the %PATH% are writeable by normal users. As these folders are inclu
CVE-2021-25142	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webstartflash function.

CVE Number	
CVE-2020-17432	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11335.
CVE-2021-26826	A stack overflow issue exists in Godot Engine up to v3.2 and is caused by improper boundary checks when loading .TGA image files. Depending on the context of the a
CVE-2021-26825	An integer overflow issue exists in Godot Engine up to v3.2 that can be triggered when loading specially crafted.TGA image files. The vulnerability exists in ImageLoade execution and/or system crash.
CVE-2021-22299	There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Su 6.5.0,6.5.0.SPC100.B210,6.5.1.1.B010,6.5.1.1.B020,6.5.1.1.B030,6.5.1.1.B040,6.5.1.SPC100.B050,6.5.1.SPC101.B010,6.5.1.SPC101.B040,6.5.1.SPC200,6.5.1.SPC LCND81,8.0.0.SPC100,8.0.1,8.0.RC2,8.0.RC3,8.0.RC3.B041,8.0.RC3.SPC100; NFV_FusionSphere versions 6.5.1.SPC23,8.0.0.SPC12; SMC2.0 versions V600R019
CVE-2020-26191	Dell EMC PowerScale OneFS versions 8.1.0 - 9.1.0 contain a privilege escalation vulnerability. A user with ISI_PRIV_JOB_ENGINE may use the PermissionRepair job
CVE-2020-18750	Buffer overflow in pdf2json 0.69 allows local users to execute arbitrary code by converting a crafted PDF file.
CVE-2020-27005	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2020-28392	A vulnerability has been identified in SIMARIS configuration (All versions < V4.0.1). During installation to default target folder, incorrect permissions are configured for tl
CVE-2021-25758	In JetBrains IntelliJ IDEA before 2020.3, potentially insecure deserialization of the workspace model could lead to local code execution.
CVE-2020-26192	Dell EMC PowerScale OneFS versions 8.2.0 - 9.1.0 contain a privilege escalation vulnerability. A non-admin user with either ISI_PRIV_LOGIN_CONSOLE or ISI_PRIV
CVE-2020-10537	An issue was discovered in Epikur before 20.1.1. A Glassfish 4.1 server with a default configuration is running on TCP port 4848. No password is required to access it v
CVE-2021-25249	An out-of-bounds write information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.(
CVE-2020-27257	This vulnerability allows local attackers to execute arbitrary code due to the lack of proper validation of user-supplied data, which can result in a type-confusion conditio
CVE-2020-27857	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11488.
CVE-2020-27856	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11434.
CVE-2020-27855	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11433.
CVE-2020-17436	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11432.
CVE-2020-17435	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11358.
CVE-2020-17434	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11357.

CVE Number	
CVE-2020-26193	Dell EMC PowerScale OneFS versions 8.1.0 - 9.1.0 contain an improper input validation vulnerability. A user with the ISI_PRIV_CLUSTER privilege may exploit this vu
CVE-2020-17433	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11356.
CVE-2020-27003	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2020-26999	A vulnerability has been identified in JT2Go (All versions < V13.1.0.2), Teamcenter Visualization (All versions < V13.1.0.2). Affected applications lack proper validation
CVE-2020-27006	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2021-26577	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so uploadsshkey function
CVE-2021-26573	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgeneratesslcfg fun
CVE-2021-26570	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webifc_setadconfig fun
CVE-2020-17419	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11192.
CVE-2020-17421	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11194.
CVE-2021-26574	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletevideof
CVE-2020-17423	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11196.
CVE-2021-26575	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletesolvid
CVE-2020-17424	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11247.
CVE-2020-13579	An exploitable integer overflow vulnerability exists in the PlanMaker document parsing functionality of SoftMaker Office 2021's PlanMaker application. A specially crafte corruptions can allow for code execution under the context of the application. An attacker can entice the victim to open a document to trigger this vulnerability.
CVE-2020-17425	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11259.
CVE-2020-17426	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vu leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11230.
CVE-2021-26910	Firejail before 0.9.64.4 allows attackers to bypass intended access restrictions because there is a TOCTOU race condition between a stat operation and an OverlayFS
CVE-2021-25275	SolarWinds Orion Platform before 2020.2.4, as used by various SolarWinds products, installs and uses a SQL Server backend, and stores database credentials to acce SWNetPerfMon.DB database. This gives access to the data collected by SolarWinds applications, and leads to admin access to the applications by inserting or changir

CVE Number	
CVE-2020-17427	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this v attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11334.
CVE-2020-17429	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11337.
CVE-2021-26576	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so uploadsshk
CVE-2020-17418	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this v in the context of the current process. Was ZDI-CAN-11197.
CVE-2021-1370	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running NCS540 could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level
CVE-2020-27249	A specially crafted document can cause the document parser to copy data from a particular record type into a static-sized buffer within an object that is smaller than the
CVE-2020-17431	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this v attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11333.
CVE-2020-13580	An exploitable heap-based buffer overflow vulnerability exists in the PlanMaker document parsing functionality of SoftMaker Office 2021's PlanMaker application. A spe of the buffer and controllably corrupt memory. This can allow an attacker to earn code execution under the context of the application. An attacker can entice the victim t
CVE-2020-13586	A memory corruption vulnerability exists in the Excel Document SST Record 0x00fc functionality of SoftMaker Software GmbH SoftMaker Office PlanMaker 2021 (Revi
CVE-2020-17430	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this v attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11332.
CVE-2020-27248	A specially crafted document can cause the document parser to copy data from a particular record type into a static-sized buffer within an object that is smaller than the
CVE-2020-27247	A specially crafted document can cause the document parser to copy data from a particular record type into a static-sized buffer within an object that is smaller than the
CVE-2021-26571	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg func
CVE-2021-25172	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so websetdefa
CVE-2021-22663	Cscape (All versions prior to 9.90 SP3.5) lacks proper validation of user-supplied data when parsing project files. This could lead to an out-of-bounds read. An attacker
CVE-2021-26572	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg func
CVE-2021-22293	Some Huawei products have an inconsistent interpretation of HTTP requests vulnerability. Attackers can exploit this vulnerability to cause information leak. Affected pro
CVE-2021-25837	Cosmos Network Ethermint <= v0.4.0 is affected by cache lifecycle inconsistency in the EVM module. Due to the inconsistency between the Storage caching cycle and
CVE-2020-24944	picoquic (before 3rd of July 2020) allows attackers to cause a denial of service (infinite loop) via a crafted QUIC frame, related to the picoquic_decode_frames and pico

