SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 29 September 2021

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

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

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

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

## CRITICAL VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34770 | A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a logic error that occurs during the validation of CAPWAP packets. An attacker could exploit this vulnerability by sending a crafted CAPWAP packet to an affected device. A successful exploit could allow the attacker to execute arbitrary code with administrative privileges or cause the affected device to crash and reload, resulting in a DoS condition. | 10.0 | More Details |
| CVE-2021-31819 | In Halibut versions prior to 4.4.7 there is a deserialisation vulnerability that could allow remote code execution on systems that already trust each other based on certificate verification. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41558 | The set_user extension module before 3.0.0 for PostgreSQL allows ProcessUtility_hook bypass via set_config. | 9.8 | More Details |
| CVE-2021-34416 | The network address administrative settings web portal for the Zoom on-premise Meeting Connector before version 4.6.360.20210325, Zoom on-premise Meeting Connector MMR before version 4.6.360.20210325, Zoom on-premise Recording Connector before version 3.8.44.20210326, Zoom on-premise Virtual Room Connector before version 4.4.6752.20210326, and Zoom on-premise Virtual Room Connector Load Balancer before version 2.5.5495.20210326 fails to validate input sent in requests to update the network configuration, which could lead to remote command injection on the on-premise image by the web portal administrators. | 9.8 | More Details |
| CVE-2021-36219 | An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address is then freed, resulting in compromised integrity of the enclave. This was resolved after v1.58.3 and not reproducible in sgxwallet v1.77.0. | 9.8 | More Details |
| CVE-2021-37539 | Zoho ManageEngine ADManager Plus before 7111 is vulnerable to unrestricted file which leads to Remote code execution. | 9.8 | More Details |
| CVE-2021-24666 | The Podlove Podcast Publisher WordPress plugin before 3.5.6 contains a 'Social & Donations' module (not activated by default), which adds the rest route '/services/contributor/(?P<id>[\d]+), takes an 'id' and 'category' parameters as arguments. Both parameters can be used for the SQLi. | 9.8 | More Details |
| CVE-2021-36879 | Unauthenticated Privilege Escalation vulnerability in WordPress uListing plugin (versions <= 2.0.5). Possible if WordPress configuration allows user registration. | 9.8 | More Details |
| CVE-2021-37761 | Zoho ManageEngine ADManager Plus version 7110 and prior is vulnerable to unrestricted file upload, leading to remote code execution. | 9.8 | More Details |
| CVE-2021-40329 | The Authentication API in Ping Identity PingFederate before 10.3 mishandles certain aspects of external password management. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-37270 | There is an unauthorized access vulnerability in the CMS Enterprise Website Construction System 5.0. Attackers can use this vulnerability to directly access the specified background path without logging in to the background to obtain the background administrator authority. | 9.8 | More Details |
| CVE-2021-36260 | A command injection vulnerability in the web server of some Hikvision product. Due to the insufficient input validation, attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands. | 9.8 | More Details |
| CVE-2021-38124 | Remote Code Execution vulnerability in Micro Focus ArcSight Enterprise Security Manager (ESM) product, affecting versions 7.0.2 through 7.5. The vulnerability could be exploited resulting in remote code execution. | 9.8 | More Details |
| CVE-2021-36363 | Nagios XI before 5.8.5 has Incorrect Permission Assignment for migrate.php. | 9.8 | More Details |
| CVE-2021-36364 | Nagios XI before 5.8.5 incorrectly allows backup_xi.sh wildcards. | 9.8 | More Details |
| CVE-2021-36365 | Nagios XI before 5.8.5 has Incorrect Permission Assignment for repairmysql.sh. | 9.8 | More Details |
| CVE-2021-36366 | Nagios XI before 5.8.5 incorrectly allows manage_services.sh wildcards. | 9.8 | More Details |
| CVE-2021-38303 | A SQL injection vulnerability exists in Sureline SUREedge Migrator 7.0.7.29360. | 9.8 | More Details |
| CVE-2020-20120 | ThinkPHP v3.2.3 and below contains a SQL injection vulnerability which is triggered when the array is not passed to the "where" and "query" methods. | 9.8 | More Details |
| CVE-2021-33907 | The Zoom Client for Meetings for Windows in all versions before 5.3.0 fails to properly validate the certificate information used to sign .msi files when performing an update of the client. This could lead to remote code execution in an elevated privileged context. | 9.8 | More Details |
| CVE-2021-40098 | An issue was discovered in Concrete CMS through 8.5.5. Path Traversal leading to RCE via external form by adding a regular expression. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-38299 | Webauthn Framework 3.3.x before 3.3.4 has Incorrect Access Control. An attacker that controls a user's system is able to login to a vulnerable service using an attached FIDO2 authenticator without passing a check of the user presence. | 9.8 | More Details |
| CVE-2021-34351 | A command injection vulnerability has been reported to affect QNAP device running QVR. If exploited, this vulnerability could allow remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.5 build 20210803 and later | 9.8 | More Details |
| CVE-2021-37925 | Zoho ManageEngine ADManager Plus version 7110 and prior has a Post-Auth OS command injection vulnerability. | 9.8 | More Details |
| CVE-2021-37927 | Zoho ManageEngine ADManager Plus version 7110 and prior allows account takeover via SSO. | 9.8 | More Details |
| CVE-2019-6288 | Edgecore ECS2020 Firmware 1.0.0.0 devices allow Unauthenticated Command Injection via the command1 HTTP header to the /EXCU_SHELL URI. | 9.8 | More Details |
| CVE-2021-1619 | A vulnerability in the authentication, authorization, and accounting (AAA) function of Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass NETCONF or RESTCONF authentication and do either of the following: Install, manipulate, or delete the configuration of an affected device Cause memory corruption that results in a denial of service (DoS) on an affected device This vulnerability is due to an uninitialized variable. An attacker could exploit this vulnerability by sending a series of NETCONF or RESTCONF requests to an affected device. A successful exploit could allow the attacker to use NETCONF or RESTCONF to install, manipulate, or delete the configuration of a network device or to corrupt memory on the device, resulting a DoS. | 9.8 | More Details |
| CVE-2021-34727 | A vulnerability in the vDaemon process in Cisco IOS XE SD-WAN Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device. This vulnerability is due to insufficient bounds checking when an affected device processes traffic. An attacker could exploit this vulnerability by sending crafted traffic to the device. A successful exploit could allow the attacker to cause a buffer overflow and possibly execute arbitrary commands with root-level privileges, or cause the device to reload, which could result in a denial of service condition. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22005 | The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file. | 9.8 | More Details |
| CVE-2021-22941 | Improper Access Control in Citrix ShareFile storage zones controller before 5.11.20 may allow an unauthenticated attacker to remotely compromise the storage zones controller. | 9.8 | More Details |
| CVE-2020-20122 | Wuzhi CMS v4.1 contains a SQL injection vulnerability in the checktitle() function in /coreframe/app/content/admin/content.php. | 9.8 | More Details |
| CVE-2021-21913 | An information disclosure vulnerability exists in the WiFi Smart Mesh functionality of D-LINK DIR-3040 1.13B03. A specially-crafted network request can lead to command execution. An attacker can connect to the MQTT service to trigger this vulnerability. | 9.8 | More Details |
| CVE-2020-4690 | IBM Security Guardium 11.3 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: 186697. | 9.8 | More Details |
| CVE-2021-26794 | Privilege escalation in 'upload.php' in FrogCMS SentCMS v0.9.5 allows attacker to execute arbitrary code via crafted php file. | 9.8 | More Details |
| CVE-2021-22869 | An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in 3.0.16 and 3.1.8 releases. | 9.8 | More Details |
| CVE-2021-34348 | A command injection vulnerability has been reported to affect QNAP device running QVR. If exploited, this vulnerability could allow remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.5 build 20210803 and later | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-20034 | An improper access control vulnerability in SMA100 allows a remote unauthenticated attacker to bypass the path traversal checks and delete an arbitrary file potentially resulting in a reboot to factory default settings. | 9.1 | More Details |
| CVE-2021-22945 | When sending data to an MQTT server, libcurl <= 7.73.0 and 7.78.0 could in some circumstances erroneously keep a pointer to an already freed memory area and both use that again in a subsequent call to send data and also free it *again*. | 9.1 | More Details |
| CVE-2021-40684 | Talend ESB Runtime in all versions from 5.1 to 7.3.1-R2021-09, 7.2.1-R2021-09, 7.1.1-R2021-09, has an unauthenticated Jolokia HTTP endpoint which allows remote access to the JMX of the runtime container, which would allow an attacker the ability to read or modify the container or software running in the container. | 9.1 | More Details |
| CVE-2021-40102 | An issue was discovered in Concrete CMS through 8.5.5. Arbitrary File deletion can occur via PHAR deserialization in is_dir (PHP Object Injection associated with the __wakeup magic method). | 9.1 | More Details |
| CVE-2021-41097 | aurelia-path is part of the Aurelia platform and contains utilities for path manipulation. There is a prototype pollution vulnerability in aurelia-path before version 1.1.7. The vulnerability exposes Aurelia application that uses `aurelia-path` package to parse a string. The majority of this will be Aurelia applications that employ the `aurelia-router` package. An example is this could allow an attacker to change the prototype of base object class `Object` by tricking an application to parse the following URL: `https://aurelia.io/blog/?__proto__[asdf]=asdf`. The problem is patched in version `1.1.7`. | 9.1 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-20693 | A Cross-Site Request Forgery (CSRF) in GilaCMS v1.11.4 allows authenticated attackers to arbitrarily add administrator accounts. | 8.8 | More Details |
