SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 12 May 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-2016-20010 | EWWW Image Optimizer before 2.8.5 allows remote command execution because it relies on a protection mechanism involving boolval, which is unavailable before PHP 5.5. | 10.0 | More Details |
| CVE-2021-28476 | Windows Hyper-V Remote Code Execution Vulnerability | 9.9 | More Details |
| CVE-2021-28152 | Hongdian H8922 3.0.5 devices have an undocumented feature that allows access to a shell as a superuser. To connect, the telnet service is used on port 5188 with the default credentials of root:superzxmn. | 9.8 | More Details |
| CVE-2021-31755 | An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setmac allows attackers to execute arbitrary code on the system via a crafted post request. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31800 | Multiple path traversal vulnerabilities exist in smbserver.py in Impacket through 0.9.22. An attacker that connects to a running smbserver instance can list and write to arbitrary files via ../ directory traversal. This could potentially be abused to achieve arbitrary code execution by replacing /etc/shadow or an SSH authorized key. | 9.8 | More Details |
| CVE-2020-18890 | Rmote Code Execution (RCE) vulnerability in puppyCMS v5.1 due to insecure permissions, which could let a remote malicious user getshell via /admin/functions.php. | 9.8 | More Details |
| CVE-2021-29203 | A security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software, prior to version 1.22. The vulnerability could be remotely exploited to bypass remote authentication leading to execution of arbitrary commands, gaining privileged access, causing denial of service, and changing the configuration. HPE has released a software update to resolve the vulnerability in the HPE Edgeline Infrastructure Manager. | 9.8 | More Details |
| CVE-2021-31737 | emlog v5.3.1 and emlog v6.0.0 have a Remote Code Execution vulnerability due to upload of database backup file in admin/data.php. | 9.8 | More Details |
| CVE-2021-32098 | Artica Pandora FMS 742 allows unauthenticated attackers to perform Phar deserialization. | 9.8 | More Details |
| CVE-2021-32099 | A SQL injection vulnerability in the pandora_console component of Artica Pandora FMS 742 allows an unauthenticated attacker to upgrade his unprivileged session via the /include/chart_generator.php session_id parameter, leading to a login bypass. | 9.8 | More Details |
| CVE-2021-32090 | The dashboard component of StackLift LocalStack 0.12.6 allows attackers to inject arbitrary shell commands via the functionName parameter. | 9.8 | More Details |
| CVE-2021-21984 | VMware vRealize Business for Cloud 7.x prior to 7.6.0 contains a remote code execution vulnerability due to an unauthorised end point. A malicious actor with network access may exploit this issue causing unauthorised remote code execution on vRealize Business for Cloud Virtual Appliance. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22679 | The affected product is vulnerable to an integer overflow while processing HTTP headers, which may allow an attacker to remotely execute code on the SimpleLink Wi-Fi (MSP432E4 SDK: v4.20.00.12 and prior, CC32XX SDK v4.30.00.06 and prior, CC13X0 SDK versions prior to v4.10.03, CC13X2 and CC26XX SDK versions prior to v4.40.00, CC3200 SDK v1.5.0 and prior, CC3100 SDK v1.3.0 and prior). | 9.8 | More Details |
| CVE-2021-22671 | Multiple integer overflow issues exist while processing long domain names, which may allow an attacker to remotely execute code on the SimpleLink Wi-Fi (MSP432E4 SDK: v4.20.00.12 and prior, CC32XX SDK v4.30.00.06 and prior, CC13X0 SDK versions prior to v4.10.03, CC13X2 and CC26XX SDK versions prior to v4.40.00, CC3200 SDK v1.5.0 and prior, CC3100 SDK v1.3.0 and prior). | 9.8 | More Details |
| CVE-2021-27573 | An issue was discovered in Emote Remote Mouse through 4.0.0.0. Remote unauthenticated users can execute arbitrary code via crafted UDP packets with no prior authorization or authentication. | 9.8 | More Details |
| CVE-2021-31757 | An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setVLAN allows attackers to execute arbitrary code on the system via a crafted post request. | 9.8 | More Details |
| CVE-2021-31756 | An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /gofrom/setwanType allows attackers to execute arbitrary code on the system via a crafted post request. This occurs when input vector controlled by malicious attack get copied to the stack variable. | 9.8 | More Details |
| CVE-2021-30473 | aom_image.c in libaom in AOMedia before 2021-04-07 frees memory that is not located on the heap. | 9.8 | More Details |
| CVE-2021-31758 | An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setportList allows attackers to execute arbitrary code on the system via a crafted post request. | 9.8 | More Details |
| CVE-2021-26583 | A potential security vulnerability was identified in HPE iLO Amplifier Pack. The vulnerabilities could be remotely exploited to allow remote code execution. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-23008 | On version 15.1.x before 15.1.3, 14.1.x before 14.1.4, 13.1.x before 13.1.4, 12.1.x before 12.1.6, and all versions of 16.0.x and 11.6.x., BIG-IP APM AD (Active Directory) authentication can be bypassed via a spoofed AS-REP (Kerberos Authentication Service Response) response sent over a hijacked KDC (Kerberos Key Distribution Center) connection or from an AD server compromised by an attacker. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 9.8 | More Details |
| CVE-2021-32563 | An issue was discovered in Thunar before 4.16.7 and 4.17.x before 4.17.2. When called with a regular file as a command-line argument, it delegates to a different program (based on the file type) without user confirmation. This could be used to achieve code execution. | 9.8 | More Details |
| CVE-2021-31909 | In JetBrains TeamCity before 2020.2.3, argument injection leading to remote code execution was possible. | 9.8 | More Details |
| CVE-2021-31897 | In JetBrains WebStorm before 2021.1, code execution without user confirmation was possible for untrusted projects. | 9.8 | More Details |
| CVE-2021-31914 | In JetBrains TeamCity before 2020.2.4 on Windows, arbitrary code execution on TeamCity Server was possible. | 9.8 | More Details |
| CVE-2021-31915 | In JetBrains TeamCity before 2020.2.4, OS command injection leading to remote code execution was possible. | 9.8 | More Details |
| CVE-2021-31166 | HTTP Protocol Stack Remote Code Execution Vulnerability | 9.8 | More Details |
| CVE-2021-32089 | An issue was discovered on Zebra (formerly Motorola Solutions) Fixed RFID Reader FX9500 devices. An unauthenticated attacker can upload arbitrary files to the filesystem that can then be accessed through the web interface. This can lead to information disclosure and code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer | 9.8 | More Details |
| CVE-2021-32030 | The administrator application on ASUS GT-AC2900 devices before 3.0.0.4.386.42643 allows authentication bypass when processing remote input from an unauthenticated user, leading to unauthorized access to the administrator interface. This relates to handle_request in router/httpd/httpd.c and auth_check in web_hook.o. An attacker-supplied value of '\0' matches the device's default value of '\0' in some situations. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32605 | zzzcms zzzphp before 2.0.4 allows remote attackers to execute arbitrary OS commands by placing them in the keys parameter of a ? location=search URI, as demonstrated by an OS command within an "if" "end if" block. | 9.8 | More Details |
| CVE-2021-20204 | A heap memory corruption problem (use after free) can be triggered in libgetdata v0.10.0 when processing maliciously crafted dirfile databases. This degrades the confidentiality, integrity and availability of third-party software that uses libgetdata as a library. This vulnerability may lead to arbitrary code execution or privilege escalation depending on input/skills of attacker. | 9.8 | More Details |
| CVE-2020-28020 | Exim 4 before 4.92 allows Integer Overflow to Buffer Overflow, in which an unauthenticated remote attacker can execute arbitrary code by leveraging the mishandling of continuation lines during header-length restriction. | 9.8 | More Details |
| CVE-2020-13665 | Access bypass vulnerability in Drupal Core allows JSON:API when JSON:API is in read/write mode. Only sites that have the read_only set to FALSE under jsonapi.settings config are vulnerable. This issue affects: Drupal Drupal Core 8.8.x versions prior to 8.8.8; 8.9.x versions prior to 8.9.1; 9.0.x versions prior to 9.0.1. | 9.8 | More Details |
| CVE-2020-4979 | IBM QRadar SIEM 7.3 and 7.4 is vulnerable to insecure inter-deployment communication. An attacker that is able to comprimise or spoof traffic between hosts may be able to execute arbitrary commands. IBM X-Force D: 192538. | 9.8 | More Details |
| CVE-2020-19107 | SQL Injection vulnerability in Online Book Store v1.0 via the isbn parameter to edit_book.php, which could let a remote malicious user execute arbitrary code. | 9.8 | More Details |
| CVE-2020-19108 | SQL Injection vulnerability in Online Book Store v1.0 via the pubid parameter to bookPerPub.php, which could let a remote malicious user execute arbitrary code. | 9.8 | More Details |
| CVE-2020-19109 | SQL Injection vulnerability in Online Book Store v1.0 via the bookisbn parameter to admin_edit.php, which could let a remote malicious user execute arbitrary code. | 9.8 | More Details |
| CVE-2020-19110 | SQL Injection vulnerability in Online Book Store v1.0 via the bookisbn parameter to book.php parameter, which could let a remote malicious user execute arbitrary code. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-19111 | Incorrect Access Control vulnerability in Online Book Store v1.0 via admin_verify.php, which could let a remote mailicious user bypass authentication and obtain sensitive information. | 9.8 | More Details |
| CVE-2020-19112 | SQL Injection vulnerability in Online Book Store v1.0 via the bookisbn parameter to admin_delete.php, which could let a remote malicious user execute arbitrary code. | 9.8 | More Details |
| CVE-2020-19113 | Arbitrary File Upload vulnerability in Online Book Store v1.0 in admin_add.php, which may lead to remote code execution. | 9.8 | More Details |
| CVE-2021-29921 | In Python before 3,9,5, the ipaddress library mishandles leading zero characters in the octets of an IP address string. This (in some situations) allows attackers to bypass access control that is based on IP addresses. | 9.8 | More Details |
| CVE-2020-28017 | Exim 4 before 4.94.2 allows Integer Overflow to Buffer Overflow in receive_add_recipient via an e-mail message with fifty million recipients. NOTE: remote exploitation may be difficult because of resource consumption. | 9.8 | More Details |
| CVE-2020-28018 | Exim 4 before 4.94.2 allows Use After Free in smtp_reset in certain situations that may be common for builds with OpenSSL. | 9.8 | More Details |
| CVE-2020-19114 | SQL Injection vulnerability in Online Book Store v1.0 via the publisher parameter to edit_book.php, which could let a remote malicious user execute arbitrary code. | 9.8 | More Details |
| CVE-2020-28022 | Exim 4 before 4.94.2 has Improper Restriction of Write Operations within the Bounds of a Memory Buffer. This occurs when processing name=value pairs within MAIL FROM and RCPT TO commands. | 9.8 | More Details |
| CVE-2021-1497 | Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2021-24236 | The Imagements WordPress plugin through 1.2.5 allows images to be uploaded in comments, however only checks for the Content-Type in the request to forbid dangerous files. This allows unauthenticated attackers to upload arbitrary files by using a valid image Content-Type along with a PHP filename and code, leading to RCE. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1508 | Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2021-1506 | Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2021-1505 | Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2021-1498 | Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2021-1468 | Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2021-1275 | Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. | 9.8 | More Details |
| CVE-2020-28026 | Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters, relevant in non-default configurations that enable Delivery Status Notification (DSN). Certain uses of ORCPT= can place a newline into a spool header file, and indirectly allow unauthenticated remote attackers to execute arbitrary commands as root. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-28024 | Exim 4 before 4.94.2 allows Buffer Underwrite that may result in unauthenticated remote attackers executing arbitrary commands, because smtp_ungetc was only intended to push back characters, but can actually push back non-character error codes such as EOF. | 9.8 | More Details |
| CVE-2021-21428 | Openapi generator is a java tool which allows generation of API client libraries (SDK generation), server stubs, documentation and configuration automatically given an OpenAPI Spec. openapi-generator-online creates insecure temporary folders with File.createTempFile during the code generation process. The insecure temporary folders store the auto-generated files which can be read and appended to by any users on the system. The issue has been patched with `Files.createTempFile` and released in the v5.1.0 stable version. | 9.3 | More Details |
| CVE-2021-27437 | The affected product allows attackers to obtain sensitive information from the WISE-PaaS dashboard. The system contains a hard-coded administrator username and password that can be used to query Grafana APIs. Authentication is not required for exploitation on the WISE-PaaS/RMM (versions prior to 9.0.1). | 9.1 | More Details |
| CVE-2021-20538 | IBM Cloud Pak for Security (CP4S) 1.5.0.0 and 1.5.0.1 could allow a user to obtain sensitive information or perform actions they should not have access to due to incorrect authorization mechanisms. IBM X-Force ID: 198919. | 9.1 | More Details |
| CVE-2021-25848 | Improper validation of the length field of LLDP-MED TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows information disclosure to attackers due to using fixed loop counter variable without checking the actual available length via a crafted lldp packet. | 9.1 | More Details |