CVE Number	
CVE-2021-25769	In JetBrains YouTrack before 2020.4.6808, the YouTrack administrator wasn't able to access attachments.
CVE-2021-0351	In wlan driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges neede
CVE-2020-17516	Apache Cassandra versions 2.1.0 to 2.1.22, 2.2.0 to 2.2.19, 3.0.0 to 3.0.23, and 3.11.0 to 3.11.9, when using 'dc' or 'rack' internode_encryption setting, allows both enc
CVE-2021-25835	Cosmos Network Ethermint <= v0.4.0 is affected by a cross-chain transaction replay vulnerability in the EVM module. Since ethermint uses the same chainIDEpoch an
CVE-2021-25836	Cosmos Network Ethermint <= v0.4.0 is affected by cache lifecycle inconsistency in the EVM module. The bytecode set in a FAILED transaction wrongfully remains in r
CVE-2021-22292	There is a denial of service (DoS) vulnerability in eCNS280 versions V100R005C00, V100R005C10. Due to a design defect, remote unauthorized attackers send a larg
CVE-2021-25834	Cosmos Network Ethermint <= v0.4.0 is affected by a transaction replay vulnerability in the EVM module. If the victim sends a very large nonce transaction, the attacke
CVE-2020-8806	Electric Coin Company Zcashd before 2.1.1-1 allows attackers to trigger consensus failure and double spending. A valid chain could be incorrectly rejected because tim
CVE-2021-21240	httplib2 is a comprehensive HTTP client library for Python. In httplib2 before version 0.19.0, a malicious server which responds with long series of "\xa0" characters in th
CVE-2021-3382	Stack buffer overflow vulnerability in gitea 1.9.0 through 1.13.1 allows remote attackers to cause a denial of service (crash) via vectors related to a file path.
CVE-2020-35667	JetBrains TeamCity Plugin before 2020.2.85695 SSRF. Vulnerability that could potentially expose user credentials.
CVE-2020-10554	An issue was discovered in Psyprax beforee 3.2.2. Passwords used to encrypt the data are stored in the database in an obfuscated format, which can be easily reverte
CVE-2021-3229	Denial of service in ASUSWRT ASUS RT-AX3000 firmware versions 3.0.0.4.384_10177 and earlier versions allows an attacker to disrupt the use of device setup servic
CVE-2020-27222	In Eclipse Californium version 2.3.0 to 2.6.0, the certificate based (x509 and RPK) DTLS handshakes accidentally fails, because the DTLS server side sticks to a wrong
CVE-2021-21475	Under specific circumstances SAP Master Data Management, versions - 710, 710.750, allows an unauthorized attacker to exploit insufficient validation of path informat
CVE-2021-26843	An issue was discovered in sthttpd through 2.27.1. On systems where the strcpy function is implemented with memcpy, the de_dotdot function may cause a Denial-of-S
CVE-2020-29166	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by file read/manipulation, which can result in remote information disclosure.
CVE-2020-25853	The function CheckMic() in the Realtek RTL8195A Wi-Fi Module prior to versions released in April 2020 (up to and excluding 2.08) does not validate the size paramete WPA2 handshake. The attacker does not need to know the network's PSK.
CVE-2020-6088	An exploitable denial of service vulnerability exists in the ENIP Request Path Network Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially c

CVE Number	
CVE-2021-1296	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow ar management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite fil
CVE-2021-1297	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow ar management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite fil
CVE-2021-26952	An issue was discovered in the ms3d crate before 0.1.3 for Rust. It might allow attackers to obtain sensitive information from uninitialized memory locations via IoReade
CVE-2020-25857	The function ClientEAPOLKeyRecvd() in the Realtek RTL8195A Wi-Fi Module prior to versions released in April 2020 (up to and excluding 2.08) does not validate the s not need to know the network's PSK.
CVE-2021-26953	An issue was discovered in the postscript crate before 0.14.0 for Rust. It might allow attackers to obtain sensitive information from uninitialized memory locations via a u
CVE-2021-25776	In JetBrains TeamCity before 2020.2, an ECR token could be exposed in a build's parameters.
CVE-2020-14246	HCL OneTest Performance V9.5, V10.0, V10.1 uses basic authentication which is relatively weak. An attacker could potentially decode the encoded credentials.
CVE-2021-1268	A vulnerability in the IPv6 protocol handling of the management interfaces of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause an IPv exploit this vulnerability by connecting to the same network as the management interfaces and injecting IPv6 packets that have an IPv6 node-local multicast group addı or a denial of service (DoS) condition.
CVE-2021-21305	CarrierWave is an open-source RubyGem which provides a simple and flexible way to upload files from Ruby applications. In CarrierWave before versions 1.3.2 and 2. to remote code execution(RCE). This is fixed in versions 1.3.2 and 2.1.1.
CVE-2020-2506	The vulnerability have been reported to affect earlier versions of QTS. If exploited, this improper access control vulnerability could allow attackers to compromise the se
CVE-2020-28895	In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allo
CVE-2021-21304	Dynamoose is an open-source modeling tool for Amazon's DynamoDB. In Dynamoose from version 2.0.0 and before version 2.7.0 there was a prototype pollution vulne since the vulnerable method was added as part of the v2 rewrite. This vulnerability also impacts v2.x.x beta/alpha versions. Version 2.7.0 includes a patch for this vulne
CVE-2021-1332	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1321	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1334	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1331	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1335	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1333	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1348	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system

