SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 17 November 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-2021-40519 | Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. | 10.0 | More Details |
| CVE-2021-41269 | cron-utils is a Java library to define, parse, validate, migrate crons as well as get human readable descriptions for them. In affected versions A template Injection was identified in cron-utils enabling attackers to inject arbitrary Java EL expressions, leading to unauthenticated Remote Code Execution (RCE) vulnerability. Versions up to 9.1.2 are susceptible to this vulnerability. Please note, that only projects using the @Cron annotation to validate untrusted Cron expressions are affected. The issue was patched and a new version was released. Please upgrade to version 9.1.6. There are no known workarounds known. | 10.0 | More Details |
| CVE-2021-43362 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MedData HBYS allows SQL Injection.This issue affects HBYS: from unspecified before 1.1. | 9.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-43361 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MedData HBYS allows SQL Injection.This issue affects HBYS: from unspecified before 1.1. | 9.9 | More Details |
| CVE-2021-1975 | Possible heap overflow due to improper length check of domain while parsing the DNS response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables | 9.8 | More Details |
| CVE-2020-16152 | The NetConfig UI administrative interface in Extreme Networks ExtremeWireless Aerohive HiveOS and IQ Engine through 10.0r8a allows attackers to execute PHP code as the root user via remote HTTP requests that insert this code into a log file and then traverse to that file. | 9.8 | More Details |
| CVE-2021-41264 | OpenZeppelin Contracts is a library for smart contract development. In affected versions upgradeable contracts using `UUPSUpgradeable` may be vulnerable to an attack affecting uninitialized implementation contracts. A fix is included in version 4.3.2 of `@openzeppelin/contracts` and `@openzeppelin/contracts-upgradeable`. For users unable to upgrade; initialize implementation contracts using `UUPSUpgradeable` by invoking the initializer function (usually called `initialize`). An example is provided [in the forum](https://forum.openzeppelin.com/t/security-advisory-initialize-uups-implementation-contracts/15301). | 9.8 | More Details |
| CVE-2021-39303 | The server in Jamf Pro before 10.32.0 has an SSRF vulnerability, aka PI-006352. NOTE: Jamf Nation will also publish an article about this vulnerability. | 9.8 | More Details |
| CVE-2021-3918 | json-schema is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 9.8 | More Details |
| CVE-2021-41653 | The PING function on the TP-Link TL-WR840N EU v5 router with firmware through TL-WR840N(EU)_V5_171211 is vulnerable to remote code execution via a crafted payload in an IP address input field. | 9.8 | More Details |
| CVE-2021-43617 | Laravel Framework through 8.70.2 does not sufficiently block the upload of executable PHP content because Illuminate/Validation/Concerns/ValidatesAttributes.php lacks a check for .phar files, which are handled as application/x-httpd-php on systems based on Debian. NOTE: this CVE Record is for Laravel Framework, and is unrelated to any reports concerning incorrectly written user applications for image upload. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42580 | Sourcecodester Online Learning System 2.0 is vunlerable to sql injection authentication bypass in admin login file (/admin/login.php) and authenticated file upload in (Master.php) file , we can craft these two vunlerablities to get unauthenticated remote command execution. | 9.8 | More Details |
| CVE-2021-43272 | An improper handling of exceptional conditions vulnerability exists in Open Design Alliance ODA Viewer sample before 2022.11. ODA Viewer continues to process invalid or malicious DWF files instead of stopping upon an exception. An attacker can leverage this vulnerability to execute code in the context of the current process. | 9.8 | More Details |
| CVE-2021-41765 | A SQL injection issue in pages/edit_fields/9_ajax/add_keyword.php of ResourceSpace 9.5 and 9.6 < rev 18274 allows remote unauthenticated attackers to execute arbitrary SQL commands via the k parameter. This allows attackers to uncover the full contents of the ResourceSpace database, including user session cookies. An attacker who gets an admin user session cookie can use the session cookie to execute arbitrary code on the server. | 9.8 | More Details |
| CVE-2021-43136 | An authentication bypass issue in FormaLMS <= 2.4.4 allows an attacker to bypass the authentication mechanism and obtain a valid access to the platform. | 9.8 | More Details |
| CVE-2021-42377 | An attacker-controlled pointer free in Busybox's hush applet leads to denial of service and possible code execution when processing a crafted shell command, due to the shell mishandling the &&& string. This may be used for remote code execution under rare conditions of filtered command input. | 9.8 | More Details |