| CVE-2021-34636 | The Countdown and CountUp, WooCommerce Sales Timers WordPress plugin is vulnerable to Cross-Site Request Forgery via the save_theme function found in the ~/includes/admin/coundown_theme_page.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.7. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-40097 | An issue was discovered in Concrete CMS through 8.5.5. Authenticated path traversal leads to to remote code execution via uploaded PHP code, related to the bFilename parameter. | 8.8 | More Details |
| CVE-2021-22952 | A vulnerability found in UniFi Talk application V1.12.3 and earlier permits a malicious actor who has already gained access to a network to subsequently control Talk device(s) assigned to said network if they are not yet adopted. This vulnerability is fixed in UniFi Talk application V1.12.5 and later. | 8.8 | More Details |
| CVE-2021-3819 | firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) | 8.8 | More Details |
| CVE-2020-19951 | A cross-site request forgery (CSRF) in /controller/pay.class.php of YzmCMS v5.5 allows attackers to access sensitive components of the application. | 8.8 | More Details |
| CVE-2021-40108 | An issue was discovered in Concrete CMS through 8.5.5. The Calendar is vulnerable to CSRF. ccm_token is not verified on the ccm/calendar/dialogs/event/add/save endpoint. | 8.8 | More Details |
| CVE-2021-37274 | Kingdee KIS Professional Edition has a privilege escalation vulnerability. Attackers can use the vulnerability to gain computer administrator rights via unspecified loopholes. | 8.8 | More Details |
| CVE-2021-38112 | In the Amazon AWS WorkSpaces client 3.0.10 through 3.1.8 on Windows, argument injection in the workspaces:// URI handler can lead to remote code execution because of the Chromium Embedded Framework (CEF) --gpu-launcher argument. This is fixed in 3.1.9. | 8.8 | More Details |
| CVE-2020-20124 | Wuzhi CMS v4.1.0 contains a remote code execution (RCE) vulnerability in \attachment\admin\index.php. | 8.8 | More Details |
| CVE-2021-40309 | A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0. allows an attacker to inject their own SQL query. The cp_id_miss_attn parameter from TakeAttendance.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request as a user with access to "Take Attendance" functionality to trigger this vulnerability. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34769 | Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit the vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition. | 8.6 | More Details |
| CVE-2021-1611 | A vulnerability in Ethernet over GRE (EoGRE) packet processing of Cisco IOS XE Wireless Controller Software for the Cisco Catalyst 9800 Family Wireless Controller, Embedded Wireless Controller, and Embedded Wireless on Catalyst 9000 Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper processing of malformed EoGRE packets. An attacker could exploit this vulnerability by sending malicious packets to the affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. | 8.6 | More Details |
| CVE-2021-1615 | A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. | 8.6 | More Details |
| CVE-2021-36880 | Unauthenticated SQL Injection (SQLi) vulnerability in WordPress uListing plugin (versions <= 2.0.3), vulnerable parameter: custom. | 8.6 | More Details |
| CVE-2021-39826 | Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could leverage this vulnerability to execute arbitrary commands. User interaction is required to abuse this vulnerability in that a user must open a maliciously crafted .epub file. | 8.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34768 | Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit the vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition. | 8.6 | More Details |
| CVE-2021-1622 | A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. | 8.6 | More Details |
| CVE-2021-1624 | A vulnerability in the Rate Limiting Network Address Translation (NAT) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause high CPU utilization in the Cisco QuantumFlow Processor of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to mishandling of the rate limiting feature within the QuantumFlow Processor. An attacker could exploit this vulnerability by sending large amounts of traffic that would be subject to NAT and rate limiting through an affected device. A successful exploit could allow the attacker to cause the QuantumFlow Processor utilization to reach 100 percent on the affected device, resulting in a DoS condition. | 8.6 | More Details |
| CVE-2021-1565 | Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit the vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition. | 8.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21522 | Dell BIOS contains a Credentials Management issue. A local authenticated malicious user may potentially exploit this vulnerability to gain access to sensitive information on an NVMe storage by resetting the BIOS password on the system via the Manageability Interface. | 8.2 | More Details |
| CVE-2021-31841 | A DLL sideloading vulnerability in McAfee Agent for Windows prior to 5.7.4 could allow a local user to perform a DLL sideloading attack with an unsigned DLL with a specific name and in a specific location. This would result in the user gaining elevated permissions and the ability to execute arbitrary code as the system user, through not checking the DLL signature. | 8.2 | More Details |
| CVE-2021-31847 | Improper access control vulnerability in the repair process for McAfee Agent for Windows prior to 5.7.4 could allow a local attacker to perform a DLL preloading attack using unsigned DLLs. This would result in elevation of privileges and the ability to execute arbitrary code as the system user, through not correctly protecting a temporary directory used in the repair process and not checking the DLL signature. | 8.2 | More Details |
| CVE-2021-41588 | In Gradle Enterprise before 2021.1.3, a crafted request can trigger deserialization of arbitrary unsafe Java objects. The attacker must have the encryption and signing keys. | 8.1 | More Details |
| CVE-2020-24930 | Beijing Wuzhi Internet Technology Co., Ltd. Wuzhi CMS 4.0.1 is an open source content management system. The five fingers CMS backend in***.php file has arbitrary file deletion vulnerability. Attackers can use vulnerabilities to delete arbitrary files. | 8.1 | More Details |
| CVE-2020-20514 | A Cross-Site Request Forgery (CSRF) in Maccms v10 via admin.php/admin/admin/del/ids/<id>.html allows authenticated attackers to delete all users. | 8.1 | More Details |
| CVE-2021-32959 | Heap-based buffer overflow in SuiteLink server while processing commands 0x05/0x06 | 8.1 | More Details |
| CVE-2021-41504 | An Elevated Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer | 8.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41088 | Elvish is a programming language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (started by `elvish -web`) hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly. As a result, if the user has the web UI backend open and visits a compromised or malicious website, the website can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be patched for previous versions by removing the web UI (found in web, pkg/web or pkg/prog/web, depending on the exact version). | 8.0 | More Details |
| CVE-2021-41503 | DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer | 8.0 | More Details |
| CVE-2021-41536 | A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13778). | 7.8 | More Details |
| CVE-2021-29366 | A buffer overflow vulnerability in FORMATS!GetPlugInInfo+0x2de9 of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted RLE file. | 7.8 | More Details |
| CVE-2021-29367 | A buffer overflow vulnerability in WPG+0x1dda of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted WPG file. | 7.8 | More Details |
| CVE-2021-22015 | The vCenter Server contains multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server Appliance. | 7.8 | More Details |
| CVE-2021-40709 | Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41537 | A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13789). | 7.8 | More Details |
| CVE-2021-41535 | A vulnerability has been identified in NX 1953 Series (All versions < V1973.3700), NX 1980 Series (All versions < V1988), Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771). | 7.8 | More Details |
| CVE-2021-28130 | Dr.Web Firewall 12.5.2.4160 on Windows incorrectly restricts applications signed by Dr.Web. A DLL for a custom payload within a legitimate binary (e.g., frwl_svc.exe) bypasses firewall filters. | 7.8 | More Details |
| CVE-2021-33035 | Apache OpenOffice opens dBase/DBF documents and shows the contents as spreadsheets. DBF are database files with data organized in fields. When reading DBF data the size of certain fields is not checked: the data is just copied into local variables. A carefully crafted document could overflow the allocated space, leading to the execution of arbitrary code by altering the contents of the program stack. This issue affects Apache OpenOffice up to and including version 4.1.10 | 7.8 | More Details |
| CVE-2021-41540 | A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13776). | 7.8 | More Details |
| CVE-2021-26750 | DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. | 7.8 | More Details |
| CVE-2021-29364 | A buffer overflow vulnerability in Formats!ReadRAS_W+0x1001 of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted RLE file. | 7.8 | More Details |
| CVE-2021-29363 | A buffer overflow vulnerability in FORMATS!ReadRAS_W+0xa74 of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted RLE file.0xa74 | 7.8 | More Details |
| CVE-2021-29362 | A buffer overflow vulnerability in FORMATS!ReadRAS_W+0xa30 of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted RLE file. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-2464 | Vulnerability in Oracle Linux (component: OSwatcher). Supported versions that are affected are 7 and 8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Linux executes to compromise Oracle Linux. Successful attacks of this vulnerability can result in takeover of Oracle Linux. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). | 7.8 | More Details |
| CVE-2021-41539 | A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13773). | 7.8 | More Details |
| CVE-2021-29361 | A buffer overflow vulnerability in FORMATS!Read_Utah_RLE+0x340 of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted RLE file. | 7.8 | More Details |
| CVE-2021-1419 | A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. | 7.8 | More Details |
| CVE-2021-34408 | The Zoom Client for Meetings for Windows in all versions before version 5.3.2 writes log files to a user writable directory as a privileged user during the installation or update of the client. This could allow for potential privilege escalation if a link was created between the user writable directory used and a non-user writable directory. | 7.8 | More Details |