CVE Number	
CVE-2021-1316	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit the
CVE-2021-1330	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1329	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1328	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1327	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1326	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1322	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1323	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1324	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1325	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1319	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1346	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1344	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1343	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1347	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1342	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1341	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1340	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1339	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system

CVE Number	
CVE-2021-1315	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit the
CVE-2021-1338	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1320	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1337	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1314	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit the
CVE-2021-1318	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit the
CVE-2021-1336	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2021-1317	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit the
CVE-2021-1345	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system
CVE-2020-27002	A vulnerability has been identified in JT2Go (All versions < V13.1.0.2), Teamcenter Visualization (All versions < V13.1.0.2). Affected applications lack proper validation
CVE-2021-22302	There is an out-of-bound read vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module does not verify the some input. Attackers can exploit this vulnerability by
CVE-2021-25276	In SolarWinds Serv-U before 15.2.2 Hotfix 1, there is a directory containing user profile files (that include users' password hashes) that is world readable and writable. A LocalSystem privileges.
CVE-2021-26708	A local privilege escalation was discovered in the Linux kernel before 5.10.13. Multiple race conditions in the AF_VSOCK implementation are caused by wrong locking
CVE-2020-26194	Dell EMC PowerScale OneFS versions 8.1.2 and 8.2.2 contain an Incorrect Permission Assignment for a Critical Resource vulnerability. This may allow a non-admin us
CVE-2021-21140	Uninitialized use in USB in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform out of bounds memory access via via a USB device.
CVE-2020-9118	There is an insufficient integrity check vulnerability in Huawei Sound X Product. The system does not check certain software package's integrity sufficiently. Successful 9.0.3.1(H100SP13C00),9.0.3.1(H100SP18C00),9.0.3.1(H100SP3C00),9.0.3.1(H100SP9C00),9.0.3.2(H100SP1C00),9.0.3.2(H100SP2C00),9.0.3.2(H100SP5C00),9.0.3
CVE-2020-11915	An issue was discovered in Svakom Siime Eye 14.1.00000001.3.330.0.0.3.14. By sending a set_params.cgi?telnetd=1&save=1&reboot=1 request to the webserver, it i exploited, an attacker must be physically close in order to connect to the device's Wi-Fi access point.
CVE-2021-22301	Mate 30 10.0.0.203(C00E201R7P2) have a buffer overflow vulnerability. After obtaining the root permission, an attacker can exploit the vulnerability to cause buffer ove
CVE-2021-0359	In netdiag, 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 neede

CVE Number	
CVE-2021-0360	In netdiag, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges nee
CVE-2021-0361	In kisd, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.
CVE-2021-0364	In mobile_log_d, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges
CVE-2021-0363	In mobile_log_d, there is a possible command injection due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges
CVE-2021-0365	In display driver, 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.
CVE-2021-0362	In aee, there is a possible memory corruption due to a stack buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. Us
CVE-2021-1244	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS
CVE-2021-0356	In netdiag, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges need
CVE-2021-0343	In kisd, 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.
CVE-2021-0344	In mtkpower, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges nee
CVE-2021-0345	In mobile_log_d, there is a possible escalation of privilege due to improper input validation. This could lead to local escalation of privilege with System execution privileg
CVE-2021-0346	In vpu, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed
CVE-2021-0353	In kisd, there is a possible memory corruption due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. Us
CVE-2021-0348	In vpu, 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. U
CVE-2021-0349	In display driver, 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.
CVE-2021-0354	In ged, 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
CVE-2021-1136	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS
CVE-2021-0355	In kisd, 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
CVE-2021-0357	In netdiag, 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 need