| CVE-2021-37580 | A flaw was found in Apache ShenYu Admin. The incorrect use of JWT in ShenyuAdminBootstrap allows an attacker to bypass authentication. This issue affected Apache ShenYu 2.3.0 and 2.4.0 | 9.8 | More Details |
| CVE-2021-3958 | Improper Handling of Parameters vulnerability in Ipack Automation Systems Ipack SCADA Software allows : Blind SQL Injection.This issue affects Ipack SCADA Software: from unspecified before 1.1.0. | 9.8 | More Details |
| CVE-2021-30321 | Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-43048 | The Interior Server and Gateway Server components of TIBCO Software Inc.'s TIBCO PartnerExpress contain a vulnerability that theoretically allows an unauthenticated attacker with network access to execute a clickjacking attack on the affected system. A successful attack using this vulnerability does not require human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: versions 6.2.1 and below. | 9.8 | More Details |
| CVE-2020-23878 | pdf2json v0.71 was discovered to contain a stack buffer overflow in the component XRef::fetch. | 9.8 | More Details |
| CVE-2021-41080 | Zoho ManageEngine Network Configuration Manager before 125465 is vulnerable to SQL Injection in a hardware details search. | 9.8 | More Details |
| CVE-2021-40520 | Airangel HSMX Gateway devices through 5.2.04 have Weak SSH Credentials. | 9.8 | More Details |
| CVE-2020-23877 | pdf2xml v2.0 was discovered to contain a stack buffer overflow in the component getObjectStream. | 9.8 | More Details |
| CVE-2021-3064 | A memory corruption vulnerability exists in Palo Alto Networks GlobalProtect portal and gateway interfaces that enables an unauthenticated network-based attacker to disrupt system processes and potentially execute arbitrary code with root privileges. The attacker must have network access to the GlobalProtect interface to exploit this issue. This issue impacts PAN-OS 8.1 versions earlier than PAN-OS 8.1.17. Prisma Access customers are not impacted by this issue. | 9.8 | More Details |
| CVE-2021-40521 | Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. | 9.8 | More Details |
| CVE-2021-33816 | The website builder module in Dolibarr 13.0.2 allows remote PHP code execution because of an incomplete protection mechanism in which system, exec, and shell_exec are blocked but backticks are not blocked. | 9.8 | More Details |
| CVE-2021-43573 | A buffer overflow was discovered on Realtek RTL8195AM devices before 2.0.10. It exists in the client code when processing a malformed IE length of HT capability information in the Beacon and Association response frame. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-23874 | pdf2xml v2.0 was discovered to contain a heap-buffer overflow in the function TextPage::addAttributsNode. | 9.8 | More Details |
| CVE-2020-23873 | pdf2xml v2.0 was discovered to contain a heap-buffer overflow in the function TextPage::dump. | 9.8 | More Details |
| CVE-2021-41081 | Zoho ManageEngine Network Configuration Manager before 125465 is vulnerable to SQL Injection in a configuration search. | 9.8 | More Details |
| CVE-2021-41833 | Zoho ManageEngine Patch Connect Plus before 90099 is vulnerable to unauthenticated remote code execution. | 9.8 | More Details |
| CVE-2021-42002 | Zoho ManageEngine ADManager Plus before 7115 is vulnerable to a filter bypass that leads to file-upload remote code execution. | 9.8 | More Details |
| CVE-2021-42847 | Zoho ManageEngine ADAudit Plus before 7006 allows attackers to write to, and execute, arbitrary files. | 9.8 | More Details |
| CVE-2021-43350 | An unauthenticated Apache Traffic Control Traffic Ops user can send a request with a specially-crafted username to the POST /login endpoint of any API version to inject unsanitized content into the LDAP filter. | 9.8 | More Details |
| CVE-2021-42774 | Broadcom Emulex HBA Manager/One Command Manager versions before 11.4.425.0 and 12.8.542.31, if not installed in Strictly Local Management mode, have a buffer overflow vulnerability in the remote firmware download feature that could allow remote unauthenticated users to perform various attacks. In non-secure mode, the user is unauthenticated. | 9.8 | More Details |
| CVE-2021-43523 | In uClibc and uClibc-ng before 1.0.39, incorrect handling of special characters in domain names returned by DNS servers via gethostbyname, getaddrinfo, gethostbyaddr, and getnameinfo can lead to output of wrong hostnames (leading to domain hijacking) or injection into applications (leading to remote code execution, XSS, applications crashes, etc.). In other words, a validation step, which is expected in any stub resolver, does not occur. | 9.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42775 | Broadcom Emulex HBA Manager/One Command Manager versions before 11.4.425.0 and 12.8.542.31, if not installed in Strictly Local Management mode, have a vulnerability in the remote firmware download feature that could allow a user to place or replace an arbitrary file on the remote host. In non-secure mode, the user is unauthenticated. | 9.1 | More Details |