| CVE-2021-34410 | A user-writable application bundle unpacked during the install for all versions of the Zoom Plugin for Microsoft Outlook for Mac before 5.0.25611.0521 allows for privilege escalation to root. | 7.8 | More Details |
| CVE-2021-0611 | In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. | 7.8 | More Details |
| CVE-2021-39818 | Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34411 | During the installation process forZoom Rooms for Conference Room for Windows before version 5.3.0 it is possible to launch Internet Explorer with elevated privileges. If the installer was launched with elevated privileges such as by SCCM this can result in a local privilege escalation. | 7.8 | More Details |
| CVE-2021-0612 | In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. | 7.8 | More Details |
| CVE-2021-29360 | A buffer overflow vulnerability in FORMATS!Read_Utah_RLE+0x37a of Irfanview 4.57 allows attackers to execute arbitrary code via a crafted RLE file. | 7.8 | More Details |
| CVE-2021-34412 | During the installation process for all versions of the Zoom Client for Meetings for Windows before 5.4.0, it is possible to launch Internet Explorer. If the installer was launched with elevated privileges such as by SCCM this can result in a local privilege escalation. | 7.8 | More Details |
| CVE-2021-0610 | In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. | 7.8 | More Details |
| CVE-2021-39819 | Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious XML file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | 7.8 | More Details |
| CVE-2021-39823 | Adobe svg-native-viewer 8182d14dfad5d1e10f53ed830328d7d9a3cfa96d and earlier versions are affected by a heap buffer overflow vulnerability due to insecure handling of a malicious .svg file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | 7.8 | More Details |
| CVE-2021-23243 | In Oppo's battery application, the third-party SDK provides the function of loading a third-party Provider, which can be used. | 7.8 | More Details |
| CVE-2021-21991 | The vCenter Server contains a local privilege escalation vulnerability due to the way it handles session tokens. A malicious actor with non-administrative user access on vCenter Server host may exploit this issue to escalate privileges to Administrator on the vSphere Client (HTML5) or vCenter Server vSphere Web Client (FLEX/Flash). | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-36297 | SupportAssist Client version 3.8 and 3.9 contains an Untrusted search path vulnerability that allows attackers to load an arbitrary .dll file via .dll planting/hijacking, only by a separate administrative action that is not a default part of the SOSInstallerTool.exe installation for executing arbitrary dll's, | 7.8 | More Details |
| CVE-2021-39825 | Photoshop Elements versions 2021 build 19.0 (20210304.m.156367) (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TTF file. | 7.8 | More Details |
| CVE-2021-34409 | It was discovered that the installation packages of the Zoom Client for Meetings for MacOS (Standard and for IT Admin) installation before version 5.2.0, Zoom Client Plugin for Sharing iPhone/iPad before version 5.2.0, and Zoom Rooms for Conference before version 5.1.0, copy pre- and post- installation shell scripts to a user-writable directory. In the affected products listed below, a malicious actor with local access to a user's machine could use this flaw to potentially run arbitrary system commands in a higher privileged context during the installation process. | 7.8 | More Details |
| CVE-2021-1620 | A vulnerability in the Internet Key Exchange Version 2 (IKEv2) support for the AutoReconnect feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to exhaust the free IP addresses from the assigned local pool. This vulnerability occurs because the code does not release the allocated IP address under certain failure conditions. An attacker could exploit this vulnerability by trying to connect to the device with a non-AnyConnect client. A successful exploit could allow the attacker to exhaust the IP addresses from the assigned local pool, which prevents users from logging in and leads to a denial of service (DoS) condition. | 7.7 | More Details |
| CVE-2021-1623 | A vulnerability in the Simple Network Management Protocol (SNMP) punt handling function of Cisco cBR-8 Converged Broadband Routers could allow an authenticated, remote attacker to overload a device punt path, resulting in a denial of service (DoS) condition. This vulnerability is due to the punt path being overwhelmed by large quantities of SNMP requests. An attacker could exploit this vulnerability by sending a large number of SNMP requests to an affected device. A successful exploit could allow the attacker to overload the device punt path, resulting in a DoS condition. | 7.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34699 | A vulnerability in the TrustSec CLI parser of Cisco IOS and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. This vulnerability is due to an improper interaction between the web UI and the CLI parser. An attacker could exploit this vulnerability by requesting a particular CLI command to be run through the web UI. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition. | 7.7 | More Details |
| CVE-2021-33601 | A vulnerability was discovered in the web user interface of F-Secure Internet Gatekeeper. An authenticated user can modify settings through the web user interface in a way that could lead to an arbitrary code execution on the F-Secure Internet Gatekeeper server. | 7.6 | More Details |
| CVE-2021-36218 | An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncrypt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0 | 7.5 | More Details |
| CVE-2021-3822 | jsoneditor is vulnerable to Inefficient Regular Expression Complexity | 7.5 | More Details |
| CVE-2021-37104 | There is a server-side request forgery vulnerability in HUAWEI P40 versions 10.1.0.118(C00E116R3P3). This vulnerability is due to insufficient validation of parameters while dealing with some messages. A successful exploit could allow the attacker to gain access to certain resource which the attacker are supposed not to do. | 7.5 | More Details |
| CVE-2021-37105 | There is an improper file upload control vulnerability in FusionCompute 6.5.0, 6.5.1 and 8.0.0. Due to the improper verification of file to be uploaded and does not strictly restrict the file access path, attackers may upload malicious files to the device, resulting in the service abnormal. | 7.5 | More Details |
| CVE-2021-3828 | nltk is vulnerable to Inefficient Regular Expression Complexity | 7.5 | More Details |
| CVE-2021-34413 | All versions of the Zoom Plugin for Microsoft Outlook for MacOS before 5.3.52553.0918 contain a Time-of-check Time-of-use (TOC/TOU) vulnerability during the plugin installation process. This could allow a standard user to write their own malicious application to the plugin directory, allowing the malicious application to execute in a privileged context. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-38864 | IBM Security Verify Bridge 1.0.5.0 could allow a user to obtain sensitive information due to improper certificate validation. IBM X-Force ID: 208155. | 7.5 | More Details |
| CVE-2021-40655 | An informtion disclosure issue exists in D-LINK-DIR-605 B2 Firmware Version : 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page | 7.5 | More Details |
| CVE-2021-3820 | inflect is vulnerable to Inefficient Regular Expression Complexity | 7.5 | More Details |
| CVE-2021-40104 | An issue was discovered in Concrete CMS through 8.5.5. There is an SVG sanitizer bypass. | 7.5 | More Details |
| CVE-2021-40103 | An issue was discovered in Concrete CMS through 8.5.5. Path Traversal can lead to Arbitrary File Reading and SSRF. | 7.5 | More Details |
| CVE-2021-41098 | Nokogiri is a Rubygem providing HTML, XML, SAX, and Reader parsers with XPath and CSS selector support. In Nokogiri v1.12.4 and earlier, on JRuby only, the SAX parser resolves external entities by default. Users of Nokogiri on JRuby who parse untrusted documents using any of these classes are affected: Nokogiri::XML::SAX::Parse, Nokogiri::HTML4::SAX::Parser or its alias Nokogiri::HTML::SAX::Parser, Nokogiri::XML::SAX::PushParser, and Nokogiri::HTML4::SAX::PushParser or its alias Nokogiri::HTML::SAX::PushParser. JRuby users should upgrade to Nokogiri v1.12.5 or later to receive a patch for this issue. There are no workarounds available for v1.12.4 or earlier. CRuby users are not affected. | 7.5 | More Details |
| CVE-2021-41096 | Rucky is a USB HID Rubber Ducky Launch Pad for Android. Versions 2.2 and earlier for release builds and versions 425 and earlier for nightly builds suffer from use of a weak cryptographic algorithm (RSA/ECB/PKCS1Padding). The issue will be patched in v2.3 for release builds and 426 onwards for nightly builds. As a workaround, one may disable an advance security feature if not required. | 7.5 | More Details |
| CVE-2021-41753 | A denial-of-service attack in WPA2, and WPA3-SAE authentication methods in D-Link DIR-X1560, v1.04B04, and DIR-X6060, v1.11B04 allows a remote unauthenticated attacker to disconnect a wireless client via sending specific spoofed SAE authentication frames. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41584 | Gradle Enterprise before 2021.1.3 can allow unauthorized viewing of a response (information disclosure of possibly sensitive build/configuration details) via a crafted HTTP request with the X-Gradle-Enterprise-Ajax-Request header. | 7.5 | More Details |
| CVE-2021-41586 | In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially reset the system user password. | 7.5 | More Details |
| CVE-2021-41587 | In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially discover credentials for other resources. | 7.5 | More Details |
| CVE-2021-34570 | Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. | 7.5 | More Details |
| CVE-2021-31606 | furlongm openvpn-monitor through 1.1.3 allows Authorization Bypass to disconnect arbitrary clients. | 7.5 | More Details |
| CVE-2021-31605 | furlongm openvpn-monitor through 1.1.3 allows %0a command injection via the OpenVPN management interface socket. This can shut down the server via signal%20SIGTERM. | 7.5 | More Details |
| CVE-2021-37146 | An infinite loop in Open Robotics ros_comm XMLRPC server in ROS Melodic through 1.4.11 and ROS Noetic through1.15.11 allows remote attackers to cause a Denial of Service in ros_comm via a crafted XMLRPC call. | 7.5 | More Details |
| CVE-2021-34415 | The Zone Controller service in the Zoom On-Premise Meeting Connector Controller before version 4.6.358.20210205 does not verify the cnt field sent in incoming network packets, which leads to exhaustion of resources and system crash. | 7.5 | More Details |