| CVE-2021-29508 | Due to how Wire handles type information in its serialization format, malicious payloads can be passed to a deserializer. e.g. using a surrogate on the sender end, an attacker can pass information about a different type for the receiving end. And by doing so allowing the serializer to create any type on the deserializing end. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300?view=vs-2019. This also applies to the fork of Wire. | 9.1 | More Details |
| CVE-2021-32055 | Mutt 1.11.0 through 2.0.x before 2.0.7 (and NeoMutt 2019-10-25 through 2021-05-04) has a $imap_qresync issue in which imap/util.c has an out-of-bounds read in situations where an IMAP sequence set ends with a comma. NOTE: the $imap_qresync setting for QRESYNC is not enabled by default. | 9.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-25847 | Improper validation of the length field of LLDP-MED TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows information disclosure to attackers due to controllable loop counter variable via a crafted lldp packet. | 9.1 | More Details |
| CVE-2020-36333 | themegrill-demo-importer before 1.6.2 does not require authentication for wiping the database, because of a reset_wizard_actions hook. | 9.1 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-23014 | On versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.3, and 14.1.x before 14.1.4, BIG-IP Advanced WAF and ASM are missing authorization checks for file uploads to a specific directory within the REST API which might allow Authenticated users with guest privileges to upload files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 8.8 | More Details |
| CVE-2021-32104 | A SQL injection vulnerability exists (with user privileges) in interface/forms/eye_mag/save.php in OpenEMR 5.0.2.1. | 8.8 | More Details |
| CVE-2020-27232 | An exploitable SQL injection vulnerability exists in ‘manageServiceStocks.jsp’ page of OpenClinic GA 5.173.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-32096 | The ConsoleAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows a CSRF attack that results in injecting arbitrary Ruby code (for an eval call) via the CONSOLE_COMMAND_STRING parameter. | 8.8 | More Details |
| CVE-2021-32094 | U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to upload arbitrary files. | 8.8 | More Details |
| CVE-2020-23264 | Cross-site request forgery (CSRF) in Fork-CMS before 5.8.2 allow remote attackers to hijack the authentication of logged administrators. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-28151 | Hongdian H8922 3.0.5 devices allow OS command injection via shell metacharacters into the ip-address (aka Destination) field to the tools.cgi ping command, which is accessible with the username guest and password guest. | 8.8 | More Details |
| CVE-2021-31912 | In JetBrains TeamCity before 2020.2.3, account takeover was potentially possible during a password reset. | 8.8 | More Details |
| CVE-2021-31616 | Insufficient length checks in the ShapeShift KeepKey hardware wallet firmware before 7.1.0 allow a stack buffer overflow via crafted messages. The overflow in ethereum_extractThorchainSwapData() in ethereum.c can circumvent stack protections and lead to code execution. The vulnerable interface is reachable remotely over WebUSB. | 8.8 | More Details |
| CVE-2021-26543 | The "gitDiff" function in Wayfair git-parse <=1.0.4 has a command injection vulnerability. Clients of the git-parse library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. The issue has been resolved in version 1.0.5. | 8.8 | More Details |
| CVE-2021-24253 | The Classyfrieds WordPress plugin through 3.8 does not properly check the uploaded file when an authenticated user adds a listing, only checking the content-type in the request. This allows any authenticated user to upload arbitrary PHP files via the Add Listing feature of the plugin, leading to RCE. | 8.8 | More Details |
| CVE-2021-24179 | The Business Directory Plugin – Easy Listing Directories for WordPress WordPress plugin before 5.11 suffered from a Cross-Site Request Forgery issue, allowing an attacker to make a logged in administrator import files. As the plugin also did not validate uploaded files, it could lead to RCE. | 8.8 | More Details |
| CVE-2021-24178 | The Business Directory Plugin – Easy Listing Directories for WordPress WordPress plugin before 5.11.1 suffered from Cross-Site Request Forgery issues, allowing an attacker to make a logged in administrator add, edit or delete form fields, which could also lead to Stored Cross-Site Scripting issues. | 8.8 | More Details |
| CVE-2021-31181 | Microsoft SharePoint Remote Code Execution Vulnerability | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-27242 | An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoLocation parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2020-27243 | An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoService parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2020-27244 | An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoCode parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2020-27245 | An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoBuyer parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-1401 | Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to obtain sensitive information from or inject arbitrary commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 8.8 | More Details |
| CVE-2021-31194 | OLE Automation Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2021-1400 | Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to obtain sensitive information from or inject arbitrary commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1284 | A vulnerability in the web-based messaging service interface of Cisco SD-WAN vManage Software could allow an unauthenticated, adjacent attacker to bypass authentication and authorization and modify the configuration of an affected system. To exploit this vulnerability, the attacker must be able to access an associated Cisco SD-WAN vEdge device. This vulnerability is due to insufficient authorization checks. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based messaging service interface of an affected system. A successful exploit could allow the attacker to gain unauthenticated read and write access to the affected vManage system. With this access, the attacker could access information about the affected vManage system, modify the configuration of the system, or make configuration changes to devices that are managed by the system. | 8.8 | More Details |
| CVE-2020-28021 | Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters. An authenticated remote SMTP client can insert newline characters into a spool file (which indirectly leads to remote code execution as root) via AUTH= in a MAIL FROM command. | 8.8 | More Details |
| CVE-2021-32102 | A SQL injection vulnerability exists (with user privileges) in library/custom_template/ajax_code.php in OpenEMR 5.0.2.1. | 8.8 | More Details |
| CVE-2020-27231 | A number of exploitable SQL injection vulnerabilities exists in ‘patientslist.do’ page of OpenClinic GA 5.173.3 application. The findDistrict parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2020-23127 | Chamilo LMS 1.11.10 is affected by Cross Site Request Forgery (CSRF) via the edit_user function by targeting an admin user. | 8.8 | More Details |
| CVE-2020-13664 | Arbitrary PHP code execution vulnerability in Drupal Core under certain circumstances. An attacker could trick an administrator into visiting a malicious site that could result in creating a carefully named directory on the file system. With this directory in place, an attacker could attempt to brute force a remote code execution vulnerability. Windows servers are most likely to be affected. This issue affects: Drupal Drupal Core 8.8.x versions prior to 8.8.8; 8.9.x versions prior to 8.9.1; 9.0.1 versions prior to 9.0.1. | 8.8 | More Details |
| CVE-2020-36334 | themegrill-demo-importer before 1.6.3 allows CSRF, as demonstrated by wiping the database. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-28663 | The Arm Mali GPU kernel driver allows privilege escalation or information disclosure because GPU memory operations are mishandled, leading to a use-after-free. This affects Bifrost r0p0 through r28p0 before r29p0, Valhall r19p0 through r28p0 before r29p0, and Midgard r4p0 through r30p0. | 8.8 | More Details |
| CVE-2021-28664 | The Arm Mali GPU kernel driver allows privilege escalation or a denial of service (memory corruption) because an unprivileged user can achieve read/write access to read-only pages. This affects Bifrost r0p0 through r29p0 before r30p0, Valhall r19p0 through r29p0 before r30p0, and Midgard r8p0 through r30p0 before r31p0. | 8.8 | More Details |
| CVE-2021-26077 | Broken Authentication in Atlassian Connect Spring Boot (ACSB) in version 1.1.0 before 2.1.3 and from version 2.1.4 before 2.1.5: Atlassian Connect Spring Boot is a Java Spring Boot package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Spring Boot app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Spring Boot versions 1.1.0 before 2.1.3 and versions 2.1.4 before 2.1.5 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app. | 8.8 | More Details |
| CVE-2021-21822 | A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.3.37598. A specially crafted PDF document can trigger the reuse of previously free memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening a malicious file or site to trigger this vulnerability if the browser plugin extension is enabled. | 8.8 | More Details |
| CVE-2020-18964 | Cross Site Request Forgery (CSRF) Vulnerability in ForestBlog latest version via the website Management background, which could let a remote malicious gain privileges. | 8.8 | More Details |
| CVE-2021-27068 | Visual Studio Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2020-19199 | A Cross Site Request Forgery (CSRF) vulnerability exists in PHPOK 5.2.060 via admin.php?c=admin&f=save, which could let a remote malicious user execute arbitrary code. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-27226 | An exploitable SQL injection vulnerability exists in ‘quickFile.jsp’ page of OpenClinic GA 5.173.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2020-27246 | An exploitable SQL injection vulnerability exists in ‘listImmoLabels.jsp’ page of OpenClinic GA 5.173.3 application. The immoComment parameter in the ‘listImmoLabels.jsp’ page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-28455 | Microsoft Jet Red Database Engine and Access Connectivity Engine Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2020-27229 | A number of exploitable SQL injection vulnerabilities exists in ‘patientslist.do’ page of OpenClinic GA 5.173.3 application. The findPersonID parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2020-27230 | A number of exploitable SQL injection vulnerabilities exists in ‘patientslist.do’ page of OpenClinic GA 5.173.3 application. The findSector parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection An attacker can make an authenticated HTTP request to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-28474 | Microsoft SharePoint Server Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2021-31899 | In JetBrains Code With Me bundled to the compatible IDEs before version 2021.1, the client could execute code in read-only mode. | 8.8 | More Details |
| CVE-2020-11284 | Locked memory can be unlocked and modified by non secure boot loader through improper system call sequence making the memory region untrusted source of input for secure boot loader in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking | 8.4 | More Details |
| CVE-2021-1927 | Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 8.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1905 | Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 8.4 | More Details |
| CVE-2021-1891 | A possible use-after-free occurrence in audio driver can happen when pointers are not properly handled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 8.4 | More Details |
| CVE-2020-11285 | Buffer over-read while unpacking the RTCP packet we may read extra byte if wrong length is provided in RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 8.2 | More Details |
| CVE-2021-23012 | On BIG-IP versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.3, 14.1.x before 14.1.4, and 13.1.x before 13.1.4, lack of input validation for items used in the system support functionality may allow users granted either "Resource Administrator" or "Administrator" roles to execute arbitrary bash commands on BIG-IP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 8.2 | More Details |
| CVE-2020-36128 | Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by a token spoofing vulnerability. Each payment terminal has a session token (called X-Terminal-Token) to access the marketplace. This allows the store to identify the terminal and make available the applications distributed by its reseller. By intercepting HTTPS traffic from the application store, it is possible to collect the request responsible for assigning the X-Terminal-Token to the terminal, which makes it possible to craft an X-Terminal-Token pretending to be another device. An attacker can use this behavior to authenticate its own payment terminal in the application store through token impersonation. | 8.2 | More Details |
| CVE-2021-32101 | The Patient Portal of OpenEMR 5.0.2.1 is affected by a incorrect access control system in portal/patient/_machine_config.php. To exploit the vulnerability, an unauthenticated attacker can register an account, bypassing the permission check of this portal's API. Then, the attacker can then manipulate and read data of every registered patient. | 8.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-28128 | In Strapi through 3.6.0, the admin panel allows the changing of one's own password without entering the current password. An attacker who gains access to a valid session can use this to take over an account by changing the password. | 8.1 | More Details |
| CVE-2021-27574 | An issue was discovered in Emote Remote Mouse through 4.0.0.0. It uses cleartext HTTP to check, and request, updates. Thus, attackers can machine-in-the-middle a victim to download a malicious binary in place of the real update, with no SSL errors or warnings. | 8.1 | More Details |