| CVE-2021-41244 | Grafana is an open-source platform for monitoring and observability. In affected versions when the fine-grained access control beta feature is enabled and there is more than one organization in the Grafana instance admins are able to access users from other organizations. Grafana 8.0 introduced a mechanism which allowed users with the Organization Admin role to list, add, remove, and update users' roles in other organizations in which they are not an admin. With fine-grained access control enabled, organization admins can list, add, remove and update users' roles in another organization, where they do not have organization admin role. All installations between v8.0 and v8.2.3 that have fine-grained access control beta enabled and more than one organization should be upgraded as soon as possible. If you cannot upgrade, you should turn off the fine-grained access control using a feature flag. | 9.1 | More Details |
| CVE-2021-41950 | A directory traversal issue in ResourceSpace 9.6 before 9.6 rev 18277 allows remote unauthenticated attackers to delete arbitrary files on the ResourceSpace server via the provider and variant parameters in pages/ajax/tiles.php. Attackers can delete configuration or source code files, causing the application to become unavailable to all users. | 9.1 | More Details |
| CVE-2021-42114 | Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. | 9.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-1924 | Information disclosure through timing and power side-channels during mod exponentiation for RSA-CRT in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 9.0 | More Details |
| CVE-2021-43616 | The npm ci command in npm 7.x and 8.x through 8.1.3 proceeds with an installation even if dependency information in package-lock.json differs from package.json. This behavior is inconsistent with the documentation, and makes it easier for attackers to install malware that was supposed to have been blocked by an exact version match requirement in package-lock.json. NOTE: The npm team believes this is not a vulnerability. It would require someone to socially engineer package.json which has different dependencies than package-lock.json. That user would have to have file system or write access to change dependencies. The npm team states preventing malicious actors from socially engineering or gaining file system access is outside the scope of the npm CLI. | 9.0 | More Details |
| CVE-2021-43047 | The Interior Server and Gateway Server components of TIBCO Software Inc.'s TIBCO PartnerExpress contain easily exploitable Stored and Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: versions 6.2.1 and below. | 9.0 | More Details |
| CVE-2021-26443 | Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-37157 | An issue was discovered in OpenGamePanel OGP-Agent-Linux through 2021-08-14. $HOME/OGP/Cfg/Config.pm has the root password in cleartext. | 8.8 | More Details |
| CVE-2021-37158 | An issue was discovered in OpenGamePanel OGP-Agent-Linux through 2021-08-14. An authenticated attacker could inject OS commands by starting a Counter-Strike server and using the map field to enter a Bash command. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42283 | NTFS Elevation of Privilege Vulnerability | 8.8 | More Details |
| CVE-2021-42316 | Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2021-34991 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6400v2 1.0.4.106_10.0.80 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPnP service, which listens on TCP port 5000 by default. When parsing the uuid request header, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-14110. | 8.8 | More Details |
| CVE-2021-34992 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Orckestra C1 CMS 6.10. Authentication is required to exploit this vulnerability. The specific flaw exists within Composite.dll. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-14740. | 8.8 | More Details |
| CVE-2021-42321 | Microsoft Exchange Server Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2021-26795 | A SQL Injection vulnerability in /appliance/shiftmgn.php in TalariaX sendQuick Alert Plus Server Admin 4.3 before 8HF11 allows attackers to obtain sensitive information via a Roster Time to Roster Management. | 8.8 | More Details |
| CVE-2021-42275 | Microsoft COM for Windows Remote Code Execution Vulnerability | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3840 | A dependency confusion vulnerability was reported in the Antilles open-source software prior to version 1.0.1 that could allow for remote code execution during installation due to a package listed in requirements.txt not existing in the public package index (PyPi). MITRE classifies this weakness as an Uncontrolled Search Path Element (CWE-427) in which a private package dependency may be replaced by an unauthorized package of the same name published to a well-known public repository such as PyPi. The configuration has been updated to only install components built by Antilles, removing all other public package indexes. Additionally, the antilles-tools dependency has been published to PyPi. | 8.8 | More Details |