| CVE-2021-22006 | The vCenter Server contains a reverse proxy bypass vulnerability due to the way the endpoints handle the URI. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to access restricted endpoints. | 7.5 | More Details |
| CVE-2021-41104 | ESPHome is a system to control the ESP8266/ESP32. Anyone with web_server enabled and HTTP basic auth configured on version 2021.9.1 or older is vulnerable to an issue in which `web_server` allows over-the-air (OTA) updates without checking user defined basic auth username & password. This issue is patched in version 2021.9.2. As a workaround, one may disable or remove `web_server`. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-23478 | Leo Editor v6.2.1 was discovered to contain a regular expression denial of service (ReDoS) vulnerability in the component plugins/importers/dart.py. | 7.5 | More Details |
| CVE-2020-23469 | gmate v0.12+bionic contains a regular expression denial of service (ReDoS) vulnerability in the gedit3 plugin. | 7.5 | More Details |
| CVE-2021-41011 | LINE client for iOS before 11.15.0 might expose authentication information for a certain service to external entities under certain conditions. This is usually impossible, but in combination with a server-side bug, attackers could get this information. | 7.5 | More Details |
| CVE-2021-22008 | The vCenter Server contains an information disclosure vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by sending a specially crafted json-rpc message to gain access to sensitive information. | 7.5 | More Details |
| CVE-2021-22009 | The vCenter Server contains multiple denial-of-service vulnerabilities in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit these issues to create a denial of service condition due to excessive memory consumption by VAPI service. | 7.5 | More Details |
| CVE-2021-22010 | The vCenter Server contains a denial-of-service vulnerability in VPXD service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to create a denial of service condition due to excessive memory consumption by VPXD service. | 7.5 | More Details |
| CVE-2021-40875 | Improper Access Control in Gurock TestRail versions < 7.2.0.3014 resulted in sensitive information exposure. A threat actor can access the /files.md5 file on the client side of a Gurock TestRail application, disclosing a full list of application files and the corresponding file paths. The corresponding file paths can be tested, and in some cases, result in the disclosure of hardcoded credentials, API keys, or other sensitive data. | 7.5 | More Details |
| CVE-2021-22012 | The vCenter Server contains an information disclosure vulnerability due to an unauthenticated appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. | 7.5 | More Details |
| CVE-2021-22013 | The vCenter Server contains a file path traversal vulnerability leading to information disclosure in the appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-37273 | A Denial of Service issue exists in China Telecom Corporation EPON Tianyi Gateway ZXHN F450(EPON ONU) 3.0. Tianyi Gateway is a hardware terminal of "Optical Modem Smart Router." Attackers can use this vulnerability to restart the device multiple times. | 7.5 | More Details |
| CVE-2021-22019 | The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 5480 on vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to create a denial of service condition. | 7.5 | More Details |
| CVE-2021-36283 | Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. | 7.5 | More Details |
| CVE-2021-41382 | Plastic SCM before 10.0.16.5622 mishandles the WebAdmin server management interface. | 7.5 | More Details |
| CVE-2021-32963 | Null pointer dereference in SuiteLink server while processing commands 0x03/0x10 | 7.5 | More Details |
| CVE-2021-32987 | Null pointer dereference in SuiteLink server while processing command 0x0b | 7.5 | More Details |
| CVE-2021-41381 | Payara Micro Community 5.2021.6 and below allows Directory Traversal. | 7.5 | More Details |
| CVE-2021-32979 | Null pointer dereference in SuiteLink server while processing commands 0x04/0x0a | 7.5 | More Details |
| CVE-2021-32971 | Null pointer dereference in SuiteLink server while processing command 0x07 | 7.5 | More Details |
| CVE-2021-32999 | Improper handling of exceptional conditions in SuiteLink server while processing command 0x01 | 7.5 | More Details |
| CVE-2021-28613 | Adobe Creative Cloud Desktop Application version 5.4 (and earlier) is affected by a file handling vulnerability that could allow an attacker to arbitrarily overwrite a file. Exploitation of this issue requires local access, administrator privileges and user interaction. | 7.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-36134 | Out of bounds write vulnerability in the JPEG parsing code of Netop Vision Pro up to and including 9.7.2 allows an adjacent unauthenticated attacker to write to arbitrary memory potentially leading to a Denial of Service (DoS). | 7.4 | More Details |
| CVE-2021-34740 | A vulnerability in the WLAN Control Protocol (WCP) implementation for Cisco Aironet Access Point (AP) software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect error handling when an affected device receives an unexpected 802.11 frame. An attacker could exploit this vulnerability by sending certain 802.11 frames over the wireless network to an interface on an affected AP. A successful exploit could allow the attacker to cause a packet buffer leak. This could eventually result in buffer allocation failures, which would trigger a reload of the affected device. | 7.4 | More Details |
| CVE-2021-34767 | A vulnerability in IPv6 traffic processing of Cisco IOS XE Wireless Controller Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, adjacent attacker to cause a Layer 2 (L2) loop in a configured VLAN, resulting in a denial of service (DoS) condition for that VLAN. The vulnerability is due to a logic error when processing specific link-local IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that would flow inbound through the wired interface of an affected device. A successful exploit could allow the attacker to cause traffic drops in the affected VLAN, thus triggering the DoS condition. | 7.4 | More Details |
| CVE-2021-34714 | A vulnerability in the Unidirectional Link Detection (UDLD) feature of Cisco FXOS Software, Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload. This vulnerability is due to improper input validation of the UDLD packets. An attacker could exploit this vulnerability by sending specifically crafted UDLD packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: The UDLD feature is disabled by default, and the conditions to exploit this vulnerability are strict. An attacker must have full control of a directly connected device. On Cisco IOS XR devices, the impact is limited to the reload of the UDLD process. | 7.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1621 | A vulnerability in the Layer 2 punt code of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a queue wedge on an interface that receives specific Layer 2 frames, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of certain Layer 2 frames. An attacker could exploit this vulnerability by sending specific Layer 2 frames on the segment the router is connected to. A successful exploit could allow the attacker to cause a queue wedge on the interface, resulting in a DoS condition. | 7.4 | More Details |
| CVE-2021-40981 | ASUS ROG Armoury Crate Lite before 4.2.10 allows local users to gain privileges by placing a Trojan horse file in the publicly writable %PROGRAMDATA%\ASUS\GamingCenterLib directory. | 7.3 | More Details |
| CVE-2021-37106 | There is a command injection vulnerability in CMA service module of FusionCompute 6.3.0, 6.3.1, 6.5.0 and 8.0.0 when processing the default certificate file. The software constructs part of a command using external special input from users, but the software does not sufficiently validate the user input. Successful exploit could allow the attacker to inject certain commands to the system. | 7.2 | More Details |
| CVE-2021-22014 | The vCenter Server contains an authenticated code execution vulnerability in VAMI (Virtual Appliance Management Infrastructure). An authenticated VAMI user with network access to port 5480 on vCenter Server may exploit this issue to execute code on the underlying operating system that hosts vCenter Server. | 7.2 | More Details |
| CVE-2021-34349 | A command injection vulnerability has been reported to affect QNAP device running QVR. If exploited, this vulnerability could allow remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.5 build 20210803 and later | 7.2 | More Details |
| CVE-2021-40099 | An issue was discovered in Concrete CMS through 8.5.5. Fetching the update json scheme over HTTP leads to remote code execution. | 7.2 | More Details |
| CVE-2021-34414 | The network proxy page on the web portal for the Zoom on-premise Meeting Connector Controller before version 4.6.348.20201217, Zoom on-premise Meeting Connector MMR before version 4.6.348.20201217, Zoom on-premise Recording Connector before version 3.8.42.20200905, Zoom on-premise Virtual Room Connector before version 4.4.6620.20201110, and Zoom on-premise Virtual Room Connector Load Balancer before version 2.5.5495.20210326 fails to validate input sent in requests to update the network proxy configuration, which could lead to remote command injection on the on-premise image by a web portal administrator. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-20692 | GilaCMS v1.11.4 was discovered to contain a SQL injection vulnerability via the $_GET parameter in /src/core/controllers/cm.php. | 7.2 | More Details |
| CVE-2021-22948 | Vulnerability in the generation of session IDs in revive-adserver < 5.3.0, based on the cryptographically insecure uniqid() PHP function. Under some circumstances, an attacker could theoretically be able to brute force session IDs in order to take over a specific account. | 7.1 | More Details |
| CVE-2016-6556 | OpenNMS version 18.0.1 and prior are vulnerable to a stored XSS issue due to insufficient filtering of SNMP agent supplied data. By creating a malicious SNMP 'sysName' or 'sysContact' response, an attacker can store an XSS payload which will trigger when a user of the web UI views the data. This issue was fixed in version 18.0.2, released on September 20, 2016. | 7.1 | More Details |
| CVE-2020-23267 | An issue was discovered in gpac 0.8.0. The gf_hinter_track_process function in isom_hinter_track_process.c has a heap-based buffer overflow which can lead to a denial of service (DOS) via a crafted media file | 7.1 | More Details |
| CVE-2016-6555 | OpenNMS version 18.0.1 and prior are vulnerable to a stored XSS issue due to insufficient filtering of SNMP trap supplied data. By creating a malicious SNMP trap, an attacker can store an XSS payload which will trigger when a user of the web UI views the events list page. This issue was fixed in version 18.0.2, released on September 20, 2016. | 7.1 | More Details |