| CVE-2021-31520 | A weak session token authentication bypass vulnerability in Trend Micro IM Security 1.6 and 1.6.5 could allow an remote attacker to guess currently logged-in administrators' session session token in order to gain access to the product's web management interface. | 8.1 | More Details |
| CVE-2021-32095 | U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to delete arbitrary files. | 8.1 | More Details |
| CVE-2020-36126 | Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by incorrect access control that can lead to remote privilege escalation. PAXSTORE marketplace endpoints allow an authenticated user to read and write data not owned by them, including third-party users, application and payment terminals, where an attacker can impersonate any user which may lead to the unauthorized disclosure, modification, or destruction of information. | 8.1 | More Details |
| CVE-2021-29501 | Ticketer is a command based ticket system cog (plugin) for the red discord bot. A vulnerability allowing discord users to expose sensitive information has been found in the Ticketer cog. Please upgrade to version 1.0.1 as soon as possible. As a workaround users may unload the ticketer cog to disable the exploitable code. | 8.1 | More Details |
| CVE-2021-27572 | An issue was discovered in Emote Remote Mouse through 4.0.0.0. Authentication Bypass can occur via Packet Replay. Remote unauthenticated users can execute arbitrary code via crafted UDP packets even when passwords are set. | 8.1 | More Details |
| CVE-2020-5013 | IBM QRadar SIEM 7.3 and 7.4 may vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 193245. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21505 | Dell EMC Integrated System for Microsoft Azure Stack Hub, versions 1906 – 2011, contain an undocumented default iDRAC account. A remote unauthenticated attacker, with the knowledge of the default credentials, could potentially exploit this to log in to the system to gain root privileges. | 8.0 | More Details |
| CVE-2021-22673 | The affected product is vulnerable to stack-based buffer overflow while processing over-the-air firmware updates from the CDN server, which may allow an attacker to remotely execute code on the SimpleLink Wi-Fi (MSP432E4 SDK: v4.20.00.12 and prior, CC32XX SDK v4.30.00.06 and prior, CC13X0 SDK versions prior to v4.10.03, CC13X2 and CC26XX SDK versions prior to v4.40.00, CC3200 SDK v1.5.0 and prior, CC3100 SDK v1.3.0 and prior). | 8.0 | More Details |
| CVE-2021-31453 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13092. | 7.8 | More Details |
| CVE-2021-31170 | Windows Graphics Component Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-31468 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D files embedded in PDF documents. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13620. | 7.8 | More Details |
| CVE-2020-28600 | An out-of-bounds write vulnerability exists in the import_stl.cc:import_stl() functionality of Openscad openscad-2020.12-RC2. A specially crafted STL file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. | 7.8 | More Details |
| CVE-2021-31167 | Windows Container Manager Service Elevation of Privilege Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31470 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12947. | 7.8 | More Details |
| CVE-2021-31472 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13011. | 7.8 | More Details |
| CVE-2021-31168 | Windows Container Manager Service Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-31449 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13280. | 7.8 | More Details |
| CVE-2020-35519 | An out-of-bounds (OOB) memory access flaw was found in x25_bind in net/x25/af_x25.c in the Linux kernel version v5.12-rc5. A bounds check failure allows a local attacker with a user account on the system to gain access to out-of-bounds memory, leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. | 7.8 | More Details |
| CVE-2021-31169 | Windows Container Manager Service Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-31214 | Visual Studio Code Remote Code Execution Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31466 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13583. | 7.8 | More Details |
| CVE-2021-32606 | In the Linux kernel 5.11 through 5.12.2, isotp_setsockopt in net/can/isotp.c allows privilege escalation to root by leveraging a use-after-free. (This does not affect earlier versions that lack CAN ISOTP SF_BROADCAST support.) | 7.8 | More Details |
| CVE-2021-31213 | Visual Studio Code Remote Containers Extension Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-31211 | Visual Studio Code Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-31175 | Microsoft Office Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-31176 | Microsoft Office Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-27616 | Under certain conditions, SAP Business One Hana Chef Cookbook, versions - 8.82, 9.0, 9.1, 9.2, 9.3, 10.0, used to install SAP Business One for SAP HANA, allows an attacker to exploit an insecure temporary backup path and to access information which would otherwise be restricted, resulting in Information Disclosure vulnerability highly impacting the confidentiality, integrity and availability of the application. | 7.8 | More Details |
| CVE-2021-31177 | Microsoft Office Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2020-22809 | In Windscribe v1.83 Build 20, 'WindscribeService' has an Unquoted Service Path that facilitates privilege escalation. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31450 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13084. | 7.8 | More Details |
| CVE-2021-31165 | Windows Container Manager Service Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-31441 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13101. | 7.8 | More Details |
| CVE-2021-31459 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13162. | 7.8 | More Details |
| CVE-2021-31442 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13239. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31452 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13091. | 7.8 | More Details |
| CVE-2021-22677 | An integer overflow exists in the APIs of the host MCU while trying to connect to a WIFI network may lead to issues such as a denial-of-service condition or code execution on the SimpleLink Wi-Fi (MSP432E4 SDK: v4.20.00.12 and prior, CC32XX SDK v4.30.00.06 and prior, CC13X0 SDK versions prior to v4.10.03, CC13X2 and CC26XX SDK versions prior to v4.40.00, CC3200 SDK v1.5.0 and prior, CC3100 SDK v1.3.0 and prior). | 7.8 | More Details |
| CVE-2021-31454 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Decimal element. A crafted leadDigits value in a Decimal element can trigger an overflow of a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current process. Was ZDI-CAN-13095. | 7.8 | More Details |
| CVE-2021-31455 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13100. | 7.8 | More Details |
| CVE-2021-31456 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13102. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31457 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13147. | 7.8 | More Details |
| CVE-2021-31451 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13089. | 7.8 | More Details |
| CVE-2021-31458 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13150. | 7.8 | More Details |
| CVE-2021-28465 | Web Media Extensions Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-31465 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13582. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1915 | Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking | 7.8 | More Details |
| CVE-2021-31460 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13096. | 7.8 | More Details |
| CVE-2021-31461 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the the handling of app.media objects. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-13333. | 7.8 | More Details |
| CVE-2020-4932 | IBM QRadar SIEM 7.3 and 7.4 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 191748. | 7.8 | More Details |
| CVE-2020-11289 | Out of bound write can occur in TZ command handler due to lack of validation of command ID in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 7.8 | More Details |
| CVE-2020-11288 | Out of bound write can occur in playready while processing command due to lack of input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music | 7.8 | More Details |
| CVE-2021-22672 | Delta Electronics' CNCSoft ScreenEditor in versions prior to v1.01.30 could allow the corruption of data, a denial-of-service condition, or code execution. The vulnerability may allow an attacker to remotely execute arbitrary code. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-20401 | IBM QRadar SIEM 7.3 and 7.4 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196075. | 7.8 | More Details |
| CVE-2021-29100 | A path traversal vulnerability exists in Esri ArcGIS Earth versions 1.11.0 and below which allows arbitrary file creation on an affected system through crafted input. An attacker could exploit this vulnerability to gain arbitrary code execution under security context of the user running ArcGIS Earth by inducing the user to upload a crafted file to an affected system. | 7.8 | More Details |
| CVE-2021-31179 | Microsoft Office Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-32471 | Insufficient input validation in the Marvin Minsky 1967 implementation of the Universal Turing Machine allows program users to execute arbitrary code via crafted data. For example, a tape head may have an unexpected location after the processing of input composed of As and Bs (instead of 0s and 1s). NOTE: the discoverer states "this vulnerability has no real-world implications." | 7.8 | More Details |
| CVE-2021-27613 | Under certain conditions, SAP Business One Chef cookbook, version - 9.2, 9.3, 10.0, used to install SAP Business One, allows an attacker to exploit an insecure temporary folder for incoming & outgoing payroll data and to access information which would otherwise be restricted, which could lead to Information Disclosure and highly impact system confidentiality, integrity and availability. | 7.8 | More Details |
| CVE-2020-28016 | Exim 4 before 4.94.2 allows an off-by-two Out-of-bounds Write because "-F "" is mishandled by parse_fix_phrase. | 7.8 | More Details |
| CVE-2020-28010 | Exim 4 before 4.94.2 allows Out-of-bounds Write because the main function, while setuid root, copies the current working directory pathname into a buffer that is too small (on some common platforms). | 7.8 | More Details |
| CVE-2020-28011 | Exim 4 before 4.94.2 allows Heap-based Buffer Overflow in queue_run via two sender options: -R and -S. This may cause privilege escalation from exim to root. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1514 | A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands to be executed with Administrator privileges on the underlying operating system. This vulnerability is due to insufficient input validation on certain CLI commands. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI. The attacker must be authenticated as a low-privileged user to execute the affected commands. A successful exploit could allow the attacker to execute commands with Administrator privileges. | 7.8 | More Details |
| CVE-2020-28012 | Exim 4 before 4.94.2 allows Exposure of File Descriptor to Unintended Control Sphere because rda_interpret uses a privileged pipe that lacks a close-on-exec flag. | 7.8 | More Details |
| CVE-2020-28013 | Exim 4 before 4.94.2 allows Heap-based Buffer Overflow because it mishandles "-F '.('" on the command line, and thus may allow privilege escalation from any user to root. This occurs because of the interpretation of negative sizes in strncpy. | 7.8 | More Details |
| CVE-2021-31187 | Windows WalletService Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2020-28015 | Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters. Local users can alter the behavior of root processes because a recipient address can have a newline character. | 7.8 | More Details |
| CVE-2021-31188 | Windows Graphics Component Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2020-28008 | Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. Because Exim operates as root in the spool directory (owned by a non-root user), an attacker can write to a /var/spool/exim4/input spool header file, in which a crafted recipient address can indirectly lead to command execution. | 7.8 | More Details |
| CVE-2021-31190 | Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-31208 | Windows Container Manager Service Elevation of Privilege Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-29263 | In JetBrains IntelliJ IDEA 2020.3.3, local code execution was possible because of insufficient checks when getting the project from VCS. | 7.8 | More Details |
| CVE-2021-31198 | Microsoft Exchange Server Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-1421 | A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to perform a command injection attack on an affected device. The vulnerability is due to insufficient validation of user-supplied input to a configuration command. An attacker could exploit this vulnerability by including malicious input during the execution of this command. A successful exploit could allow a non-privileged attacker authenticated in the restricted CLI to execute arbitrary commands on the underlying operating system (OS) with root privileges. | 7.8 | More Details |
| CVE-2021-25319 | A Incorrect Default Permissions vulnerability in the packaging of virtualbox of openSUSE Factory allows local attackers in the vboxusers groupu to escalate to root. This issue affects: openSUSE Factory virtualbox version 6.1.20-1.1 and prior versions. | 7.8 | More Details |
| CVE-2021-31192 | Windows Media Foundation Core Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2020-28009 | Exim 4 before 4.94.2 allows Integer Overflow to Buffer Overflow because get_stdinput allows unbounded reads that are accompanied by unbounded increases in a certain size variable. NOTE: exploitation may be impractical because of the execution time needed to overflow (multiple days). | 7.8 | More Details |
| CVE-2021-30005 | In JetBrains PyCharm before 2020.3.4, local code execution was possible because of insufficient checks when getting the project from VCS. | 7.8 | More Details |