| CVE-2021-3577 | An unauthenticated remote code execution vulnerability was reported in some Motorola-branded Binatone Hubble Cameras that could allow an attacker on the same network unauthorized access to the device. | 8.8 | More Details |
| CVE-2020-21141 | iCMS v7.0.15 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admincp.php?app=members&do=add. | 8.8 | More Details |
| CVE-2021-25940 | In ArangoDB, versions v3.7.6 through v3.8.3 are vulnerable to Insufficient Session Expiration. When a user's password is changed by the administrator, the session isn't invalidated, allowing a malicious user to still be logged in and perform arbitrary actions within the system. | 8.8 | More Details |
| CVE-2021-25965 | In Calibre-web, versions 0.6.0 to 0.6.13 are vulnerable to Cross-Site Request Forgery (CSRF). By luring an authenticated user to click on a link, an attacker can create a new user role with admin privileges and attacker-controlled credentials, allowing them to take over the application. | 8.8 | More Details |
| CVE-2021-42839 | Grand Vice info Co. webopac7 file upload function fails to filter special characters. While logging in with general user's permission, remote attackers can upload malicious script and execute arbitrary code to control the system or interrupt services. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41254 | kustomize-controller is a Kubernetes operator, specialized in running continuous delivery pipelines for infrastructure and workloads defined with Kubernetes manifests and assembled with Kustomize. Users that can create Kubernetes Secrets, Service Accounts and Flux Kustomization objects, could execute commands inside the kustomize-controller container by embedding a shell script in a Kubernetes Secret. This can be used to run `kubectl` commands under the Service Account of kustomize-controller, thus allowing an authenticated Kubernetes user to gain cluster admin privileges. In affected versions multitenant environments where non-admin users have permissions to create Flux Kustomization objects are affected by this issue. This vulnerability was fixed in kustomize-controller v0.15.0 (included in flux2 v0.18.0) released on 2021-10-08. Starting with v0.15, the kustomize-controller no longer executes shell commands on the container OS and the `kubectl` binary has been removed from the container image. To prevent the creation of Kubernetes Service Accounts with `secrets` in namespaces owned by tenants, a Kubernetes validation webhook such as Gatekeeper OPA or Kyverno can be used. | 8.8 | More Details |
| CVE-2021-43563 | An issue was discovered in the pixxio (aka pixx.io integration or DAM) extension before 1.0.6 for TYPO3. The Access Control in the bundled media browser is broken, which allows an unauthenticated attacker to perform requests to the pixx.io API for the configured API user. This allows an attacker to download various media files from the DAM system. | 8.8 | More Details |
| CVE-2021-25980 | In Talkyard, versions v0.04.01 through v0.6.74-WIP-63220cb, v0.2020.22-WIP-b2e97fe0e through v0.2021.02-WIP-879ef3fe1 and tyse-v0.2021.02-879ef3fe1-regular through tyse-v0.2021.28-af66b6905-regular, are vulnerable to Host Header Injection. By luring a victim application-user to click on a link, an unauthenticated attacker can use the “forgot password” functionality to reset the victim’s password and successfully take over their account. | 8.8 | More Details |
| CVE-2021-3058 | An OS command injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator with permissions to use XML API the ability to execute arbitrary OS commands to escalate privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20-h1; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14-h3; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11-h2; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8; PAN-OS 10.1 versions earlier than PAN-OS 10.1.3. This issue does not impact Prisma Access firewalls. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3056 | A memory corruption vulnerability in Palo Alto Networks PAN-OS GlobalProtect Clientless VPN enables an authenticated attacker to execute arbitrary code with root user privileges during SAML authentication. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1. Prisma Access customers with Prisma Access 2.1 Preferred firewalls are impacted by this issue. | 8.8 | More Details |
| CVE-2021-38666 | Remote Desktop Client Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2021-43397 | LiquidFiles before 3.6.3 allows remote attackers to elevate their privileges from Admin (or User Admin) to Sysadmin. | 8.8 | More Details |
| CVE-2021-43562 | An issue was discovered in the pixxio (aka pixx.io integration or DAM) extension before 1.0.6 for TYPO3. The extension fails to restrict the image download to the configured pixx.io DAM URL, resulting in SSRF. As a result, an attacker can download various content from a remote location and save it to a user-controlled filename, which may result in Remote Code Execution. A TYPO3 backend user account is required to exploit this. | 8.8 | More Details |