| CVE-2021-3583 | A flaw was found in Ansible, where a user's controller is vulnerable to template injection. This issue can occur through facts used in the template if the user is trying to put templates in multi-line YAML strings and the facts being handled do not routinely include special template characters. This flaw allows attackers to perform command injection, which discloses sensitive information. The highest threat from this vulnerability is to confidentiality and integrity. | 7.1 | More Details |
| CVE-2021-36874 | Authenticated Insecure Direct Object References (IDOR) vulnerability in WordPress uListing plugin (versions <= 2.0.5). | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-36286 | Dell SupportAssist Client Consumer versions 3.9.13.0 and any versions prior to 3.9.13.0 contain an arbitrary file deletion vulnerability that can be exploited by using the Windows feature of NTFS called Symbolic links. Symbolic links can be created by any(non-privileged) user under some object directories, but by themselves are not sufficient to successfully escalate privileges. However, combining them with a different object, such as the NTFS junction point allows for the exploitation. Support assist clean files functionality do not distinguish junction points from the physical folder and proceeds to clean the target of the junction that allows nonprivileged users to create junction points and delete arbitrary files on the system which can be accessed only by the admin. | 7.1 | More Details |
| CVE-2021-41617 | sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user. | 7.0 | More Details |
| CVE-2021-36841 | Authenticated Stored Cross-Site Scripting (XSS) vulnerability in YITH Maintenance Mode (WordPress plugin) versions <= 1.3.7, vulnerable parameter &yith_maintenance_newsletter_submit_label. Possible even when unfiltered HTML is disallowed by WordPress configuration. | 6.9 | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2021-36845 | Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities in YITH Maintenance Mode (WordPress plugin) versions <= 1.3.8, there are 46 vulnerable parameters that were missed by the vendor while patching the 1.3.7 version to 1.3.8. Vulnerable parameters: 1 - "Newsletter" tab, &yith_maintenance_newsletter_submit_label parameter: payload should start with a single quote (') symbol to break the context, i.e.: NOTIFY ME' autofocus onfocus=alert(/Visse/);// v=' - this payload will be auto triggered while admin visits this page/tab. 2 - "General" tab issues, vulnerable parameters: &yith_maintenance_message, &yith_maintenance_custom_style, &yith_maintenance_mascotte, &yith_maintenance_title_font[size], &yith_maintenance_title_font[family], &yith_maintenance_title_font[color], &yith_maintenance_paragraph_font[size], &yith_maintenance_paragraph_font[family], &yith_maintenance_paragraph_font[color], &yith_maintenance_border_top. 3 - "Background" tab issues, vulnerable parameters: &yith_maintenance_background_image, &yith_maintenance_background_color. 4 - "Logo" tab issues, vulnerable parameters: &yith_maintenance_logo_image, &yith_maintenance_logo_tagline, &yith_maintenance_logo_tagline_font[size], &yith_maintenance_logo_tagline_font[family], &yith_maintenance_logo_tagline_font[color]. 5 - "Newsletter" tab issues, vulnerable parameters: &yith_maintenance_newsletter_email_font[size], &yith_maintenance_newsletter_email_font[family], &yith_maintenance_newsletter_email_font[color], &yith_maintenance_newsletter_submit_font[size], &yith_maintenance_newsletter_submit_font[family], &yith_maintenance_newsletter_submit_font[color], &yith_maintenance_newsletter_submit_background, &yith_maintenance_newsletter_submit_background_hover, &yith_maintenance_newsletter_title, &yith_maintenance_newsletter_action, &yith_maintenance_newsletter_email_label, &yith_maintenance_newsletter_email_name, &yith_maintenance_newsletter_submit_label, &yith_maintenance_newsletter_hidden_fields. 6 - "Socials" tab issues, vulnerable parameters: &yith_maintenance_socials_facebook, &yith_maintenance_socials_twitter, &yith_maintenance_socials_gplus, &yith_maintenance_socials_youtube, &yith_maintenance_socials_rss, &yith_maintenance_socials_skype, &yith_maintenance_socials_email, &yith_maintenance_socials_behance, &yith_maintenance_socials_dribble, &yith_maintenance_socials_flickr, &yith_maintenance_socials_instagram, &yith_maintenance_socials_pinterest, &yith_maintenance_socials_tumblr, | 6.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| | &yith_maintenance_socials_linkedin. | | |
| CVE-2021-34703 | A vulnerability in the Link Layer Discovery Protocol (LLDP) message parser of Cisco IOS Software and Cisco IOS XE Software could allow an attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper initialization of a buffer. An attacker could exploit this vulnerability via any of the following methods: An authenticated, remote attacker could access the LLDP neighbor table via either the CLI or SNMP while the device is in a specific state. An unauthenticated, adjacent attacker could corrupt the LLDP neighbor table by injecting specific LLDP frames into the network and then waiting for an administrator of the device or a network management system (NMS) managing the device to retrieve the LLDP neighbor table of the device via either the CLI or SNMP. An authenticated, adjacent attacker with SNMP read-only credentials or low privileges on the device CLI could corrupt the LLDP neighbor table by injecting specific LLDP frames into the network and then accessing the LLDP neighbor table via either the CLI or SNMP. A successful exploit could allow the attacker to cause the affected device to crash, resulting in a reload of the device. | 6.8 | More Details |
| CVE-2021-21569 | Dell NetWorker, versions 18.x and 19.x contain a Path traversal vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information. | 6.8 | More Details |
| CVE-2021-21570 | Dell NetWorker, versions 18.x and 19.x contain an Information disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information. | 6.8 | More Details |
| CVE-2021-34729 | A vulnerability in the CLI of Cisco IOS XE SD-WAN Software and Cisco IOS XE Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges on an affected device. This vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input in the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands with elevated privileges on the underlying operating system. An attacker would need valid user credentials to exploit this vulnerability. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34726 | A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands to be executed with root-level privileges on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation on certain CLI commands. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the CLI. The attacker must be authenticated as an administrative user to execute the affected commands. A successful exploit could allow the attacker to execute commands with root-level privileges. | 6.7 | More Details |
| CVE-2021-34725 | A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands to be executed with root-level 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 an affected device and submitting crafted input to the CLI. The attacker must be authenticated as an administrative user to execute the affected commands. A successful exploit could allow the attacker to execute commands with root-level privileges. | 6.7 | More Details |
| CVE-2021-34723 | A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. | 6.7 | More Details |
| CVE-2021-36823 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cusmin AGCA - Absolutely Glamorous Custom Admin (WordPress plugin) allows Stored XSS.This issue affects AGCA - Absolutely Glamorous Custom Admin (WordPress plugin): from n/a through 6.8. | 6.6 | More Details |
| CVE-2021-41329 | Datalust Seq before 2021.2.6259 allows users (with view filters applied to their accounts) to see query results not constrained by their view filter. This information exposure, caused by an internal cache key collision, occurs when the user's view filter includes an array or IN clause, and when another user has recently executed an identical query differing only by the array elements. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21992 | The vCenter Server contains a denial-of-service vulnerability due to improper XML entity parsing. A malicious actor with non-administrative user access to the vCenter Server vSphere Client (HTML5) or vCenter Server vSphere Web Client (FLEX/Flash) may exploit this issue to create a denial-of-service condition on the vCenter Server host. | 6.5 | More Details |
| CVE-2021-31604 | furlongm openvpn-monitor through 1.1.3 allows CSRF to disconnect an arbitrary client. | 6.5 | More Details |
| CVE-2021-1589 | A vulnerability in the disaster recovery feature of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain unauthorized access to user credentials. This vulnerability exists because access to API endpoints is not properly restricted. An attacker could exploit this vulnerability by sending a request to an API endpoint. A successful exploit could allow the attacker to gain unauthorized access to administrative credentials that could be used in further attacks. | 6.5 | More Details |
| CVE-2021-41385 | The third party intelligence connector in Securonix SNYPR 6.3.1 Build 184295_0302 allows an authenticated user to obtain access to server configuration details via SSRF. | 6.5 | More Details |
| CVE-2021-40654 | An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page | 6.5 | More Details |
| CVE-2021-36749 | In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource. This issue was previously mentioned as being fixed in 0.21.0 as per CVE-2021-26920 but was not fixed in 0.21.0 or 0.21.1. | 6.5 | More Details |
| CVE-2021-20035 | Improper neutralization of special elements in the SMA100 management interface allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user which potentially leads to DoS. | 6.5 | More Details |
| CVE-2021-22950 | Concrete CMS prior to 8.5.6 had a CSFR vulnerability allowing attachments to comments in the conversation section to be deleted.Credit for discovery: "Solar Security Research Team" | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-20691 | An issue in Monstra CMS v3.0.4 allows attackers to execute arbitrary web scripts or HTML via bypassing the file extension filter and uploading crafted HTML files. | 6.5 | More Details |
| CVE-2021-39827 | Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary file write vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to write an arbitrary file to the system. User interaction is required before product installation to abuse this vulnerability. | 6.5 | More Details |