| CVE-2021-31193 | Windows SSDP Service Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-31180 | Microsoft Office Graphics Remote Code Execution Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-28007 | Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. Because Exim operates as root in the log directory (owned by a non-root user), a symlink or hard link attack allows overwriting critical root-owned files anywhere on the filesystem. | 7.8 | More Details |
| CVE-2021-29489 | Highcharts JS is a JavaScript charting library based on SVG. In Highcharts versions 8 and earlier, the chart options structure was not systematically filtered for XSS vectors. The potential impact was that content from untrusted sources could execute code in the end user's browser. The vulnerability is patched in version 9. As a workaround, implementers who are not able to upgrade may apply DOMPurify recursively to the options structure to filter out malicious markup. | 7.6 | More Details |
| CVE-2021-28478 | Microsoft SharePoint Server Spoofing Vulnerability | 7.6 | More Details |
| CVE-2021-20311 | A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGBTransformImage() in the MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability. | 7.5 | More Details |
| CVE-2021-23011 | On versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.3, 14.1.x before 14.1.4, 13.1.x before 13.1.4, 12.1.x before 12.1.6, and 11.6.x before 11.6.5.3, when the BIG-IP system is buffering packet fragments for reassembly, the Traffic Management Microkernel (TMM) may consume an excessive amount of resources, eventually leading to a restart and failover event. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 7.5 | More Details |
| CVE-2021-32074 | HashiCorp vault-action (aka Vault GitHub Action) before 2.2.0 allows attackers to obtain sensitive information from log files because a multi-line secret was not correctly registered with GitHub Actions for log masking. | 7.5 | More Details |
| CVE-2021-30482 | In JetBrains UpSource before 2020.1.1883, application passwords were not revoked correctly | 7.5 | More Details |
| CVE-2020-28019 | Exim 4 before 4.94.2 has Improper Initialization that can lead to recursion-based stack consumption or other consequences. This occurs because use of certain getc functions is mishandled when a client uses BDAT instead of DATA. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-20313 | A flaw was found in ImageMagick in versions before 7.0.11. A potential cipher leak when the calculate signatures in TransformSignature is possible. The highest threat from this vulnerability is to data confidentiality. | 7.5 | More Details |
| CVE-2020-11268 | Potential UE reset while decoding a crafted Sib1 or SIB1 that schedules unsupported SIBs and can lead to denial of service in Snapdragon Auto, Snapdragon Mobile | 7.5 | More Details |
| CVE-2020-11273 | Histogram type KPI was teardown with the assumption of the existence of histogram binning info and will lead to null pointer access when histogram binning info is missing due to lack of null check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile | 7.5 | More Details |
| CVE-2020-11274 | Denial of service in MODEM due to assert to the invalid configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 7.5 | More Details |
| CVE-2020-11279 | Memory corruption while processing crafted SDES packets due to improper length check in sdes packets recieved in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 7.5 | More Details |
| CVE-2020-23575 | A directory traversal vulnerability exists in Kyocera Printer d-COPIA253MF plus. Successful exploitation of this vulnerability could allow an attacker to retrieve or view arbitrary files from the affected server. | 7.5 | More Details |
| CVE-2021-31409 | Unsafe validation RegEx in EmailValidator component in com.vaadin:vaadin-compatibility-server versions 8.0.0 through 8.12.4 (Vaadin versions 8.0.0 through 8.12.4) allows attackers to cause uncontrolled resource consumption by submitting malicious email addresses. | 7.5 | More Details |
| CVE-2021-29101 | ArcGIS GeoEvent Server versions 10.8.1 and below has a read-only directory path traversal vulnerability that could allow an unauthenticated, remote attacker to perform directory traversal attacks and read arbitrary files on the system. | 7.5 | More Details |
| CVE-2021-20309 | A flaw was found in ImageMagick in versions before 7.0.11 and before 6.9.12, where a division by zero in WaveImage() of MagickCore/visual-effects.c may trigger undefined behavior via a crafted image file submitted to an application using ImageMagick. The highest threat from this vulnerability is to system availability. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31901 | In JetBrains Hub before 2021.1.13079, two-factor authentication wasn't enabled properly for the All Users group. | 7.5 | More Details |
| CVE-2021-20310 | A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero ConvertXYZToJzazbz() of MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker and processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability. | 7.5 | More Details |
| CVE-2020-28025 | Exim 4 before 4.94.2 allows Out-of-bounds Read because pdkim_finish_bodyhash does not validate the relationship between sig->bodyhash.len and b->bh.len; thus, a crafted DKIM-Signature header might lead to a leak of sensitive information from process memory. | 7.5 | More Details |
| CVE-2021-31910 | In JetBrains TeamCity before 2020.2.3, information disclosure via SSRF was possible. | 7.5 | More Details |
| CVE-2021-31898 | In JetBrains WebStorm before 2021.1, HTTP requests were used instead of HTTPS. | 7.5 | More Details |
| CVE-2021-1925 | Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking | 7.5 | More Details |
| CVE-2021-31542 | In Django 2.2 before 2.2.21, 3.1 before 3.1.9, and 3.2 before 3.2.1, MultiPartParser, UploadedFile, and FieldFile allowed directory traversal via uploaded files with suitably crafted file names. | 7.5 | More Details |
| CVE-2021-30006 | In IntelliJ IDEA before 2020.3.3, XXE was possible, leading to information disclosure. | 7.5 | More Details |
| CVE-2021-31518 | Trend Micro Home Network Security 6.5.599 and earlier is vulnerable to a file-parsing vulnerability which could allow an attacker to exploit the vulnerability and cause a denial-of-service to the device. This vulnerability is similar, but not identical to CVE-2021-31517. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31517 | Trend Micro Home Network Security 6.5.599 and earlier is vulnerable to a file-parsing vulnerability which could allow an attacker to exploit the vulnerability and cause a denial-of-service to the device. This vulnerability is similar, but not identical to CVE-2021-31518. | 7.5 | More Details |
| CVE-2021-31905 | In JetBrains YouTrack before 2020.6.8801, information disclosure in an issue preview was possible. | 7.5 | More Details |
| CVE-2020-28023 | Exim 4 before 4.94.2 allows Out-of-bounds Read. smtp_setup_msg may disclose sensitive information from process memory to an unauthenticated SMTP client. | 7.5 | More Details |
| CVE-2021-30504 | In JetBrains IntelliJ IDEA before 2021.1, DoS was possible because of unbounded resource allocation. | 7.5 | More Details |
| CVE-2021-1511 | Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 7.5 | More Details |
| CVE-2021-31918 | A flaw was found in tripleo-ansible version as shipped in Red Hat Openstack 16.1. The Ansible log file is readable to all users during stack update and creation. The highest threat from this vulnerability is to data confidentiality. | 7.5 | More Details |
| CVE-2021-25845 | Improper validation of the ChassisID TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows attackers to cause a denial of service due to a NULL pointer dereference via a crafted lldp packet. | 7.5 | More Details |
| CVE-2021-29499 | SIF is an open source implementation of the Singularity Container Image Format. The `siftool new` command and func siftool.New() produce predictable UUID identifiers due to insecure randomness in the version of the `github.com/satori/go.uuid` module used as a dependency. A patch is available in version >= v1.2.3 of the module. Users are encouraged to upgrade. As a workaround, users passing CreateInfo struct should ensure the `ID` field is generated using a version of `github.com/satori/go.uuid` that is not vulnerable to this issue. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-23009 | On BIG-IP version 16.0.x before 16.0.1.1 and 15.1.x before 15.1.3, malformed HTTP/2 requests may cause an infinite loop which causes a Denial of Service for Data Plane traffic. TMM takes the configured HA action when the TMM process is aborted. There is no control plane exposure, this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 7.5 | More Details |
| CVE-2021-22209 | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.8. GitLab was not properly validating authorisation tokens which resulted in GraphQL mutation being executed. | 7.5 | More Details |
| CVE-2021-25846 | Improper validation of the ChassisID TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows attackers to cause a denial of service due to a negative number passed to the memcpy function via a crafted lldp packet. | 7.5 | More Details |
| CVE-2021-31902 | In JetBrains YouTrack before 2020.6.6600, access control during the exporting of issues was implemented improperly. | 7.5 | More Details |
| CVE-2021-1513 | A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. | 7.5 | More Details |
| CVE-2021-25849 | An integer underflow was discovered in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, improper validation of the PortID TLV leads to Denial of Service via a crafted lldp packet. | 7.5 | More Details |
| CVE-2021-31913 | In JetBrains TeamCity before 2020.2.3, insufficient checks of the redirect_uri were made during GitHub SSO token exchange. | 7.5 | More Details |
| CVE-2021-23013 | On BIG-IP versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.3, 14.1.x before 14.1.4, 13.1.x before 13.1.3.6, and 12.1.x before 12.1.5.3, the Traffic Management Microkernel (TMM) may stop responding when processing Stream Control Transmission Protocol (SCTP) traffic under certain conditions. This vulnerability affects TMM by way of a virtual server configured with an SCTP profile. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31793 | An issue exists on NightOwl WDB-20-V2 WDB-20-V2_20190314 devices that allows an unauthenticated user to gain access to snapshots and video streams from the doorbell. The binary app offers a web server on port 80 that allows an unauthenticated user to take a snapshot from the doorbell camera via the /snapshot URI. | 7.5 | More Details |
| CVE-2021-26310 | In the TeamCity IntelliJ plugin before 2020.2.2.85899, DoS was possible. | 7.5 | More Details |
| CVE-2021-1510 | Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 7.5 | More Details |
| CVE-2020-18888 | Arbitrary File Deletion vulnerability in puppyCMS v5.1 allows remote malicious attackers to delete the file/folder via /admin/functions.php. | 7.5 | More Details |
| CVE-2021-29509 | Puma is a concurrent HTTP 1.1 server for Ruby/Rack applications. The fix for CVE-2019-16770 was incomplete. The original fix only protected existing connections that had already been accepted from having their requests starved by greedy persistent-connections saturating all threads in the same process. However, new connections may still be starved by greedy persistent-connections saturating all threads in all processes in the cluster. A `puma` server which received more concurrent `keep-alive` connections than the server had threads in its threadpool would service only a subset of connections, denying service to the unserved connections. This problem has been fixed in `puma` 4.3.8 and 5.3.1. Setting `queue_requests false` also fixes the issue. This is not advised when using `puma` without a reverse proxy, such as `nginx` or `apache`, because you will open yourself to slow client attacks (e.g. slowloris). The fix is very small and a git patch is available for those using unsupported versions of Puma. | 7.5 | More Details |
| CVE-2021-32077 | Primary Source Verification in VerityStream MSOW Solutions before 3.1.1 allows an anonymous internet user to discover Social Security Number (SSN) values via a brute-force attack on a (sometimes hidden) search field, because the last four SSN digits are part of the supported combination of search selectors. This discloses doctors' and nurses' social security numbers and PII. | 7.5 | More Details |
| CVE-2021-26419 | Scripting Engine Memory Corruption Vulnerability | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-23010 | On versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.5, and 12.1.x before 12.1.5.3, when the BIG-IP ASM/Advanced WAF system processes WebSocket requests with JSON payloads using the default JSON Content Profile in the ASM Security Policy, the BIG-IP ASM bd process may produce a core file. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 7.5 | More Details |
| CVE-2021-20312 | A flaw was found in ImageMagick in versions 7.0.11, where an integer overflow in WriteTHUMBNAILImage of coders/thumbnail.c may trigger undefined behavior via a crafted image file that is submitted by an attacker and processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability. | 7.5 | More Details |
| CVE-2021-28665 | Stormshield SNS with versions before 3.7.18, 3.11.6 and 4.1.6 has a memory-management defect in the SNMP plugin that can lead to excessive consumption of memory and CPU resources, and possibly a denial of service. | 7.5 | More Details |
| CVE-2021-1509 | Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. | 7.5 | More Details |
| CVE-2021-31186 | Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability | 7.4 | More Details |
| CVE-2021-31936 | Microsoft Accessibility Insights for Web Information Disclosure Vulnerability | 7.4 | More Details |
| CVE-2021-29502 | WarnSystem is a cog (plugin) for the Red discord bot. A vulnerability has been found in the code that allows any user to access sensible informations by setting up a specific template which is not properly sanitized. The problem has been patched in version 1.3.18. Users should update and type `!warnsysteminfo` to check that their version is 1.3.18 or above. As a workaround users may unload the WarnSystem cog or disable the `!warnset description` command globally. | 7.3 | More Details |
| CVE-2021-1910 | Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 7.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31204 | .NET and Visual Studio Elevation of Privilege Vulnerability | 7.3 | More Details |