CVE Number	
CVE-2021-0358	In netdiag, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges need
CVE-2020-36151	Incorrect handling of input data in mysofa_resampler_reset_mem function in the libmysofa library 0.5 - 1.1 will lead to heap buffer overflow and overwriting large memo
CVE-2020-36150	Incorrect handling of input data in loudness function in the libmysofa library 0.5 - 1.1 will lead to heap buffer overflow and access to unallocated memory block.
CVE-2020-36149	Incorrect handling of input data in changeAttribute function in the libmysofa library 0.5 - 1.1 will lead to NULL pointer dereference and segmentation fault error in case o
CVE-2020-36148	Incorrect handling of input data in verifyAttribute function in the libmysofa library 0.5 - 1.1 will lead to NULL pointer dereference and segmentation fault error in case of r
CVE-2021-20359	IBM Cloud Pak for Automation 20.0.3, 20.0.2-IF002 - Business Automation Application Designer Component stores potentially sensitive information in log files that coul
CVE-2021-20358	IBM Cloud Pak for Automation 20.0.3, 20.0.2-IF002 stores potentially sensitive information in clear text in API connection log files. This information could be obtained b
CVE-2021-26905	1Password SCIM Bridge before 1.6.2 mishandles validation of authenticated requests for log files, leading to disclosure of a TLS private key.
CVE-2020-9388	CSRF protection was not present in SquaredUp before version 4.6.0. A CSRF attack could have been possible by an administrator executing arbitrary code in a HTML
CVE-2021-21474	SAP HANA Database, versions - 1.0, 2.0, accepts SAML tokens with MD5 digest, an attacker who manages to obtain an MD5-digest signed SAML Assertion issued fo
CVE-2020-27873	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR R7450 1.2.0.62_1.0.1 routers. Authenticatio further compromise. Was ZDI-CAN-11559.
CVE-2020-4828	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 is vulnerable to web cache poisoning, caused by improper input validation by modifyin
CVE-2020-14247	HCL OneTest Performance V9.5, V10.0, V10.1 contains an inadequate session timeout, which could allow an attacker time to guess and use a valid session ID.
CVE-2021-21139	Inappropriate implementation in iframe sandbox in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass navigation restrictions via a crafted HTML
CVE-2021-21129	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTM
CVE-2021-22161	In OpenWrt 19.07.x before 19.07.7, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream I the netifd and odhcp6c packages.
CVE-2021-21131	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTM
CVE-2020-10234	The AscRegistryFilter.sys kernel driver in IObit Advanced SystemCare 13.2 allows an unprivileged user to send an IOCTL to the device driver. If the user provides a NU 0x8001E048. \DosDevices\AscRegistryFilter and \Device\AscRegistryFilter are affected.
CVE-2021-21126	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension

CVE Number	
CVE-2021-21133	Insufficient policy enforcement in Downloads in Google Chrome prior to 88.0.4324.96 allowed an attacker who convinced a user to download files to bypass navigation
CVE-2021-21123	Insufficient data validation in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML pa
CVE-2020-35943	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload. (It is possible to bypass CSRF protection by
CVE-2021-21134	Incorrect security UI in Page Info in Google Chrome on iOS prior to 88.0.4324.96 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-27994	SolarWinds Serv-U before 15.2.2 allows Authenticated Directory Traversal.
CVE-2021-21135	Inappropriate implementation in Performance API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-25246	An improper access control information disclosure vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG SP1, and Worry-Free Business Secu
CVE-2021-21136	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML p
CVE-2021-21137	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to obtain potentially sensitive information from disk via a c
CVE-2021-25759	In JetBrains Hub before 2020.1.12629, an authenticated user can delete 2FA settings of any other user.
CVE-2021-21141	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass file extension policy via a crafted HTML
CVE-2021-26719	A directory traversal issue was discovered in Gradle gradle-enterprise-test-distribution-agent before 1.3.2, test-distribution-gradle-plugin before 1.3.2, and gradle-enterp
CVE-2020-28388	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGE TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). Initial Sequence Numbers (ISNs) for TCP connections are derived
CVE-2021-22298	There is a logic vulnerability in Huawei Gauss100 OLTP Product. An attacker with certain permissions could perform specific SQL statement to exploit this vulnerability. 6.5.1.SPC200.B030, 6.5.1.SPC200.B040, 6.5.1.SPC200.B050, 6.5.1.SPC200.B060, 6.5.1.SPC200.B070, 6.5.1RC1.B070, 6.5.1RC1.B080, 6.5.1RC2.B040, 6.5.1RC2.
CVE-2021-22500	Cross Site Request Forgery vulnerability in Micro Focus Application Performance Management product, affecting versions 9.40, 9.50 and 9.51. The vulnerability could l
CVE-2020-4790	IBM Security Identity Governance and Intelligence 5.2.6 could allow a user to cause a denial of service due to improperly validating a supplied URL, rendering the appli
CVE-2021-26921	In util/session/sessionmanager.go in Argo CD before 1.8.4, tokens continue to work even when the user account is disabled.
CVE-2021-26676	gdhcp in ConnMan before 1.39 could be used by network-adjacent attackers to leak sensitive stack information, allowing further exploitation of bugs in gdhcp.
CVE-2021-21130	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTM

CVE Number	
CVE-2021-23327	The package apexcharts before 3.24.0 are vulnerable to Cross-site Scripting (XSS) via lack of sanitization of graph legend fields.
CVE-2021-21290	Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissi written to this file, other local users can read this information. This is the case in netty's "AbstractDiskHttpData" is vulnerable. This has been fixed in version 4.1.59.Fina
CVE-2021-3333	Opmantek Open-AudIT 4.0.1 is affected by cross-site scripting (XSS). When outputting SQL statements for debugging, a maliciously crafted query can trigger an XSS a
CVE-2021-26723	Jenzabar 9.2.x through 9.2.2 allows /ics?tool=search&query= XSS.
CVE-2020-13947	An instance of a cross-site scripting vulnerability was identified to be present in the web based administration console on the message.jsp page of Apache ActiveMQ ve
CVE-2020-22839	Reflected cross-site scripting vulnerability (XSS) in the evoadm.php file in b2evolution cms version 6.11.6-stable allows remote attackers to inject arbitrary webscript or
CVE-2021-21476	SAP UI5 versions before 1.38.49, 1.52.49, 1.60.34, 1.71.31, 1.78.18, 1.84.5, 1.85.4, 1.86.1 allows an unauthenticated attacker to redirect users to a malicious site due
CVE-2021-21478	SAP Web Dynpro ABAP allow an attacker to redirect users to a malicious site due to Reverse Tabnabbing vulnerabilities.
CVE-2021-26916	In nopCommerce 4.30, a Reflected XSS issue in the Discount Coupon component allows remote attackers to inject arbitrary web script or HTML through the Filters/Che
CVE-2021-22122	An improper neutralization of input during web page generation in FortiWeb GUI interface 6.3.0 through 6.3.7 and version before 6.2.4 may allow an unauthenticated, re
CVE-2021-21444	SAP Business Objects BI Platform, versions - 410, 420, 430, allows multiple X-Frame-Options headers entries in the response headers, which may not be predictably t
CVE-2020-29164	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by cross-site scripting (XSS).
CVE-2020-22840	Open redirect vulnerability in b2evolution CMS version prior to 6.11.6 allows an attacker to perform malicious open redirects to an attacker controlled resource via redir
CVE-2021-25773	JetBrains TeamCity before 2020.2 was vulnerable to reflected XSS on several pages.
CVE-2020-35572	Adminer through 4.7.8 allows XSS via the history parameter to the default URI.
CVE-2021-26722	LinkedIn Oncall through 1.4.0 allows reflected XSS via /query because of mishandling of the "No results found for" message in the search bar.
CVE-2021-25757	In JetBrains Hub before 2020.1.12629, an open redirect was possible.
CVE-2021-26023	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to XSS.
CVE-2021-26710	A cross-site scripting (XSS) issue in the login panel in Redwood Report2Web 4.3.4.5 and 4.5.3 allows remote attackers to inject JavaScript via the signIn.do urll parame

CVE Number	
CVE-2020-18737	An issue was discovered in Typora 0.9.67. There is an XSS vulnerability that causes Remote Code Execution.
CVE-2021-1072	NVIDIA GeForce Experience, all versions prior to 3.21, contains a vulnerability in GameStream (rxdiag.dll) where an arbitrary file deletion due to improper handling of lo
CVE-2020-13409	Tufin SecureTrack < R20-2 GA contains reflected + stored XSS (as in, the value is reflected back to the user, but is also stored within the DB and can be later triggered elevating privileges and obtaining admin access. (issue 3 of 3)
CVE-2020-13408	Tufin SecureTrack < R20-2 GA contains reflected + stored XSS (as in, the value is reflected back to the user, but is also stored within the DB and can be later triggered elevating privileges and obtaining admin access. (issue 2 of 3)
CVE-2020-13407	Tufin SecureTrack < R20-2 GA contains reflected + stored XSS (as in, the value is reflected back to the user, but is also stored within the DB and can be later triggered elevating privileges and obtaining admin access. (issue 1 of 3)
CVE-2021-22267	Idelji Web ViewPoint Suite, as used in conjunction with HPE NonStop, allows a remote replay attack for T0320L01^ABP through T0320L01^ABZ, T0952L01^AAH throu
CVE-2020-14312	A flaw was found in the default configuration of dnsmasq, as shipped with Fedora versions prior to 31 and in all versions Red Hat Enterprise Linux, where it listens on a conduct a Distributed Denial of Service (DDoS) against other systems.
CVE-2020-5812	Nessus AMI versions 8.12.0 and earlier were found to either not validate, or incorrectly validate, a certificate which could allow an attacker to spoof a trusted entity by u
CVE-2021-21303	Helm is open-source software which is essentially "The Kubernetes Package Manager". Helm is a tool for managing Charts. Charts are packages of pre-configured Kub without sanitizing. Helm fails to properly sanitized some fields present on Helm repository `index.yaml` files. Helm does not properly sanitized some fields in the `plugin. on the screen. In some cases, we could send codes that terminals used to execute higher-order logic, like clearing a terminal screen. Further, during evaluation, the He Those who use Helm as a library should verify that they either sanitize this data on their own, or use the proper Helm API calls to sanitize the data.
CVE-2021-1389	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote atta traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.
CVE-2020-13462	Insecure Direct Object Reference (IDOR) exists in Tufin SecureChange, affecting all versions prior to R20-2 GA. Fixed in version R20-2 GA.
CVE-2021-21435	Article Bcc fields and agent personal information are shown when customer prints the ticket (PDF) via external interface. This issue affects: OTRS AG OTRS 7.0.x vers
CVE-2020-16144	When using an object storage like S3 as the file store, when a user creates a public link to a folder where anonymous users can upload files, and another user uploads
CVE-2020-10538	An issue was discovered in Epikur before 20.1.1. It stores the secret passwords of the users as MD5 hashes in the database. MD5 can be brute-forced efficiently and s
CVE-2020-9453	In Epson iProjection v2.30, the driver file EMP_MPAU.sys allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of
CVE-2020-10553	An issue was discovered in Psyprax before 3.2.2. The file %PROGRAMDATA%\Psyprax32\PPScreen.ini contains a hash for the lockscreen (aka screensaver) of the a
CVE-2020-9014	In Epson iProjection v2.30, the driver file (EMP_NSAU.sys) allows local users to cause a denial of service (BSOD) via crafted input to the virtual audio device driver witl
CVE-2020-4832	IBM PowerHA 7.2 could allow a local attacker to obtain sensitive information from temporary directories after a discovery failure occurs. IBM X-Force ID: 189969.
CVE-2020-36241	autoar-extractor.c in GNOME gnome-autoar through 0.2.4, as used by GNOME Shell, Nautilus, and other software, allows Directory Traversal during extraction becaus