| CVE-2021-34647 | The Ninja Forms WordPress plugin is vulnerable to sensitive information disclosure via the bulk_export_submissions function found in the ~/includes/Routes/Submissions.php file, in versions up to and including 3.5.7. This allows authenticated attackers to export all Ninja Forms submissions data via the /ninja-forms-submissions/export REST API which can include personally identifiable information. | 6.5 | More Details |
| CVE-2021-21993 | The vCenter Server contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in vCenter Server Content Library. An authorised user with access to content library may exploit this issue by sending a POST request to vCenter Server leading to information disclosure. | 6.5 | More Details |
| CVE-2021-29816 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 204341. | 6.5 | More Details |
| CVE-2021-24652 | The PostX – Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 performs incorrect checks before allowing any logged in user to perform some ajax based requests, allowing any user to modify, delete or add ultp_options values. | 6.5 | More Details |
| CVE-2021-26587 | A potential DOM-based Cross Site Scripting security vulnerability has been identified in HPE StoreOnce. The vulnerability could be remotely exploited to cause an elevation of privilege leading to partial impact to confidentiality, availability, and integrity. HPE has made the following software update - HPE StoreOnce 4.3.0, to resolve the vulnerability in HPE StoreOnce. | 6.5 | More Details |
| CVE-2021-41583 | vpn-user-portal (aka eduVPN or Let's Connect!) before 2.3.14, as packaged for Debian 10, Debian 11, and Fedora, allows remote authenticated users to obtain OS filesystem access, because of the interaction of QR codes with an exec that uses the -r option. This can be leveraged to obtain additional VPN access. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-40712 | Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper input validation vulnerability via the path parameter. An authenticated attacker can send a malformed POST request to achieve server-side denial of service. | 6.5 | More Details |
| CVE-2021-22018 | The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files. | 6.5 | More Details |
| CVE-2021-22272 | The vulnerability origins in the commissioning process where an attacker of the ControlTouch can enter a serial number in a specific way to transfer the device virtually into her/his my.busch-jaeger.de or mybuildings.abb.com profile. A successful attacker can observe and control a ControlTouch remotely under very specific circumstances. The issue is fixed in the cloud side of the system. No firmware update is needed for customer products. If a user wants to understand if (s)he is affected, please read the advisory. This issue affects: ABB and Busch-Jaeger, ControlTouch | 6.5 | More Details |
| CVE-2021-34648 | The Ninja Forms WordPress plugin is vulnerable to arbitrary email sending via the trigger_email_action function found in the ~/includes/Routes/Submissions.php file, in versions up to and including 3.5.7. This allows authenticated attackers to send arbitrary emails from the affected server via the /ninja-forms-submissions/email-action REST API which can be used to socially engineer victims. | 6.4 | More Details |
| CVE-2021-40109 | A SSRF issue was discovered in Concrete CMS through 8.5.5. Users can access forbidden files on their local network. A user with permissions to upload files from external sites can upload a URL that redirects to an internal resource of any file type. The redirect is followed and loads the contents of the file from the redirected-to server. Files of disallowed types can be uploaded. | 6.4 | More Details |
| CVE-2021-40105 | An issue was discovered in Concrete CMS through 8.5.5. There is XSS via Markdown Comments. | 6.1 | More Details |
| CVE-2021-40106 | An issue was discovered in Concrete CMS through 8.5.5. There is unauthenticated stored XSS in blog comments via the website field. | 6.1 | More Details |
| CVE-2021-24632 | The Recipe Card Blocks by WPZOOM WordPress plugin before 2.8.1 does not escape the message parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting issue | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-20125 | EARCLINK ESPCMS-P8 contains a cross-site scripting (XSS) vulnerability in espcms_web\espcms_load.php. | 6.1 | More Details |
| CVE-2021-30086 | Cross Site Scripting (XSS) vulnerability exists in KindEditor (Chinese versions) 4.1.12, which can be exploited by an attacker to obtain user cookie information. | 6.1 | More Details |
| CVE-2021-39246 | Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network). | 6.1 | More Details |
| CVE-2021-22016 | The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link. | 6.1 | More Details |
| CVE-2021-40714 | Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability via the accesskey parameter. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser | 6.1 | More Details |
| CVE-2021-41318 | In Progress WhatsUp Gold prior to version 21.1.0, an application endpoint failed to adequately sanitize malicious input. which could allow an unauthenticated attacker to execute arbitrary code in a victim's browser. | 6.1 | More Details |
| CVE-2021-23054 | On version 16.x before 16.1.0, 15.1.x before 15.1.4, 14.1.x before 14.1.4.4, and all versions of 13.1.x, 12.1.x, and 11.6.x, a reflected cross-site scripting (XSS) vulnerability exists in the resource information page for authenticated users when a full webtop is configured on the BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 6.1 | More Details |
| CVE-2021-3824 | OpenVPN Access Server 2.9.0 through 2.9.4 allow remote attackers to inject arbitrary web script or HTML via the web login page URL. | 6.1 | More Details |
| CVE-2021-22276 | The vulnerability allows a successful attacker to bypass the integrity check of FW uploaded to the free@home System Access Point. | 6.1 | More Details |
| CVE-2020-20508 | Shopkit v2.7 contains a reflective cross-site scripting (XSS) vulnerability in the /account/register component, which allows attackers to hijack user credentials via a crafted payload in the E-Mail text field. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-37267 | Cross Site Scripting (XSS) vulnerability exists in all versions of KindEditor, which can be exploited by an attacker to obtain user cookie information. | 6.1 | More Details |
| CVE-2021-34724 | A vulnerability in the Cisco IOS XE SD-WAN Software CLI could allow an authenticated, local attacker to elevate privileges and execute arbitrary code on the underlying operating system as the root user. An attacker must be authenticated on an affected device as a PRIV15 user. This vulnerability is due to insufficient file system protection and the presence of a sensitive file in the bootflash directory on an affected device. An attacker could exploit this vulnerability by overwriting an installer file stored in the bootflash directory with arbitrary commands that can be executed with root-level privileges. A successful exploit could allow the attacker to read and write changes to the configuration database on the affected device. | 6.0 | More Details |
| CVE-2021-40713 | Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper certificate validation vulnerability in the cold storage component. If an attacker can achieve a man in the middle when the cold server establishes a new certificate, they would be able to harvest sensitive information. | 5.9 | More Details |
| CVE-2021-38153 | Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerable to timing attacks that make brute force attacks for such credentials more likely to be successful. Users should upgrade to 2.8.1 or higher, or 3.0.0 or higher where this vulnerability has been fixed. The affected versions include Apache Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, and 2.8.0. | 5.9 | More Details |
| CVE-2021-39339 | The Telefication WordPress plugin is vulnerable to Open Proxy and Server-Side Request Forgery via the ~/bypass.php file due to a user-supplied URL request value that gets called by a curl requests. This affects versions up to, and including, 1.8.0. | 5.8 | More Details |
| CVE-2021-34697 | A vulnerability in the Protection Against Distributed Denial of Service Attacks feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct denial of service (DoS) attacks to or through the affected device. This vulnerability is due to incorrect programming of the half-opened connections limit, TCP SYN flood limit, or TCP SYN cookie features when the features are configured in vulnerable releases of Cisco IOS XE Software. An attacker could exploit this vulnerability by attempting to flood traffic to or through the affected device. A successful exploit could allow the attacker to initiate a DoS attack to or through an affected device. | 5.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34696 | A vulnerability in the access control list (ACL) programming of Cisco ASR 900 and ASR 920 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to incorrect programming of hardware when an ACL is configured using a method other than the configuration CLI. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device. | 5.8 | More Details |
| CVE-2021-1625 | A vulnerability in the Zone-Based Policy Firewall feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent the Zone-Based Policy Firewall from correctly classifying traffic. This vulnerability exists because ICMP and UDP responder-to-initiator flows are not inspected when the Zone-Based Policy Firewall has either Unified Threat Defense (UTD) or Application Quality of Experience (AppQoE) configured. An attacker could exploit this vulnerability by attempting to send UDP or ICMP flows through the network. A successful exploit could allow the attacker to inject traffic through the Zone-Based Policy Firewall, resulting in traffic being dropped because it is incorrectly classified or in incorrect reporting figures being produced by high-speed logging (HSL). | 5.8 | More Details |
| CVE-2021-39828 | Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User interaction is required before product installation to abuse this vulnerability. | 5.8 | More Details |
| CVE-2021-36284 | Dell BIOS contains an Improper Restriction of Excessive Authentication Attempts vulnerability. A local authenticated malicious administrator could exploit this vulnerability to bypass excessive admin password attempt mitigations in order to carry out a brute force attack. | 5.7 | More Details |
| CVE-2021-36285 | Dell BIOS contains an Improper Restriction of Excessive Authentication Attempts vulnerability. A local authenticated malicious administrator could exploit this vulnerability to bypass excessive NVMe password attempt mitigations in order to carry out a brute force attack. | 5.7 | More Details |