| CVE-2021-24248 | The Business Directory Plugin – Easy Listing Directories for WordPress WordPress plugin before 5.11.1 did not properly check for imported files, forbidding certain extension via a blacklist approach, allowing administrator to import an archive with a .php4 inside for example, leading to RCE | 7.2 | More Details |
| CVE-2021-31200 | Common Utilities Remote Code Execution Vulnerability | 7.2 | More Details |
| CVE-2021-23015 | On BIG-IP 15.1.x before 15.1.3, 14.1.x before 14.1.4.2, 13.1.0.8 through 13.1.3.6, and all versions of 16.0.x, when running in Appliance Mode, an authenticated user assigned the 'Administrator' role may be able to bypass Appliance Mode restrictions utilizing undisclosed iControl REST endpoints. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 7.2 | More Details |
| CVE-2021-22675 | The affected product is vulnerable to integer overflow while parsing malformed over-the-air firmware update files, which may allow an attacker to remotely execute code on SimpleLink Wi-Fi (MSP432E4 SDK: v4.20.00.12 and prior, CC32XX SDK v4.30.00.06 and prior, CC13X0 SDK versions prior to v4.10.03, CC13X2 and CC26XX SDK versions prior to v4.40.00, CC3200 SDK v1.5.0 and prior, CC3100 SDK v1.3.0 and prior). | 7.2 | More Details |
| CVE-2021-24254 | The College publisher Import WordPress plugin through 0.1 does not check for the uploaded CSV file to import, allowing high privilege users to upload arbitrary files, such as PHP, leading to RCE. Due to the lack of CSRF check, the issue could also be exploited via a CSRF attack. | 7.2 | More Details |
| CVE-2021-26422 | Skype for Business and Lync Remote Code Execution Vulnerability | 7.2 | More Details |
| CVE-2021-24252 | The Event Banner WordPress plugin through 1.3 does not verify the uploaded image file, allowing admin accounts to upload arbitrary files, such as .exe, .php, or others executable, leading to RCE. Due to the lack of CSRF check, the issue can also be used via such vector to achieve the same result, or via a LFI as authorisation checks are missing (but would require WP to be loaded) | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1363 | Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. These vulnerabilities are due to improper validation of user-submitted parameters. An attacker could exploit these vulnerabilities by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database. | 7.1 | More Details |
| CVE-2021-27614 | SAP Business One Hana Chef Cookbook, versions - 8.82, 9.0, 9.1, 9.2, 9.3, 10.0, used to install SAP Business One on SAP HANA, allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behaviour of the application thereby highly impacting the integrity and availability of the application. | 7.1 | More Details |
| CVE-2021-21656 | Jenkins Xcode integration Plugin 2.0.14 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. | 7.1 | More Details |
| CVE-2020-36125 | Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by incorrect access control where password revalidation in sensitive operations can be bypassed remotely by an authenticated attacker through requesting the endpoint directly. | 7.1 | More Details |
| CVE-2021-21655 | A cross-site request forgery (CSRF) vulnerability in Jenkins P4 Plugin 1.11.4 and earlier allows attackers to connect to an attacker-specified Perforce server using attacker-specified username and password. | 7.1 | More Details |
| CVE-2021-31182 | Microsoft Bluetooth Driver Spoofing Vulnerability | 7.1 | More Details |
| CVE-2021-31172 | Microsoft SharePoint Server Spoofing Vulnerability | 7.1 | More Details |
| CVE-2021-3501 | A flaw was found in the Linux kernel in versions before 5.12. The value of internal.ndata, in the KVM API, is mapped to an array index, which can be updated by a user process at anytime which could lead to an out-of-bounds write. The highest threat from this vulnerability is to data integrity and system availability. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31828 | An SSRF issue in Open Distro for Elasticsearch (ODFE) before 1.13.1.0 allows an existing privileged user to enumerate listening services or interact with configured resources via HTTP requests exceeding the Alerting plugin's intended scope. | 7.1 | More Details |
| CVE-2021-1365 | Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. These vulnerabilities are due to improper validation of user-submitted parameters. An attacker could exploit these vulnerabilities by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database. | 7.1 | More Details |
| CVE-2021-21652 | A cross-site request forgery (CSRF) vulnerability in Jenkins Xray - Test Management for Jira Plugin 2.4.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. | 7.1 | More Details |
| CVE-2021-1429 | Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. | 7.0 | More Details |
| CVE-2021-1426 | Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. | 7.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1428 | Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. | 7.0 | More Details |
| CVE-2021-1496 | Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. | 7.0 | More Details |
| CVE-2021-1427 | Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. | 7.0 | More Details |
| CVE-2020-28198 | The 'id' parameter of IBM Tivoli Storage Manager Version 5 Release 2 (Command Line Administrative Interface, dsmadmc.exe) is vulnerable to an exploitable stack buffer overflow. Note: the vulnerability can be exploited when it is used in "interactive" mode while, cause of a max number characters limitation, it cannot be exploited in batch or command line usage (e.g. dsmadmc.exe -id=username -password=pwd). NOTE: This vulnerability only affects products that are no longer supported by the maintainer | 7.0 | More Details |
| CVE-2021-1430 | Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. | 7.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32399 | net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller. | 7.0 | More Details |
| CVE-2021-20254 | A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity. | 6.8 | More Details |
| CVE-2020-11295 | Use after free in camera If the threadmanager is being cleaned up while the worker thread is processing objects in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 6.8 | More Details |
| CVE-2021-31532 | NXP LPC55S6x microcontrollers (0A and 1B), i.MX RT500 (silicon rev B1 and B2), i.MX RT600 (silicon rev A0, B0), LPC55S6x, LPC55S2x, LPC552x (silicon rev 0A, 1B), LPC55S1x, LPC551x (silicon rev 0A) and LPC55S0x, LPC550x (silicon rev 0A) include an undocumented ROM patch peripheral that allows unsigned, non-persistent modification of the internal ROM. | 6.8 | More Details |
| CVE-2021-22206 | An issue has been discovered in GitLab affecting all versions starting from 11.6. Pull mirror credentials are exposed that allows other maintainers to be able to view the credentials in plain-text, | 6.8 | More Details |
| CVE-2021-1895 | Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music | 6.8 | More Details |
| CVE-2021-1520 | A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-29246 | BTCPay Server through 1.0.7.0 suffers from directory traversal, which allows an attacker with admin privileges to achieve code execution. The attacker must craft a malicious plugin file with special characters to upload the file outside of the restricted directory. | 6.7 | More Details |
| CVE-2021-31916 | An out-of-bounds (OOB) memory write flaw was found in list_devices in drivers/md/dm-ioctl.c in the Multi-device driver module in the Linux kernel before 5.12. A bound check failure allows an attacker with special user (CAP_SYS_ADMIN) privilege to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability. | 6.7 | More Details |
| CVE-2021-27611 | SAP NetWeaver AS ABAP, versions - 700, 701, 702, 730, 731, allow a high privileged attacker to inject malicious code by executing an ABAP report when the attacker has access to the local SAP system. The attacker could then get access to data, overwrite them, or execute a denial of service. | 6.7 | More Details |
| CVE-2021-1447 | A vulnerability in the user account management system of Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an authenticated, local attacker to elevate their privileges to root. This vulnerability is due to a procedural flaw in the password generation algorithm. An attacker could exploit this vulnerability by enabling specific Administrator-only features and connecting to the appliance through the CLI with elevated privileges. A successful exploit could allow the attacker to execute arbitrary commands as root and access the underlying operating system. To exploit this vulnerability, the attacker must have valid Administrator credentials. | 6.7 | More Details |
| CVE-2021-31207 | Microsoft Exchange Server Security Feature Bypass Vulnerability | 6.6 | More Details |
| CVE-2020-20267 | Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/resolver process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access. | 6.5 | More Details |
| CVE-2020-20265 | Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /ram/pckg/wireless/nova/bin/wireless process. An authenticated remote attacker can cause a Denial of Service due via a crafted packet. | 6.5 | More Details |
| CVE-2021-32100 | A remote file inclusion vulnerability exists in Artica Pandora FMS 742, exploitable by the lowest privileged user. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-27619 | SAP Commerce (Backoffice Search), versions - 1808, 1811, 1905, 2005, 2011, allows a low privileged user to search for attributes which are not supposed to be displayed to them. Although the search results are masked, the user can iteratively enter one character at a time to search and determine the masked attribute value thereby leading to information disclosure. | 6.5 | More Details |
| CVE-2021-1532 | A vulnerability in the video endpoint API (xAPI) of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an authenticated, remote attacker to read arbitrary files from the underlying operating system. This vulnerability is due to insufficient path validation of command arguments. An attacker could exploit this vulnerability by sending a crafted command request to the xAPI. A successful exploit could allow the attacker to read the contents of any file that is located on the device filesystem. | 6.5 | More Details |
| CVE-2021-28149 | Hongdian H8922 3.0.5 devices allow Directory Traversal. The /log_download.cgi log export handler does not validate user input and allows a remote attacker with minimal privileges to download any file from the device by substituting ../ (e.g., ../../etc/passwd) This can be carried out with a web browser by changing the file name accordingly. Upon visiting log_download.cgi?type=../../etc/passwd and logging in, the web server will allow a download of the contents of the /etc/passwd file. | 6.5 | More Details |
| CVE-2020-26140 | An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration. | 6.5 | More Details |
| CVE-2020-18889 | Cross Site Request Forgery (CSRF) vulnerability in puppyCMS v5.1 that can change the admin's password via /admin/settings.php. | 6.5 | More Details |
| CVE-2021-24244 | An AJAX action registered by the WPBakery Page Builder (Visual Composer) Clipboard WordPress plugin before 4.5.8 did not have capability checks, allowing low privilege users, such as subscribers, to update the license options (key, email). | 6.5 | More Details |
| CVE-2021-29493 | Kennnyshiwa-cogs contains cogs for Red Discordbot. An RCE exploit has been found in the Tickets module of kennnyshiwa-cogs. This exploit allows discord users to craft a message that can reveal sensitive and harmful information. Users can upgrade to version 5a84d60018468e5c0346f7ee74b2b4650a6dade7 to receive a patch or, as a workaround, unload tickets to render the exploit unusable. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-26141 | An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The Wi-Fi implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol. | 6.5 | More Details |
| CVE-2020-26143 | An issue was discovered in the ALFA Windows 10 driver 1030.36.604 for AWUS036ACH. The WEP, WPA, WPA2, and WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration. | 6.5 | More Details |
| CVE-2020-26144 | An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration. | 6.5 | More Details |
| CVE-2020-26145 | An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration. | 6.5 | More Details |
| CVE-2021-31209 | Microsoft Exchange Server Spoofing Vulnerability | 6.5 | More Details |
| CVE-2021-32093 | The ConfigFileAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to read arbitrary files via the ConfigName parameter. | 6.5 | More Details |
| CVE-2021-1521 | A vulnerability in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause an affected IP camera to reload. This vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected IP camera. A successful exploit could allow the attacker to cause the affected IP camera to reload unexpectedly, resulting in a denial of service (DoS) condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-4883 | IBM QRadar SIEM 7.3 and 7.4 could disclose sensitive information about other domains which could be used in further attacks against the system. IBM X-Force ID: 190907. | 6.5 | More Details |
| CVE-2021-31205 | Windows SMB Client Security Feature Bypass Vulnerability | 6.5 | More Details |
| CVE-2021-30173 | Local File Inclusion vulnerability of the omni-directional communication system allows remote authenticated attacker inject absolute path into Url parameter and access arbitrary file. | 6.5 | More Details |
| CVE-2020-36124 | Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by XML External Entity (XXE) injection. An authenticated attacker can compromise the private keys of a JWT token and reuse them to manipulate the access tokens to access the platform as any desired user (clients and administrators). | 6.5 | More Details |
| CVE-2020-36127 | Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by an information disclosure vulnerability. Through the PUK signature functionality, an administrator will not have access to the current p12 certificate and password. When accessing this functionality, the administrator has the option to replace the current certificate and it is not possible to view the certificate password (p12) already deployed on the platform. The replacement p12 certificate returns to users in base64 with its password, which can be accessed by non-administrator users. | 6.5 | More Details |