CVE Number	
CVE-2020-10375	An issue was discovered in New Media Smarty before 9.10. Passwords are stored in the database in an obfuscated format that can be easily reversed. The file data.m
CVE-2020-11836	OPPO Android Phone with MTK chipset and Android 8.1/9/10/11 versions have an information leak vulnerability. The “adb shell getprop ro.vendor.aee.enforcing” or “ac
CVE-2020-27008	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2020-27007	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2020-27004	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2021-1128	A vulnerability in the CLI parser of Cisco IOS XR Software could allow an authenticated, local attacker to view more information than their privileges allow. The vulnerat configuration that otherwise might not have been accessible beyond the privileges of the invoking user.
CVE-2020-26998	A vulnerability has been identified in JT2Go (All versions < V13.1.0.2), Teamcenter Visualization (All versions < V13.1.0.2). Affected applications lack proper validation
CVE-2020-4996	IBM Security Identity Governance and Intelligence 5.2.6 could allow a local user to obtain sensitive information via the capturing of screenshots of authentication creder
CVE-2020-10048	A vulnerability has been identified in SIMATIC PCS 7 (All versions), SIMATIC WinCC (All versions < V7.5 SP2). Due to an insecure password verification process, an a
CVE-2020-8587	OnCommand System Manager 9.x versions prior to 9.3P20 and 9.4 prior to 9.4P3 are susceptible to a vulnerability that could allow HTTP clients to cache sensitive res
CVE-2021-25248	An out-of-bounds read information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0
CVE-2020-28394	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation
CVE-2021-26550	An issue was discovered in SmartFoxServer 2.17.0. Cleartext password disclosure can occur via /config/server.xml.
CVE-2020-14391	A flaw was found in the GNOME Control Center in Red Hat Enterprise Linux 8 versions prior to 8.2, where it improperly uses Red Hat Customer Portal credentials wher
CVE-2021-22307	There is a weak algorithm vulnerability in Mate 3010.0.0.203(C00E201R7P2). The protection is insufficient for the modules that should be protected. Local attackers ca
CVE-2021-26917	PyBitmessage through 0.6.3.2 allows attackers to write screen captures to Potentially Unwanted Directories via a crafted apinotifypath value. NOTE: the discoverer stat
CVE-2021-20176	A divide-by-zero flaw was found in ImageMagick 6.9.11-57 and 7.0.10-57 in gem.c. This flaw allows an attacker who submits a crafted file that is processed by ImageM
CVE-2020-26196	Dell EMC PowerScale OneFS versions 8.1.0-9.1.0 contain a Backup/Restore Privilege implementation issue. A user with the BackupAdmin role may potentially exploit
CVE-2020-8294	A missing link validation in Nextcloud Server before 20.0.2, 19.0.5, 18.0.11 allows execution of a stored XSS attack using Internet Explorer when saving a 'javascript:' U

CVE Number	
CVE-2020-18723	Stored cross-site scripting (XSS) in file attachment field in MDaemon webmail 19.5.5 allows an attacker to execute code on the email recipient side while forwarding an
CVE-2020-4825	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary J
CVE-2021-3294	CASAP Automated Enrollment System 1.0 is affected by cross-site scripting (XSS) in users.php. An attacker can steal a cookie to perform user redirection to a maliciou
CVE-2020-28001	SolarWinds Serv-U before 15.2.2 allows Authenticated Stored XSS.
CVE-2020-18724	Authenticated stored cross-site scripting (XSS) in the contact name field in the distribution list of MDaemon webmail 19.5.5 allows an attacker to executes code and per
CVE-2021-26549	An XSS issue was discovered in SmartFoxServer 2.17.0. Input passed to the AdminTool console is not properly sanitized before being returned to the user. This can be
CVE-2020-35482	SolarWinds Serv-U before 15.2.2 allows authenticated reflected XSS.
CVE-2021-3258	Question2Answer Q2A Ultimate SEO Version 1.3 is affected by cross-site scripting (XSS), which may lead to arbitrary remote code execution.
CVE-2021-26925	Roundcube before 1.4.11 allows XSS via crafted Cascading Style Sheets (CSS) token sequences during HTML email rendering.
CVE-2020-9390	SquaredUp allowed Stored XSS before version 4.6.0. A user was able to create a dashboard that executed malicious content in iframe or by uploading an SVG that con
CVE-2020-26052	Online Marriage Registration System 1.0 is affected by stored cross-site scripting (XSS) vulnerabilities in multiple parameters.
CVE-2021-1243	A vulnerability in the Local Packet Transport Services (LPTS) programming of the SNMP with the management plane protection feature of Cisco IOS XR Software coul protection. An attacker could exploit this vulnerability by connecting to an affected device using SNMP. A successful exploit could allow the attacker to connect to the de
CVE-2021-25778	In JetBrains TeamCity before 2020.2.1, permissions during user deletion were checked improperly.
CVE-2021-25760	In JetBrains Hub before 2020.1.12669, information disclosure via the public API was possible.
CVE-2021-25777	In JetBrains TeamCity before 2020.2.1, permissions during token removal were checked improperly.
CVE-2021-25756	In JetBrains IntelliJ IDEA before 2020.2, HTTP links were used for several remote repositories instead of HTTPS.
CVE-2021-25761	In JetBrains Ktor before 1.5.0, a birthday attack on SessionStorage key was possible.
CVE-2020-26195	Dell EMC PowerScale OneFS versions 8.1.2 – 9.1.0 contain an issue where the OneFS SMB directory auto-create may erroneously create a directory for a user. A rem
CVE-2021-25762	In JetBrains Ktor before 1.4.3, HTTP Request Smuggling was possible.