| CVE-2021-31836 | Improper privilege management vulnerability in maconfig for McAfee Agent for Windows prior to 5.7.4 allows a local user to gain access to sensitive information. The utility was able to be run from any location on the file system and by a low privileged user. | 5.6 | More Details |
| CVE-2021-29365 | Irfanview 4.57 is affected by an infinite loop when processing a crafted BMP file in the EFFECTS!AutoCrop_W component. This can cause a denial of service (DOS). | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-29358 | A buffer overflow vulnerability in FORMATS!ReadPVR_W+0xfa of Irfanview 4.57 allows attackers to cause a denial of service (DOS) via a crafted PVR file. | 5.5 | More Details |
| CVE-2020-23266 | An issue was discovered in gpac 0.8.0. The OD_ReadUTF8String function in odf_code.c has a heap-based buffer overflow which can lead to a denial of service (DOS) via a crafted media file. | 5.5 | More Details |
| CVE-2021-21742 | There is an information leak vulnerability in the message service app of a ZTE mobile phone. Due to improper parameter settings, attackers could use this vulnerability to obtain some sensitive information of users by accessing specific pages. | 5.5 | More Details |
| CVE-2021-36872 | Authenticated Persistent Cross-Site Scripting (XSS) vulnerability in WordPress Popular Posts plugin (versions <= 5.3.3). Vulnerable at &widget-wpp[2][post_type]. | 5.5 | More Details |
| CVE-2021-29904 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 207610. | 5.5 | More Details |
| CVE-2021-38863 | IBM Security Verify Bridge 1.0.5.0 stores user credentials in plain clear text which can be read by a locally authenticated user. IBM X-Force ID: 208154. | 5.5 | More Details |
| CVE-2021-0421 | In memory management driver, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381235. | 5.5 | More Details |
| CVE-2021-36873 | Authenticated Persistent Cross-Site Scripting (XSS) vulnerability in WordPress iQ Block Country plugin (versions <= 1.2.11). Vulnerable parameter: &blockcountry_blockmessage. | 5.5 | More Details |
| CVE-2021-41581 | x509_constraints_parse_mailbox in lib/libcrypto/x509/x509_constraints.c in LibreSSL through 3.4.0 has a stack-based buffer over-read. When the input exceeds DOMAIN_PART_MAX_LEN, the buffer lacks '\0' termination. | 5.5 | More Details |
| CVE-2021-0423 | In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-0424 | In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. | 5.5 | More Details |
| CVE-2021-0425 | In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. | 5.5 | More Details |
| CVE-2021-20435 | IBM Security Verify Bridge 1.0.5.0 does not properly validate a certificate which could allow a local attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 196355. | 5.5 | More Details |
| CVE-2021-0422 | In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. | 5.5 | More Details |
| CVE-2021-22020 | The vCenter Server contains a denial-of-service vulnerability in the Analytics service. Successful exploitation of this issue may allow an attacker to create a denial-of-service condition on vCenter Server. | 5.5 | More Details |
| CVE-2021-22007 | The vCenter Server contains a local information disclosure vulnerability in the Analytics service. An authenticated user with non-administrative privilege may exploit this issue to gain access to sensitive information. | 5.5 | More Details |
| CVE-2021-1612 | A vulnerability in the Cisco IOS XE SD-WAN Software CLI could allow an authenticated, local attacker to overwrite arbitrary files on the local system. This vulnerability is due to improper access controls on files within the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system. A successful exploit could allow the attacker to overwrite arbitrary files on an affected device. | 5.5 | More Details |
| CVE-2020-23269 | An issue was discovered in gpac 0.8.0. The stbl_GetSampleSize function in isomedia/stbl_read.c has a heap-based buffer overflow which can lead to a denial of service (DOS) via a crafted media file. | 5.5 | More Details |
| CVE-2021-1546 | A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-23273 | Heap-buffer overflow in the randomize_iparp function in edit_packet.c. of Tcpreplay v4.3.2 allows attackers to cause a denial of service (DOS) via a crafted pcap. | 5.5 | More Details |
| CVE-2021-22953 | A CSRF in Concrete CMS version 8.5.5 and below allows an attacker to clone topics which can lead to UI inconvenience, and exhaustion of disk space.Credit for discovery: "Solar Security Research Team" | 5.4 | More Details |
| CVE-2020-20696 | A cross-site scripting (XSS) vulnerability in /admin/content/post of GilaCMS v1.11.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Tags field. | 5.4 | More Details |
| CVE-2021-38870 | IBM Aspera Cloud is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 208343. | 5.4 | More Details |
| CVE-2021-29905 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 207616. | 5.4 | More Details |
| CVE-2021-29833 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204825. | 5.4 | More Details |
| CVE-2021-29815 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204340. | 5.4 | More Details |
| CVE-2021-29814 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204334. | 5.4 | More Details |
| CVE-2021-29813 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204331. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-20695 | A stored cross-site scripting (XSS) vulnerability in GilaCMS v1.11.4 allows attackers to execute arbitrary web scripts or HTML via a crafted SVG file. | 5.4 | More Details |
| CVE-2021-29810 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204279. | 5.4 | More Details |
| CVE-2021-33600 | A denial-of-service (DoS) vulnerability was discovered in the web user interface of F-Secure Internet Gatekeeper. The vulnerability occurs because of an attacker can trigger assertion via malformed HTTP packet to web interface. An unauthenticated attacker could exploit this vulnerability by sending a large username parameter. A successful exploitation could lead to a denial-of-service of the product. | 5.4 | More Details |
| CVE-2021-29812 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204330. | 5.4 | More Details |
| CVE-2021-22949 | A CSRF in Concrete CMS version 8.5.5 and below allows an attacker to duplicate files which can lead to UI inconvenience, and exhaustion of disk space.Credit for discovery: "Solar Security CMS Research Team" | 5.4 | More Details |
| CVE-2020-23481 | CMS Made Simple 2.2.14 was discovered to contain a cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Field Definition text field. | 5.4 | More Details |
| CVE-2021-29800 | IBM Tivoli Netcool/OMNIbus_GUI and IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 5.4 | More Details |
| CVE-2021-20484 | IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 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: 197666. | 5.4 | More Details |
| CVE-2021-37271 | Cross Site Scripting (XSS) vulnerability exists in UEditor v1.4.3.3, which can be exploited by an attacker to obtain user cookie information. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34712 | A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct cypher query language injection attacks on an affected system. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface of an affected system. A successful exploit could allow the attacker to obtain sensitive information. | 5.4 | More Details |
| CVE-2021-38877 | IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 208405. | 5.4 | More Details |
| CVE-2021-29832 | IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204824. | 5.4 | More Details |
| CVE-2021-3830 | btcpayserver is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 5.4 | More Details |
| CVE-2021-24660 | The PostX – Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10, with Saved Templates Addon enabled, allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the plugin's shortcode. | 5.4 | More Details |
| CVE-2021-24643 | The WP Map Block WordPress plugin before 1.2.3 does not escape some attributes of the WP Map Block, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2021-24634 | The Recipe Card Blocks by WPZOOM WordPress plugin before 2.8.3 does not properly sanitise or escape some of the properties of the Recipe Card Block (such as ingredientsLayout, iconSet, steps, ingredients, recipeTitle, or settings), which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2021-40310 | OpenSIS Community Edition version 8.0 is affected by a cross-site scripting (XSS) vulnerability in the TakeAttendance.php via the cp_id_miss_attn parameter. | 5.4 | More Details |
| CVE-2021-24659 | The PostX – Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the plugin's block. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3799 | grav-plugin-admin is vulnerable to Improper Restriction of Rendered UI Layers or Frames | 5.4 | More Details |
| CVE-2021-24670 | The CoolClock WordPress plugin before 4.3.5 does not escape some shortcode attributes, allowing users with a role as low as Contributor toperform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2021-40100 | An issue was discovered in Concrete CMS through 8.5.5. Stored XSS can occur in Conversations when the Active Conversation Editor is set to Rich Text. | 5.4 | More Details |
| CVE-2021-40711 | Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a stored XSS vulnerability when creating Content Fragments. An authenticated attacker can send a malformed POST request to achieve arbitrary code execution. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. | 5.4 | More Details |
| CVE-2021-36876 | Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in WordPress uListing plugin (versions <= 2.0.5) as it lacks CSRF checks on plugin administration pages. | 5.4 | More Details |
| CVE-2021-24671 | The MX Time Zone Clocks WordPress plugin before 3.4.1 does not escape the time_zone attribute of the mxmtzc_time_zone_clocks shortcode, allowing users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2021-36165 | RICON Industrial Cellular Router S9922L 16.10.3(3794) is affected by cleartext storage of sensitive information and sends username and password as base64. | 5.3 | More Details |
| CVE-2020-24327 | Server Side Request Forgery (SSRF) vulnerability exists in Discourse 2.3.2 and 2.6 via the email function. When writing an email in an editor, you can upload pictures of remote websites. | 5.3 | More Details |
| CVE-2021-41580 | The passport-oauth2 package before 1.6.1 for Node.js mishandles the error condition of failure to obtain an access token. This is exploitable in certain use cases where an OAuth identity provider uses an HTTP 200 status code for authentication-failure error reports, and an application grants authorization upon simply receiving the access token (i.e., does not try to use the token). NOTE: the passport-oauth2 vendor does not consider this a passport-oauth2 vulnerability | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22017 | Rhttproxy as used in vCenter Server contains a vulnerability due to improper implementation of URI normalization. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to bypass proxy leading to internal endpoints being accessed. | 5.3 | More Details |