| CVE-2021-26421 | Skype for Business and Lync Spoofing Vulnerability | 6.5 | More Details |
| CVE-2020-4901 | IBM Robotic Process Automation with Automation Anywhere 11.0 could allow an attacker on the network to obtain sensitive information or cause a denial of service through username enumeration. IBM X-Force ID: 190992. | 6.5 | More Details |
| CVE-2021-31195 | Microsoft Exchange Server Remote Code Execution Vulnerability | 6.5 | More Details |
| CVE-2021-32560 | The Logging subsystem in OctoPrint before 1.6.0 has incorrect access control because it attempts to manage files that are not *.log files. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-24249 | The Business Directory Plugin – Easy Listing Directories for WordPress WordPress plugin before 5.11.2 suffered from a Cross-Site Request Forgery issue, allowing an attacker to make a logged in administrator export files, which could then be downloaded by the attacker to get access to PII, such as email, home addresses etc | 6.5 | More Details |
| CVE-2021-1507 | A vulnerability in an API of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the application web-based interface. This vulnerability exists because the API does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending malicious input to the API. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based interface or access sensitive, browser-based information. | 6.4 | More Details |
| CVE-2021-27216 | Exim 4 before 4.94.2 has Execution with Unnecessary Privileges. By leveraging a delete_pid_file race condition, a local user can delete arbitrary files as root. This involves the -oP and -oPX options. | 6.3 | More Details |
| CVE-2021-24011 | A privilege escalation vulnerability in FortiNAC version below 8.8.2 may allow an admin user to escalate the privileges to root by abusing the sudo privileges. | 6.3 | More Details |
| CVE-2021-31411 | Insecure temporary directory usage in frontend build functionality of com.vaadin:flow-server versions 2.0.9 through 2.5.2 (Vaadin 14.0.3 through Vaadin 14.5.2), 3.0 prior to 6.0 (Vaadin 15 prior to 19), and 6.0.0 through 6.0.5 (Vaadin 19.0.0 through 19.0.4) allows local users to inject malicious code into frontend resources during application rebuilds. | 6.3 | More Details |
| CVE-2020-14009 | Proofpoint Enterprise Protection (PPS/PoD) before 8.16.4 contains a vulnerability that could allow an attacker to deliver an email message with a malicious attachment that bypasses scanning and file-blocking rules. The vulnerability exists because messages with certain crafted and malformed multipart structures are not properly handled. | 6.3 | More Details |
| CVE-2021-21430 | OpenAPI Generator allows generation of API client libraries (SDK generation), server stubs, documentation and configuration automatically given an OpenAPI Spec. Using `File.createTempFile` in JDK will result in creating and using insecure temporary files that can leave application and system data vulnerable to attacks. Auto-generated code (Java, Scala) that deals with uploading or downloading binary data through API endpoints will create insecure temporary files during the process. Affected generators: `java` (jersey2, okhttp-gson (default library)), `scala-finch`. The issue has been patched with `Files.createTempFile` and released in the v5.1.0 stable version. | 6.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-11254 | Memory corruption during buffer allocation due to dereferencing session ctx pointer without checking if pointer is valid in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile | 6.2 | More Details |
| CVE-2021-1906 | Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 6.2 | More Details |
| CVE-2020-23371 | Cross-site scripting (XSS) vulnerability in static/admin/js/kindeditor/plugins/multiimage/images/swfupload.swf in noneCms v1.3.0 allows remote attackers to inject arbitrary web script or HTML via the movieName parameter. | 6.1 | More Details |
| CVE-2021-31911 | In JetBrains TeamCity before 2020.2.3, reflected XSS was possible on several pages. | 6.1 | More Details |
| CVE-2020-23369 | In YzmCMS 5.6, XSS was discovered in member/member_content/init.html via the SRC attribute of an IFRAME element because of using UEditor 1.4.3.3. | 6.1 | More Details |
| CVE-2021-32561 | OctoPrint before 1.6.0 allows XSS because API error messages include the values of input parameters. | 6.1 | More Details |
| CVE-2020-23376 | NoneCMS v1.3 has a CSRF vulnerability in public/index.php/admin/nav/add.html, as demonstrated by adding a navigation column which can be injected with arbitrary web script or HTML via the name parameter to launch a stored XSS attack. | 6.1 | More Details |
| CVE-2020-18102 | Cross Site Scripting (XSS) in Hotels_Server v1.0 allows remote attackers to execute arbitrary code by injecting crafted commands the data fields in the component "/controller/publishHotel.php". | 6.1 | More Details |
| CVE-2021-21990 | VMware Workspace one UEM console (2102 prior to 21.2.0.8, 2101 prior to 21.1.0.14, 2011 prior to 20.11.0.27, 2010 prior to 20.10.0.16,2008 prior to 20.8.0.28, 2007 prior to 20.7.0.14,2006 prior to 20.6.0.19, 2005 prior to 20.5.0.46, 2004 prior to 20.4.0.21, 2003 prior to 20.3.0.23, 2001 prior to 20.1.0.32, 1912 prior to 19.12.0.24) contain a cross-site scripting vulnerability. VMware Workspace ONE UEM console does not validate incoming requests during device enrollment after leading to rendering of unsanitized input on the user device in response. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-35438 | Cross Site Scripting (XSS) vulnerability in the kk Star Ratings plugin before 4.1.5. | 6.1 | More Details |
| CVE-2021-20577 | IBM Cloud Pak for Security (CP4S) 1.5.0.0 and 1.5.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199281. | 6.1 | More Details |
| CVE-2020-13529 | An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server. | 6.1 | More Details |
| CVE-2021-32470 | Craft CMS before 3.6.13 has an XSS vulnerability. | 6.1 | More Details |
| CVE-2021-21648 | Jenkins Credentials Plugin 2.3.18 and earlier does not escape user-controlled information on a view it provides, resulting in a reflected cross-site scripting (XSS) vulnerability. | 6.1 | More Details |
| CVE-2020-28014 | Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. The -oP option is available to the exim user, and allows a denial of service because root-owned files can be overwritten. | 6.1 | More Details |
| CVE-2020-23263 | Persistent Cross-site scripting vulnerability on Fork CMS version 5.8.2 allows remote attackers to inject arbitrary Javascript code via the "navigation_title" parameter and the "title" parameter in /private/en/pages/add. | 6.1 | More Details |
| CVE-2021-3507 | A heap buffer overflow was found in the floppy disk emulator of QEMU up to 6.0.0 (including). It could occur in fdctrl_transfer_handler() in hw/block/fdc.c while processing DMA read data transfers from the floppy drive to the guest system. A privileged guest user could use this flaw to crash the QEMU process on the host resulting in DoS scenario, or potential information leakage from the host memory. | 6.1 | More Details |
| CVE-2021-32052 | In Django 2.2 before 2.2.22, 3.1 before 3.1.10, and 3.2 before 3.2.2 (with Python 3.9.5+), URLValidator does not prohibit newlines and tabs (unless the URLField form field is used). If an application uses values with newlines in an HTTP response, header injection can occur. Django itself is unaffected because HttpResponse prohibits newlines in HTTP headers. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-20717 | Cross-site scripting vulnerability in EC-CUBE 4.0.0 to 4.0.5 allows a remote attacker to inject a specially crafted script in the specific input field of the EC web site which is created using EC-CUBE. As a result, it may lead to an arbitrary script execution on the administrator's web browser. | 6.1 | More Details |
| CVE-2021-24245 | The Stop Spammers WordPress plugin before 2021.9 did not escape user input when blocking requests (such as matching a spam word), outputting it in an attribute after sanitising it to remove HTML tags, which is not sufficient and lead to a reflected Cross-Site Scripting issue. | 6.1 | More Details |
| CVE-2021-24214 | The OpenID Connect Generic Client WordPress plugin 3.8.0 and 3.8.1 did not sanitise the login error when output back in the login form, leading to a reflected Cross-Site Scripting issue. This issue does not require authentication and can be exploited with the default configuration. | 6.1 | More Details |
| CVE-2021-24293 | In the eCommerce module of the NextGEN Gallery Pro WordPress plugin before 3.1.11, there is an action to call get_cart_items via photocrati_ajax , after that the settings[shipping_address][name] is able to inject malicious javascript. | 6.1 | More Details |
| CVE-2021-32091 | A Cross-site scripting (XSS) vulnerability exists in StackLift LocalStack 0.12.6. | 6.1 | More Details |
| CVE-2021-24276 | The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue | 6.1 | More Details |
| CVE-2021-24275 | The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue | 6.1 | More Details |
| CVE-2021-24274 | The Ultimate Maps by Supsystic WordPress plugin before 1.2.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue | 6.1 | More Details |
| CVE-2021-20397 | IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196017. | 6.1 | More Details |
| CVE-2020-13662 | Open Redirect vulnerability in Drupal Core allows a user to be tricked into visiting a specially crafted link which would redirect them to an arbitrary external URL. This issue affects: Drupal Drupal Core 7 version 7.70 and prior versions. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-13666 | Cross-site scripting vulnerability in Drupal Core. Drupal AJAX API does not disable JSONP by default, allowing for an XSS attack. This issue affects: Drupal Drupal Core 7.x versions prior to 7.73; 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6. | 6.1 | More Details |
| CVE-2021-31904 | In JetBrains TeamCity before 2020.2.2, XSS was potentially possible on the test history page. | 6.1 | More Details |
| CVE-2021-31903 | In JetBrains YouTrack before 2021.1.9819, a pull request's title was sanitized insufficiently, leading to XSS. | 6.1 | More Details |
| CVE-2021-32092 | A Cross-site scripting (XSS) vulnerability in the DocumentAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the uuid parameter. | 6.1 | More Details |
| CVE-2021-26122 | LivingLogic XIST4C before 0.107.8 allows XSS via feedback.htm or feedback.wihtm. | 6.1 | More Details |
| CVE-2021-27612 | In specific situations SAP GUI for Windows until and including 7.60 PL9, 7.70 PL0, forwards a user to specific malicious website which could contain malware or might lead to phishing attacks to steal credentials of the victim. | 6.1 | More Details |
| CVE-2021-31537 | SIS SIS-REWE Go before 7.7 SP17 allows XSS: rewe/prod/web/index.php (affected parameters are config, version, win, db, pwd, and user) and /rewe/prod/web/rewe_go_check.php (version and all other parameters). | 6.1 | More Details |
| CVE-2021-25179 | SolarWinds Serv-U before 15.2 is affected by Cross Site Scripting (XSS) via the HTTP Host header. | 6.1 | More Details |
| CVE-2021-28461 | Dynamics Finance and Operations Cross-site Scripting Vulnerability | 6.1 | More Details |
| CVE-2021-26123 | LivingLogic XIST4C before 0.107.8 allows XSS via login.htm, login.wihtm, or login-form.htm. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21527 | Dell PowerScale OneFS 8.1.0-9.1.0 contain an improper neutralization of special elements used in an OS command vulnerability. This vulnerability may allow an authenticated user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE privileges to escalate privileges. | 6.0 | More Details |
| CVE-2021-21550 | Dell EMC PowerScale OneFS 8.1.0-9.1.0 contain an improper neutralization of special elements used in an OS command vulnerability. This vulnerability can allow an authenticated user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE privileges to escalate privileges. | 6.0 | More Details |
| CVE-2021-1512 | A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. | 6.0 | More Details |
| CVE-2021-29495 | Nim is a statically typed compiled systems programming language. In Nim standard library before 1.4.2, httpClient SSL/TLS certificate verification was disabled by default. Users can upgrade to version 1.4.2 to receive a patch or, as a workaround, set "verifyMode = CVerifyPeer" as documented. | 5.9 | More Details |
| CVE-2021-31245 | omr-admin.py in openmptcprouter-vps-admin 0.57.3 and earlier compares the user provided password with the original password in a length dependent manner, which allows remote attackers to guess the password via a timing attack. | 5.9 | More Details |
| CVE-2020-11294 | Out of bound write in logger due to prefix size is not validated while prepended to logging string in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables | 5.9 | More Details |
| CVE-2021-29490 | Jellyfin is a free software media system that provides media from a dedicated server to end-user devices via multiple apps. Verions prior to 10.7.3 vulnerable to unauthenticated Server-Side Request Forgery (SSRF) attacks via the imageUrl parameter. This issue potentially exposes both internal and external HTTP servers or other resources available via HTTP `GET` that are visible from the Jellyfin server. The vulnerability is patched in version 10.7.3. As a workaround, disable external access to the API endpoints `/Items/*/RemoteImages/Download`, `/Items/RemoteSearch/Image` and `/Images/Remote` via reverse proxy, or limit to known-friendly IPs. | 5.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3502 | A flaw was found in avahi 0.8-5. A reachable assertion is present in avahi_s_host_name_resolver_start function allowing a local attacker to crash the avahi service by requesting hostname resolutions through the avahi socket or dbus methods for invalid hostnames. The highest threat from this vulnerability is to the service availability. | 5.5 | More Details |
| CVE-2021-31471 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12955. | 5.5 | More Details |
| CVE-2021-28479 | Windows CSC Service Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2021-31829 | kernel/bpf/verifier.c in the Linux kernel through 5.12.1 performs undesirable speculative loads, leading to disclosure of stack content via side-channel attacks, aka CID-801c6058d14a. The specific concern is not protecting the BPF stack area against speculative loads. Also, the BPF stack can contain uninitialized data that might represent sensitive information previously operated on by the kernel. | 5.5 | More Details |