CVE Number	
CVE-2021-25763	In JetBrains Ktor before 1.4.2, weak cipher suites were enabled by default.
CVE-2021-25766	In JetBrains YouTrack before 2020.4.4701, improper resource access checks were made.
CVE-2020-16194	An Insecure Direct Object Reference (IDOR) vulnerability was found in Prestashop Opart devis < 4.0.2. Unauthenticated attackers can have access to any user's invoic
CVE-2021-25767	In JetBrains YouTrack before 2020.6.1767, an issue's existence could be disclosed via YouTrack command execution.
CVE-2021-25768	In JetBrains YouTrack before 2020.4.4701, permissions for attachments actions were checked improperly.
CVE-2021-26024	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to Insecure Direct Object Reference: it is possible to create favorites for any other user account
CVE-2021-25228	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-21306	Marked is an open-source markdown parser and compiler (npm package "marked"). In marked from version 1.1.1 and before version 2.0.0, there is a Regular expressi
CVE-2021-25237	An improper access control vulnerability in Trend Micro Apex One (on-prem) could allow an unauthenticated user to obtain information about the managing port used b
CVE-2021-25229	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain informati
CVE-2021-25241	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an unauthe
CVE-2020-25208	In JetBrains YouTrack before 2020.4.4701, an attacker could enumerate users via the REST API without appropriate permissions.
CVE-2021-26540	Apostrophe Technologies sanitize-html before 2.3.2 does not properly validate the hostnames set by the "allowedIframeHostnames" option when the "allowIframeRelat
CVE-2021-26539	Apostrophe Technologies sanitize-html before 2.3.1 does not properly handle internationalized domain name (IDN) which could allow an attacker to bypass hostname v
CVE-2021-3293	emlog v5.3.1 has full path disclosure vulnerability in t/index.php, which allows an attacker to see the path to the webroot/file.
CVE-2020-29582	In JetBrains Kotlin before 1.4.21, a vulnerable Java API was used for temporary file and folder creation. An attacker was able to read data from such files and list direct
CVE-2020-10858	Zulip Desktop before 5.0.0 allows attackers to perform recording via the webcam and microphone due to a missing permission request handler.
CVE-2021-26711	A frame-injection issue in the online help in Redwood Report2Web 4.3.4.5 allows remote attackers to render an external resource inside a frame via the help/Online_H
CVE-2020-8807	In Electric Coin Company Zcashd before 2.1.1-1, the time offset between messages could be leveraged to obtain sensitive information about the relationship between a

CVE Number	
CVE-2021-25245	An improper access control vulnerability in Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain various pieces of settings informaiton
CVE-2021-25244	An improper access control vulnerability in Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain various pieces of configuration inform
CVE-2021-25230	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain informati
CVE-2021-25242	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-25243	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-25240	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-25234	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-25231	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-25232	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain informati
CVE-2021-25233	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2020-4995	IBM Security Identity Governance and Intelligence 5.2.6 does not invalidate session after logout which could allow a user to obtain sensitive information from another us
CVE-2021-25239	An improper access control vulnerability in Trend Micro Apex One (on-prem), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthe
CVE-2021-26954	An issue was discovered in the qwutils crate before 0.3.1 for Rust. When a Clone panic occurs, insert_slice_clone can perform a double drop.
CVE-2020-4791	IBM Security Identity Governance and Intelligence 5.2.6 could allow an attacker to obtain sensitive information using main in the middle attacks due to improper certifica
CVE-2021-25235	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain informati
CVE-2021-25236	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow a
CVE-2021-25772	In JetBrains TeamCity before 2020.2.2, TeamCity server DoS was possible via server integration.
CVE-2021-25238	An improper access control information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthe
CVE-2020-9205	There has a CSV injection vulnerability in ManageOne 8.0.1. An attacker with common privilege may exploit this vulnerability through some operations to inject the CS\