| CVE-2021-22011 | vCenter Server contains an unauthenticated API endpoint vulnerability in vCenter Server Content Library. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to perform unauthenticated VM network setting manipulation. | 5.3 | More Details |
| CVE-2021-31923 | Ping Identity PingAccess before 5.3.3 allows HTTP request smuggling via header manipulation. | 5.3 | More Details |
| CVE-2021-40349 | e7d Speed Test (aka speedtest) 0.5.3 allows a path-traversal attack that results in information disclosure via the "GET /.." substring. | 5.3 | More Details |
| CVE-2021-34705 | A vulnerability in the Voice Telephony Service Provider (VTSP) service of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass configured destination patterns and dial arbitrary numbers. This vulnerability is due to insufficient validation of dial strings at Foreign Exchange Office (FXO) interfaces. An attacker could exploit this vulnerability by sending a malformed dial string to an affected device via either the ISDN protocol or SIP. A successful exploit could allow the attacker to conduct toll fraud, resulting in unexpected financial impact to affected customers. | 5.3 | More Details |
| CVE-2021-3818 | grav is vulnerable to Reliance on Cookies without Validation and Integrity Checking | 5.3 | More Details |
| CVE-2021-0660 | In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145. | 4.9 | More Details |
| CVE-2021-22535 | Unauthorized information security disclosure vulnerability on Micro Focus Directory and Resource Administrator (DRA) product, affecting all DRA versions prior to 10.1 Patch 1. The vulnerability could lead to unauthorized information disclosure. | 4.9 | More Details |
| CVE-2021-36875 | Authenticated Reflected Cross-Site Scripting (XSS) vulnerability in WordPress uListing plugin (versions <= 2.0.5). Vulnerable parameters: &filter[id], &filter[user], &filter[expired_date], &filter[created_date], &filter[updated_date]. | 4.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-24610 | The TranslatePress WordPress plugin before 2.0.9 does not implement a proper sanitisation on the translated strings. The 'trp_sanitize_string' function only removes script tag with a regex, still allowing other HTML tags and attributes to execute javascript, which could lead to authenticated Stored Cross-Site Scripting issues. | 4.8 | More Details |
| CVE-2021-39404 | MaianAffiliate v1.0 allows an authenticated administrative user to save an XSS to the database. | 4.8 | More Details |
| CVE-2020-19949 | A cross-site scripting (XSS) vulnerability in the /link/add.html component of YzmCMS v5.3 allows attackers to execute arbitrary web scripts or HTML. | 4.8 | More Details |
| CVE-2021-24569 | The Cookie Notice & Compliance for GDPR / CCPA WordPress plugin before 2.1.2 does not escape the value of its Button Text setting when outputting it in an attribute in the frontend, allowing high privilege users such as admin to perform Cross-Site Scripting even when the unfiltered_html capability is disallowed. | 4.8 | More Details |
| CVE-2020-19950 | A cross-site scripting (XSS) vulnerability in the /banner/add.html component of YzmCMS v5.3 allows attackers to execute arbitrary web scripts or HTML. | 4.8 | More Details |
| CVE-2021-1616 | A vulnerability in the H.323 application level gateway (ALG) used by the Network Address Translation (NAT) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass the ALG. This vulnerability is due to insufficient data validation of traffic that is traversing the ALG. An attacker could exploit this vulnerability by sending crafted traffic to a targeted device. A successful exploit could allow the attacker to bypass the ALG and open connections that should not be allowed to a remote device located behind the ALG. Note: This vulnerability has been publicly discussed as NAT Slipstreaming. | 4.7 | More Details |
| CVE-2021-37786 | Certain Federal Office of Information Technology Systems and Telecommunication FOITT products are affected by improper handling of exceptional conditions. This affects COVID Certificate App IOS 2.2.0 and below affected, patch in progress and COVID Certificate Check App IOS 2.2.0 and below affected, patch in progress. A denial of service (physically proximate) could be caused by scanning a crafted QR code. | 4.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41106 | JWT is a library to work with JSON Web Token and JSON Web Signature. Prior to versions 3.4.6, 4.0.4, and 4.1.5, users of HMAC-based algorithms (HS256, HS384, and HS512) combined with `Lcobucci\JWT\Signer\Key\LocalFileReference` as key are having their tokens issued/validated using the file path as hashing key - instead of the contents. The HMAC hashing functions take any string as input and, since users can issue and validate tokens, users are lead to believe that everything works properly. Versions 3.4.6, 4.0.4, and 4.1.5 have been patched to always load the file contents, deprecated the `Lcobucci\JWT\Signer\Key\LocalFileReference`, and suggest `Lcobucci\JWT\Signer\Key\InMemory` as the alternative. As a workaround, use `Lcobucci\JWT\Signer\Key\InMemory` instead of `Lcobucci\JWT\Signer\Key\LocalFileReference` to create the instances of one's keys. | 4.4 | More Details |
| CVE-2021-20434 | IBM Security Verify Bridge 1.0.5.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 196346. | 4.4 | More Details |
| CVE-2021-20317 | A flaw was found in the Linux kernel. A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c. This flaw allows a local attacker with special user privileges to cause a denial of service, slowing and eventually stopping the system while running OSP. | 4.4 | More Details |
| CVE-2021-20563 | IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 could allow a remote authenciated user to obtain sensitive information. By sending a specially crafted request, the user could disclose a valid filepath on the server which could be used in further attacks against the system. IBM X-Force ID: 199234. | 4.3 | More Details |
| CVE-2021-24661 | The PostX – Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10, with Saved Templates Addon enabled, allows users with Contributor roles or higher to read password-protected or private post contents the user is otherwise unable to read, given the post ID. | 4.3 | More Details |
| CVE-2021-36878 | Cross-Site Request Forgery (CSRF) vulnerability in WordPress uListing plugin (versions <= 2.0.5) makes it possible for attackers to update settings. | 4.3 | More Details |
| CVE-2021-24633 | The Countdown Block WordPress plugin before 1.1.2 does not have authorisation in the eb_write_block_css AJAX action, which allows any authenticated user, such as Subscriber, to modify post contents displayed to users. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22868 | A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This vulnerability was reported via the GitHub Bug Bounty program. This is the result of an incomplete fix for CVE-2021-22867. | 4.3 | More Details |
| CVE-2021-20485 | IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 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: 197667. | 4.3 | More Details |
| CVE-2021-36877 | Cross-Site Request Forgery (CSRF) vulnerability in WordPress uListing plugin (versions <= 2.0.5) makes it possible for attackers to modify user roles. | 4.3 | More Details |
| CVE-2020-4941 | IBM Edge 4.2 could reveal sensitive version information about the server from error pages that could aid an attacker in further attacks against the system. IBM X-Force ID: 191941. | 4.3 | More Details |
| CVE-2021-41095 | Discourse is an open source discussion platform. There is a cross-site scripting (XSS) vulnerability in versions 2.7.7 and earlier of the `stable` branch, versions 2.8.0.beta6 and earlier of the `beta` branch, and versions 2.8.0.beta6 and earlier of the `tests-passed` branch. Rendering of some error messages that contain user input can be susceptible to XSS attacks. This vulnerability only affects sites which have blocked watched words that contain HTML tags, modified or disabled Discourse's default Content Security Policy. This issue is patched in the latest `stable`, `beta` and `tests-passed` versions of Discourse. As a workaround, avoid modifying or disabling Discourse’s default Content Security Policy, and blocking watched words containing HTML tags. | 4.2 | More Details |
| CVE-2021-37860 | Mattermost 5.38 and earlier fails to sufficiently sanitize clipboard contents, which allows a user-assisted attacker to inject arbitrary web script in product deployments that explicitly disable the default CSP. | 3.7 | More Details |
| CVE-2021-41534 | A vulnerability has been identified in NX 1980 Series (All versions < V1984), Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13703). | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41533 | A vulnerability has been identified in NX 1980 Series (All versions < V1984), Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13565). | 3.3 | More Details |
| CVE-2020-4803 | IBM Edge 4.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 189535. | 3.3 | More Details |
| CVE-2020-4805 | IBM Edge 4.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 189539. | 3.3 | More Details |
| CVE-2021-41538 | A vulnerability has been identified in NX 1953 Series (All versions < V1973.3700), NX 1980 Series (All versions < V1988), Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ files. An attacker could leverage this vulnerability to leak information from unexpected memory locations (ZDI-CAN-13770). | 3.3 | More Details |
| CVE-2020-4809 | IBM Edge 4.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 189633. | 3.3 | More Details |
| CVE-2021-23445 | This affects the package datatables.net before 1.11.3. If an array is passed to the HTML escape entities function it would not have its contents escaped. | 3.1 | More Details |
| CVE-2021-20377 | IBM Security Guardium 11.3 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: 195569. | 2.7 | More Details |
| CVE-2021-40701 | Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-40703 | Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | N/A | More Details |
| CVE-2021-40702 | Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious psd file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | N/A | More Details |
| CVE-2021-40700 | Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | N/A | More Details |
| CVE-2021-35313 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none | N/A | More Details |
| CVE-2021-41428 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none | N/A | More Details |
| CVE-2021-39824 | Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious png file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. | N/A | More Details |