| CVE-2021-31178 | Microsoft Office Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2021-1438 | A vulnerability in Cisco Wide Area Application Services (WAAS) Software could allow an authenticated, local attacker to gain access to sensitive information on an affected device. The vulnerability is due to improper input validation and authorization of specific commands that a user can execute within the CLI. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to read arbitrary files that they originally did not have permissions to access. | 5.5 | More Details |
| CVE-2021-31191 | Windows Projected File System FS Filter Driver Information Disclosure Vulnerability | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-28588 | An information disclosure vulnerability exists in the /proc/pid/syscall functionality of Linux Kernel 5.1 Stable and 5.4.66. More specifically, this issue has been introduced in v5.1-rc4 (commit 631b7abacd02b88f4b0795c08b54ad4fc3e7c7c0) and is still present in v5.10-rc4, so it's likely that all versions in between are affected. An attacker can read /proc/pid/syscall to trigger this vulnerability, which leads to the kernel leaking memory contents. | 5.5 | More Details |
| CVE-2021-31185 | Windows Desktop Bridge Denial of Service Vulnerability | 5.5 | More Details |
| CVE-2021-31184 | Microsoft Windows Infrared Data Association (IrDA) Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2021-28150 | Hongdian H8922 3.0.5 devices allow the unprivileged guest user to read cli.conf (with the administrator password and other sensitive data) via /backup2.cgi. | 5.5 | More Details |
| CVE-2021-31174 | Microsoft Excel Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2021-3315 | In JetBrains TeamCity before 2020.2.2, stored XSS on a tests page was possible. | 5.4 | More Details |
| CVE-2021-31908 | In JetBrains TeamCity before 2020.2.3, stored XSS was possible on several pages. | 5.4 | More Details |
| CVE-2020-4535 | IBM OpenPages GRC Platform 8.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182906. | 5.4 | More Details |
| CVE-2020-26147 | An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21649 | Jenkins Dashboard View Plugin 2.15 and earlier does not escape URLs referenced in Image Dashboard Portlets, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with View/Configure permission. | 5.4 | More Details |
| CVE-2021-32604 | Share/IncomingWizard.htm in SolarWinds Serv-U before 15.2.3 mishandles the user-supplied SenderEmail parameter, aka "Share URL XSS." | 5.4 | More Details |
| CVE-2021-3504 | A flaw was found in the hivex library in versions before 1.3.20. It is caused due to a lack of bounds check within the hivex_open function. An attacker could input a specially crafted Windows Registry (hive) file which would cause hivex to read memory beyond its normal bounds or cause the program to crash. The highest threat from this vulnerability is to system availability. | 5.4 | More Details |
| CVE-2021-24261 | The “HT Mega – Absolute Addons for Elementor Page Builder” WordPress Plugin before 1.5.7 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24265 | The “Rife Elementor Extensions & Templates” WordPress Plugin before 1.1.6 has a widget that is vulnerable to stored Cross-Site Scripting(XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24260 | The “Livemesh Addons for Elementor” WordPress Plugin before 6.8 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24243 | An AJAX action registered by the WPBakery Page Builder (Visual Composer) Clipboard WordPress plugin before 4.5.6 did not have capability checks nor sanitization, allowing low privilege users (subscriber+) to call it and set XSS payloads, which will be triggered in all backend pages. | 5.4 | More Details |
| CVE-2020-29444 | Affected versions of Team Calendar in Confluence Server before 7.11.0 allow attackers to inject arbitrary HTML or Javascript via a Cross Site Scripting Vulnerability in admin global setting parameters. | 5.4 | More Details |
| CVE-2021-24262 | The “WooLentor – WooCommerce Elementor Addons + Builder” WordPress Plugin before 1.8.6 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-24263 | The “Elementor Addons – PowerPack Addons for Elementor” WordPress Plugin before 2.3.2 for WordPress has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24264 | The “Image Hover Effects – Elementor Addon” WordPress Plugin before 1.3.4 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24266 | The “The Plus Addons for Elementor Page Builder Lite” WordPress Plugin before 2.0.6 has four widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24246 | The Workscout Core WordPress plugin before 1.3.4, used by the WorkScout Theme did not sanitise the chat messages sent via the workscout_send_message_chat AJAX action, leading to Stored Cross-Site Scripting and Cross-Frame Scripting issues | 5.4 | More Details |
| CVE-2021-24267 | The “All-in-One Addons for Elementor – WidgetKit” WordPress Plugin before 2.3.10 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24268 | The “JetWidgets For Elementor” WordPress Plugin before 1.0.9 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24269 | The “Sina Extension for Elementor” WordPress Plugin before 3.3.12 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24270 | The “DeTheme Kit for Elementor” WordPress Plugin before 1.5.5.5 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24271 | The “Ultimate Addons for Elementor” WordPress Plugin before 1.30.0 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24273 | The “Clever Addons for Elementor” WordPress Plugin before 2.1.0 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-24259 | The “Elementor Addon Elements” WordPress Plugin before 1.11.2 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-24258 | The Elements Kit Lite and Elements Kit Pro WordPress Plugins before 2.2.0 have a number of widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2020-23370 | In YzmCMS 5.6, stored XSS exists via the common/static/plugin/ueditor/1.4.3.3/php/controller.php action parameter, which allows remote attackers to upload a swf file. The swf file can be injected with arbitrary web script or HTML. | 5.4 | More Details |
| CVE-2021-24250 | The Business Directory Plugin – Easy Listing Directories for WordPress WordPress plugin before 5.11.2 suffered from lack of sanitisation in the label of the Form Fields, leading to Authenticated Stored Cross-Site Scripting issues across various pages of the plugin. | 5.4 | More Details |
| CVE-2021-27733 | In JetBrains YouTrack before 2020.6.6441, stored XSS was possible via an issue attachment. | 5.4 | More Details |
| CVE-2021-32544 | Special characters of IGT search function in igt+ are not filtered in specific fields, which allow remote authenticated attackers can inject malicious JavaScript and carry out DOM-based XSS (Cross-site scripting) attacks. | 5.4 | More Details |
| CVE-2021-30174 | RiyaLab CloudISO event item is added, special characters in specific field of time management page are not properly filtered, which allow remote authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks. | 5.4 | More Details |
| CVE-2020-23374 | Cross-site scripting (XSS) vulnerability in admin/article/add.html in noneCMS v1.3.0 allows remote authenticated attackers to inject arbitrary web script or HTML via the name parameter. | 5.4 | More Details |
| CVE-2020-23373 | Cross-site scripting (XSS) vulnerability in admin/nav/add.html in noneCMS v1.3.0 allows remote authenticated attackers to inject arbitrary web script or HTML via the name parameter. | 5.4 | More Details |
| CVE-2021-24257 | The “Premium Addons for Elementor” WordPress Plugin before 4.2.8 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1530 | A vulnerability in the web-based management interface of Cisco BroadWorks Messaging Server Software could allow an authenticated, remote attacker to access sensitive information or cause a partial denial of service (DoS) condition on an affected system. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a partial DoS condition on an affected system. There are workarounds that address this vulnerability. | 5.4 | More Details |
| CVE-2021-29250 | BTCPay Server through 1.0.7.0 suffers from a Stored Cross Site Scripting (XSS) vulnerability within the POS Add Products functionality. This enables cookie stealing. | 5.4 | More Details |
| CVE-2020-4929 | IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 191706. | 5.4 | More Details |
| CVE-2021-20559 | IBM Control Desk 7.6.1.2 and 7.6.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199228. | 5.4 | More Details |
| CVE-2021-24255 | The Essential Addons for Elementor Lite WordPress Plugin before 4.5.4 has two widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, both via a similar method. | 5.4 | More Details |
| CVE-2021-24247 | The Contact Form Check Tester WordPress plugin through 1.0.2 settings are visible to all registered users in the dashboard and are lacking any sanitisation. As a result, any registered user, such as subscriber, can leave an XSS payload in the plugin settings, which will be triggered by any user visiting them, and could allow for privilege escalation. The vendor decided to close the plugin. | 5.4 | More Details |
| CVE-2021-24256 | The “Elementor – Header, Footer & Blocks Template” WordPress Plugin before 1.5.8 has two widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. | 5.4 | More Details |
| CVE-2021-31173 | Microsoft SharePoint Server Information Disclosure Vulnerability | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32062 | MapServer before 7.0.8, 7.1.x and 7.2.x before 7.2.3, 7.3.x and 7.4.x before 7.4.5, and 7.5.x and 7.6.x before 7.6.3 does not properly enforce the MS_MAP_NO_PATH and MS_MAP_PATTERN restrictions that are intended to control the locations from which a mapfile may be loaded (with MapServer CGI). | 5.3 | More Details |
| CVE-2021-1535 | A vulnerability in the cluster management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to view sensitive information on an affected system. To be affected by this vulnerability, the Cisco SD-WAN vManage Software must be in cluster mode. This vulnerability is due to the absence of authentication for sensitive information in the cluster management interface. An attacker could exploit this vulnerability by sending a crafted request to the cluster management interface of an affected system. A successful exploit could allow the attacker to allow the attacker to view sensitive information on the affected system. | 5.3 | More Details |
| CVE-2021-1499 | A vulnerability in the web-based management interface of Cisco HyperFlex HX Data Platform could allow an unauthenticated, remote attacker to upload files to an affected device. This vulnerability is due to missing authentication for the upload function. An attacker could exploit this vulnerability by sending a specific HTTP request to an affected device. A successful exploit could allow the attacker to upload files to the affected device with the permissions of the tomcat8 user. | 5.3 | More Details |
| CVE-2021-31900 | In JetBrains Code With Me bundled to the compatible IDE versions before 2021.1, a client could open a browser on a host. | 5.3 | More Details |
| CVE-2021-1486 | A vulnerability in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to enumerate user accounts. This vulnerability is due to the improper handling of HTTP headers. An attacker could exploit this vulnerability by sending authenticated requests to an affected system. A successful exploit could allow the attacker to compare the HTTP responses that are returned by the affected system to determine which accounts are valid user accounts. | 5.3 | More Details |
| CVE-2021-1478 | A vulnerability in the Java Management Extensions (JMX) component of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. This vulnerability is due to an unsecured TCP/IP port. An attacker could exploit this vulnerability by accessing the port and restarting the JMX process. A successful exploit could allow the attacker to cause a DoS condition on an affected system. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-26139 | An issue was discovered in the kernel in NetBSD 7.1. An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients. | 5.3 | More Details |
| CVE-2020-26142 | An issue was discovered in the kernel in OpenBSD 6.6. The WEP, WPA, WPA2, and WPA3 implementations treat fragmented frames as full frames. An adversary can abuse this to inject arbitrary network packets, independent of the network configuration. | 5.3 | More Details |
| CVE-2020-26146 | An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design. | 5.3 | More Details |
| CVE-2021-29248 | BTCPay Server through 1.0.7.0 could allow a remote attacker to obtain sensitive information, caused by failure to set the Secure flag for a cookie. | 5.3 | More Details |
| CVE-2021-29247 | BTCPay Server through 1.0.7.0 could allow a remote attacker to obtain sensitive information, caused by failure to set the HTTPOnly flag for a cookie. | 5.3 | More Details |
| CVE-2021-29245 | BTCPay Server through 1.0.7.0 uses a weak method Next to produce pseudo-random values to generate a legacy API key. | 5.3 | More Details |
| CVE-2019-25043 | ModSecurity 3.x before 3.0.4 mishandles key-value pair parsing, as demonstrated by a "string index out of range" error and worker-process crash for a "Cookie: =abc" header. | 5.3 | More Details |
| CVE-2021-22210 | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.2. When querying the repository branches through API, GitLab was ignoring a query parameter and returning a considerable amount of results. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21419 | Eventlet is a concurrent networking library for Python. A websocket peer may exhaust memory on Eventlet side by sending very large websocket frames. Malicious peer may exhaust memory on Eventlet side by sending highly compressed data frame. A patch in version 0.31.0 restricts websocket frame to reasonable limits. As a workaround, restricting memory usage via OS limits would help against overall machine exhaustion, but there is no workaround to protect Eventlet process. | 5.3 | More Details |
| CVE-2021-27569 | An issue was discovered in Emote Remote Mouse through 4.0.0.0. Attackers can maximize or minimize the window of a running process by sending the process name in a crafted packet. This information is sent in cleartext and is not protected by any authentication logic. | 5.3 | More Details |