CVE Number	
CVE-2020-22841	Stored XSS in b2evolution CMS version 6.11.6 and prior allows an attacker to perform malicious JavaScript code execution via the plugin name input field in the plugin
CVE-2021-22499	Persistent Cross-Site scripting vulnerability in Micro Focus Application Performance Management product, affecting versions 9.40, 9.50 and 9.51. The vulnerability coul
CVE-2019-16268	Zoho ManageEngine Remote Access Plus 10.0.259 allows HTML injection via the Description field on the Admin - User Administration userMgmt.do?actionToCall=Sho
CVE-2021-22306	There is an out-of-bound read vulnerability in Mate 30 10.0.0.182(C00E180R6P2). A module does not verify the some input when dealing with messages. Attackers ca
CVE-2020-35152	Cloudflare WARP for Windows allows privilege escalation due to an unquoted service path. A malicious user or process running with non-administrative privileges can l
CVE-2021-0347	In ccu, 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. U
CVE-2021-0350	In ged, there is a possible system crash due to an improper input validation. This could lead to local denial of service with System execution privileges needed. User int
CVE-2021-23331	This affects all versions of package com.squareup:connect. The method prepareDownloadFilecreates creates a temporary file with the permissions bits of -rw-r--r-- on u property java.io.tmpdir to a safe directory as remediation. Note: This version of the SDK is end of life and no longer maintained, please upgrade to the latest version.
CVE-2021-25141	A security vulnerability has been identified in in certain HPE and Aruba L2/L3 switch firmware. A data processing error due to improper handling of an unexpected data must have administrator privileges to exploit this vulnerability.
CVE-2021-0352	In RT regmap driver, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. U
CVE-2020-28644	The CSRF (Cross Site Request Forgery) token check was improperly implemented on cookie authenticated requests against some ocs API endpoints. This affects own
CVE-2021-21288	CarrierWave is an open-source RubyGem which provides a simple and flexible way to upload files from Ruby applications. In CarrierWave before versions 1.3.2 and 2.
CVE-2021-25666	A vulnerability has been identified in SCALANCE W780 and W740 (IEEE 802.11n) family (All versions < V6.3). Sending specially crafted packets through the ARP prot
CVE-2020-1779	When dynamic templates are used (OTRSTicketForms), admin can use OTRS tags which are not masked properly and can reveal sensitive information. This issue affe
CVE-2020-13461	Username enumeration in present in Tufin SecureTrack. It's affecting all versions of SecureTrack. The vendor has decided not to fix this vulnerability. Vendor's respons
CVE-2021-25774	In JetBrains TeamCity before 2020.2.1, a user could get access to the GitHub access token of another user.
CVE-2021-25771	In JetBrains YouTrack before 2020.6.1099, project information could be potentially disclosed.
CVE-2021-1354	A vulnerability in the certificate registration process of Cisco Unified Computing System (UCS) Central Software could allow an authenticated, adjacent attacker to regis rogue Cisco UCSM and gain access to Cisco UCS Central Software data and Cisco UCSM inventory data.
CVE-2021-1266	A vulnerability in the REST API of Cisco Managed Services Accelerator (MSX) could allow an authenticated, remote attacker to cause a denial of service (DoS) conditi condition on the affected device.

CVE Number	
CVE-2020-5032	IBM QRadar SIEM 7.3 and 7.4 in some configurations may be vulnerable to a temporary denial of service attack when sent particular payloads. IBM X-Force ID: 19417
CVE-2020-4827	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 is vulnerable to cross-site request forgery which could allow an attacker to execute ma
CVE-2020-4826	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 is vulnerable to cross-site request forgery which could allow an attacker to execute ma
CVE-2021-21147	Inappropriate implementation in Skia in Google Chrome prior to 88.0.4324.146 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a crafted HT
CVE-2021-22300	There is an information leak vulnerability in eCNS280_TD versions V100R005C00 and V100R005C10. A command does not have timeout exit mechanism. Temporary
CVE-2020-4640	Certain IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 configurations can result in sensitive information in the URL fragment identifier
CVE-2021-1221	A vulnerability in the user interface of Cisco Webex Meetings and Cisco Webex Meetings Server Software could allow an authenticated, remote attacker to inject a hyp contains a link to a destination of their choosing. Because this email is sent from a trusted source, the recipient may be more likely to click the link.
CVE-2021-25775	In JetBrains TeamCity before 2020.2.1, the server admin could create and see access tokens for any other users.
CVE-2020-9389	A username enumeration issue was discovered in SquaredUp before version 4.6.0. The login functionality was implemented in a way that would enable a malicious use
CVE-2020-29021	A vulnerability in web UI input field of GateManager allows authenticated attacker to enter script tags that could cause XSS. This issue affects: GateManager all versior
CVE-2020-8588	Clustered Data ONTAP versions prior to 9.3P20 and 9.5P15 are susceptible to a vulnerability which could allow unauthorized tenant users to discover the existence of
CVE-2020-8589	Clustered Data ONTAP versions prior to 9.3P20 and 9.5P15 are susceptible to a vulnerability which could allow unauthorized tenant users to discover the names of oth
CVE-2021-21436	Agents are able to see and link Config Items without permissions, which are defined in General Catalog. This issue affects: OTRS AG OTRSCIsInCustomerFrontend 7.
CVE-2021-21434	Survey administrator can craft a survey in such way that malicious code can be executed in the agent interface (i.e. another agent who wants to make changes in the s
CVE-2020-17428	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11336.
CVE-2021-25227	Trend Micro Antivirus for Mac 2021 (Consumer) is vulnerable to a memory exhaustion vulnerability that could lead to disabling all the scanning functionality within the a
CVE-2021-22303	There is a pointer double free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). There is a lack of muti-thread protection when a function is called. Attackers can ex
CVE-2020-17422	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11195.
CVE-2021-22304	There is a use after free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module may refer to some memory after it has been freed while dealing with some mes

CVE Number	
CVE-2021-22305	There is a buffer overflow vulnerability in Mate 30 10.1.0.126(C00E125R5P3). A module does not verify the some input when dealing with messages. Attackers can exp
CVE-2020-8578	Clustered Data ONTAP versions prior to 9.3P20 are susceptible to a vulnerability which could allow an attacker to discover node names via AutoSupport bundles even
CVE-2020-8590	Clustered Data ONTAP versions prior to 9.1P18 and 9.3P12 are susceptible to a vulnerability which could allow an attacker to discover node names via AutoSupport bu
CVE-2020-17420	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploi attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11193.
CVE-2021-25755	In JetBrains Code With Me before 2020.3, an attacker on the local network, knowing a session ID, could get access to the encrypted traffic.
CVE-2020-18715	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none
CVE-2021-26959	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-21299. Reason: This candidate is a duplicate of CVE-2021-21299. Notes: All CV