| CVE-2021-31907 | In JetBrains TeamCity before 2020.2.2, permission checks for changing TeamCity plugins were implemented improperly. | 5.3 | More Details |
| CVE-2021-32053 | JPA Server in HAPI FHIR before 5.4.0 allows a user to deny service (e.g., disable access to the database after the attack stops) via history requests. This occurs because of a SELECT COUNT statement that requires a full index scan, with an accompanying large amount of server resources if there are many simultaneous history requests. | 5.3 | More Details |
| CVE-2021-27570 | An issue was discovered in Emote Remote Mouse through 3.015. Attackers can close any running process by sending the process name in a specially crafted packet. This information is sent in cleartext and is not protected by any authentication logic. | 5.3 | More Details |
| CVE-2021-29022 | In InvoicePlane 1.5.11, the upload feature discloses the full path of the file upload directory. | 5.3 | More Details |
| CVE-2021-23016 | On BIG-IP APM versions 15.1.x before 15.1.3, 14.1.x before 14.1.4.1, 13.1.x before 13.1.4, and all versions of 16.0.x, 12.1.x, and 11.6.x, an attacker may be able to bypass APM's internal restrictions and retrieve static content that is hosted within APM by sending specifically crafted requests to an APM Virtual Server. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 5.3 | More Details |
| CVE-2021-3003 | Agenzia delle Entrate Desktop Telematico 1.0.0 contacts the jws.agenziaentrate.it server over cleartext HTTP, which allows man-in-the-middle attackers to spoof product updates. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-27571 | An issue was discovered in Emote Remote Mouse through 4.0.0.0. Attackers can retrieve recently used and running applications, their icons, and their file paths. This information is sent in cleartext and is not protected by any authentication logic. | 5.3 | More Details |
| CVE-2020-11293 | Out of bound read can happen in Widevine TA while copying data to buffer from user data due to lack of check of buffer length received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 5.1 | More Details |
| CVE-2020-4993 | IBM QRadar SIEM 7.3 and 7.4 when decompressing or verifying signature of zip files processes data in a way that may be vulnerable to path traversal attacks. IBM X-Force ID: 192905. | 4.9 | More Details |
| CVE-2021-27617 | The Integration Builder Framework of SAP Process Integration versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate an XML document uploaded from local source. An attacker can craft a malicious XML which when uploaded and parsed by the application, could lead to Denial-of-service conditions due to consumption of a large amount of system memory, thus highly impacting system availability. | 4.9 | More Details |
| CVE-2021-27618 | The Integration Builder Framework of SAP Process Integration versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not check the file type extension of the file uploaded from local source. An attacker could craft a malicious file and upload it to the application, which could lead to denial of service and impact the availability of the application. | 4.9 | More Details |
| CVE-2020-23128 | Chamilo LMS 1.11.10 does not properly manage privileges which could allow a user with Sessions administrator privilege to create a new user then use the edit user function to change this new user to administrator privilege. | 4.9 | More Details |
| CVE-2020-22428 | SolarWinds Serv-U before 15.1.6 Hotfix 3 is affected by Cross Site Scripting (XSS) via a directory name (entered by an admin) containing a JavaScript payload. | 4.8 | More Details |
| CVE-2021-32103 | A Stored XSS vulnerability in interface/usergroup/usergroup_admin.php in OpenEMR before 5.0.2.1 allows a admin authenticated user to inject arbitrary web script or HTML via the lname parameter. | 4.8 | More Details |
| CVE-2021-32573 | The express-cart package through 1.1.10 for Node.js allows Reflected XSS (for an admin) via a user input field for product options. NOTE: the vendor states that this "would rely on an admin hacking his/her own website. | 4.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1397 | A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. | 4.7 | More Details |
| CVE-2021-1490 | A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by persuading a user to retrieve a crafted file that contains malicious payload and upload it to the affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. | 4.7 | More Details |
| CVE-2021-1519 | A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client Software could allow an authenticated, local attacker to overwrite VPN profiles on an affected device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to modify VPN profile files. To exploit this vulnerability, the attacker must have valid credentials on the affected system. | 4.7 | More Details |
| CVE-2021-30170 | Special characters of ERP POS customer profile page are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks, additionally access and manipulate customer's information. | 4.6 | More Details |
| CVE-2021-26418 | Microsoft SharePoint Server Spoofing Vulnerability | 4.6 | More Details |
| CVE-2021-30171 | Special characters of ERP POS news page are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks, additionally access and manipulate customer's information. | 4.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-27941 | Unconstrained Web access to the device's private encryption key in the QR code pairing mode in the eWeLink mobile application (through 4.9.2 on Android and through 4.9.1 on iOS) allows a physically proximate attacker to eavesdrop on Wi-Fi credentials and other sensitive information by monitoring the Wi-Fi spectrum during a device pairing process. | 4.6 | More Details |
| CVE-2021-30172 | Special characters of picture preview page in the Quan-Fang-Wei-Tong-Xun system are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out Reflected XSS (Cross-site scripting) attacks, additionally access and manipulate customer's information. | 4.6 | More Details |
| CVE-2021-32489 | An issue was discovered in the _send_secure_msg() function of Yubico yubihsm-shell through 2.0.3. The function does not correctly validate the embedded length field of an authenticated message received from the device because response_msg.st.len=8 can be accepted but triggers an integer overflow, which causes CRYPTO_cbc128_decrypt (in OpenSSL) to encounter an undersized buffer and experience a segmentation fault. The yubihsm-shell project is included in the YubiHSM 2 SDK product. | 4.4 | More Details |
| CVE-2021-25645 | An issue was discovered in Couchbase Server before 6.0.5, 6.1.x through 6.5.x before 6.5.2, and 6.6.x before 6.6.1. An internal user with administrator privileges, @ns_server, leaks credentials in cleartext in the cbcollect_info.log, debug.log, ns_couchdb.log, indexer.log, and stats.log files. NOTE: updating the product does not automatically address leaks that occurred in the past. | 4.4 | More Details |
| CVE-2021-21654 | Jenkins P4 Plugin 1.11.4 and earlier does not perform permission checks in multiple HTTP endpoints, allowing attackers with Overall/Read permission to connect to an attacker-specified Perforce server using attacker-specified username and password. | 4.3 | More Details |
| CVE-2021-1516 | A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-29445 | Affected versions of Confluence Server before 7.4.8, and versions from 7.5.0 before 7.11.0 allow attackers to identify internal hosts and ports via a blind server-side request forgery vulnerability in Team Calendars parameters. | 4.3 | More Details |
| CVE-2021-32056 | Cyrus IMAP before 3.2.7, and 3.3.x and 3.4.x before 3.4.1, allows remote authenticated users to bypass intended access restrictions on server annotations and consequently cause replication to stall. | 4.3 | More Details |
| CVE-2021-22208 | An issue has been discovered in GitLab affecting versions starting with 13.5 up to 13.9.7. Improper permission check could allow the change of timestamp for issue creation or update. | 4.3 | More Details |
| CVE-2021-21650 | Jenkins S3 publisher Plugin 0.11.6 and earlier does not perform Run/Artifacts permission checks in various HTTP endpoints and API models, allowing attackers with Item/Read permission to obtain information about artifacts uploaded to S3, if the optional Run/Artifacts permission is enabled. | 4.3 | More Details |
| CVE-2021-21651 | Jenkins S3 publisher Plugin 0.11.6 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to obtain the list of configured profiles. | 4.3 | More Details |
| CVE-2021-21653 | Jenkins Xray - Test Management for Jira Plugin 2.4.0 and earlier does not perform a permission check in an HTTP endpoint, allowing with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. | 4.3 | More Details |
| CVE-2021-24272 | The fitness calculators WordPress plugin before 1.9.6 add calculators for Water intake, BMI calculator, protein Intake, and Body Fat and was lacking CSRF check, allowing attackers to make logged in users perform unwanted actions, such as change the calculator headers. Due to the lack of sanitisation, this could also lead to a Stored Cross-Site Scripting issue | 4.3 | More Details |
| CVE-2021-1515 | A vulnerability in Cisco SD-WAN vManage Software could allow an unauthenticated, adjacent attacker to gain access to sensitive information. This vulnerability is due to improper access controls on API endpoints when Cisco SD-WAN vManage Software is running in multi-tenant mode. An attacker with access to a device that is managed in the multi-tenant environment could exploit this vulnerability by sending a request to an affected API endpoint on the vManage system. A successful exploit could allow the attacker to gain access to sensitive information that may include hashed credentials that could be used in future attacks. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-4536 | IBM OpenPages GRC Platform 8.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 182907. | 4.3 | More Details |
| CVE-2021-24251 | The Business Directory Plugin – Easy Listing Directories for WordPress WordPress plugin before 5.11.2 suffered from a Cross-Site Request Forgery issue, allowing an attacker to make a logged in administrator update arbitrary payment history, such as change their status (from pending to completed to example) | 4.3 | More Details |
| CVE-2021-29488 | SABnzbd is an open source binary newsreader. A vulnerability was discovered in SABnzbd that could trick the `filesystem.renamer()` function into writing downloaded files outside the configured Download Folder via malicious PAR2 files. A patch was released as part of SABnzbd 3.2.1RC1. As a workaround, limit downloads to NZBs without PAR2 files, deny write permissions to the SABnzbd process outside areas it must access to perform its job, or update to a fixed version. | 4.3 | More Details |
| CVE-2021-31171 | Microsoft SharePoint Information Disclosure Vulnerability | 4.1 | More Details |
| CVE-2021-29471 | Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.33.2 "Push rules" can specify conditions under which they will match, including `event_match`, which matches event content against a pattern including wildcards. Certain patterns can cause very poor performance in the matching engine, leading to a denial-of-service when processing moderate length events. The issue is patched in version 1.33.2. A potential workaround might be to prevent users from making custom push rules, by blocking such requests at a reverse-proxy. | 3.7 | More Details |
| CVE-2020-24586 | The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to inject arbitrary network packets and/or exfiltrate user data. | 3.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-24588 | The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets. | 3.5 | More Details |
| CVE-2021-31447 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13269. | 3.3 | More Details |
| CVE-2021-25317 | A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. | 3.3 | More Details |
| CVE-2021-26309 | Information disclosure in the TeamCity plugin for IntelliJ before 2020.2.2.85899 was possible because a local temporary file had Insecure Permissions. | 3.3 | More Details |
| CVE-2021-31443 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13240. | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31444 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13241. | 3.3 | More Details |
| CVE-2021-31445 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13244. | 3.3 | More Details |
| CVE-2021-31448 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13273. | 3.3 | More Details |
| CVE-2021-31469 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12936. | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31446 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13245. | 3.3 | More Details |
| CVE-2021-31467 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D files embedded in PDF documents. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13621. | 3.3 | More Details |
| CVE-2021-31464 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13574. | 3.3 | More Details |
| CVE-2021-31463 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13573. | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31462 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13572. | 3.3 | More Details |
| CVE-2021-22211 | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7. GitLab Dependency Proxy, under certain circumstances, can impersonate a user resulting in possibly incorrect access handling. | 3.1 | More Details |
| CVE-2021-31906 | In JetBrains TeamCity before 2020.2.2, audit logs were not sufficient when an administrator uploaded a file. | 2.7 | More Details |
| CVE-2020-24587 | The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed. | 2.6 | More Details |
| CVE-2021-29491 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-28860. Reason: This candidate is a reservation duplicate of CVE-2021-28860. Notes: All CVE users should reference CVE-2021-28860 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage | N/A | More Details |
| CVE-2021-31877 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA due to lack of a reference providing provenance. Notes: none | N/A | More Details |
| CVE-2021-32259 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA | N/A | More Details |