| CVE-2021-22048 | The vCenter Server contains a privilege escalation vulnerability in the IWA (Integrated Windows Authentication) authentication mechanism. A malicious actor with non-administrative access to vCenter Server may exploit this issue to elevate privileges to a higher privileged group. | 8.8 | More Details |
| CVE-2021-41426 | Beeline Smart box 2.0.38 is vulnerable to Cross Site Request Forgery (CSRF) via mgt_end_user.htm. | 8.8 | More Details |
| CVE-2021-40502 | SAP Commerce - versions 2105.3, 2011.13, 2005.18, 1905.34, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. Authenticated attackers will be able to access and edit data from b2b units they do not belong to. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41266 | Minio console is a graphical user interface for the for MinIO operator. Minio itself is a multi-cloud object storage project. Affected versions are subject to an authentication bypass issue in the Operator Console when an external IDP is enabled. All users on release v0.12.2 and before are affected and are advised to update to 0.12.3 or newer. Users unable to upgrade should add automountServiceAccountToken: false to the operator-console deployment in Kubernetes so no service account token will get mounted inside the pod, then disable the external identity provider authentication by unset the CONSOLE_IDP_URL, CONSOLE_IDP_CLIENT_ID, CONSOLE_IDP_SECRET and CONSOLE_IDP_CALLBACK environment variable and instead use the Kubernetes service account token. | 8.6 | More Details |
| CVE-2021-1912 | Possible integer overflow can occur due to improper length check while calculating count and grace period in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile | 8.4 | More Details |
| CVE-2021-41263 | rails_multisite provides multi-db support for Rails applications. In affected versions this vulnerability impacts any Rails applications using `rails_multisite` alongside Rails' signed/encrypted cookies. Depending on how the application makes use of these cookies, it may be possible for an attacker to re-use cookies on different 'sites' within a multi-site Rails application. The issue has been patched in v4 of the `rails_multisite` gem. Note that this upgrade will invalidate all previous signed/encrypted cookies. The impact of this invalidation will vary based on the application architecture. | 8.3 | More Details |
| CVE-2021-38684 | A stack buffer overflow vulnerability has been reported to affect QNAP NAS running Multimedia Console. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of Multimedia Console: Multimedia Console 1.4.3 ( 2021/10/05 ) and later Multimedia Console 1.5.3 ( 2021/10/05 ) and later | 8.1 | More Details |
| CVE-2021-40501 | SAP ABAP Platform Kernel - versions 7.77, 7.81, 7.85, 7.86, does not perform necessary authorization checks for an authenticated business user, resulting in escalation of privileges. That means this business user is able to read and modify data beyond the vulnerable system. However, the attacker can neither significantly reduce the performance of the system nor stop the system. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3059 | An OS command injection vulnerability in the Palo Alto Networks PAN-OS management interface exists when performing dynamic updates. This vulnerability enables a man-in-the-middle attacker to execute arbitrary OS commands to escalate privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20-h1; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14-h3; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11-h2; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8; PAN-OS 10.1 versions earlier than PAN-OS 10.1.3. Prisma Access customers that have Prisma Access 2.1 Preferred or Prisma Access 2.1 Innovation firewalls are impacted by this issue. | 8.1 | More Details |
| CVE-2021-3060 | An OS command injection vulnerability in the Simple Certificate Enrollment Protocol (SCEP) feature of PAN-OS software allows an unauthenticated network-based attacker with specific knowledge of the firewall configuration to execute arbitrary code with root user privileges. The attacker must have network access to the GlobalProtect interfaces to exploit this issue. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20-h1; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14-h3; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11-h2; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8; PAN-OS 10.1 versions earlier than PAN-OS 10.1.3. Prisma Access customers with Prisma Access 2.1 Preferred and Prisma Access 2.1 Innovation firewalls are impacted by this issue. | 8.1 | More Details |
| CVE-2021-43578 | Jenkins Squash TM Publisher (Squash4Jenkins) Plugin 1.0.0 and earlier implements an agent-to-controller message that does not implement any validation of its input, allowing attackers able to control agent processes to replace arbitrary files on the Jenkins controller file system with an attacker-controlled JSON string. | 8.1 | More Details |
| CVE-2021-3062 | An improper access control vulnerability in PAN-OS software enables an attacker with authenticated access to GlobalProtect portals and gateways to connect to the EC2 instance metadata endpoint for VM-Series firewalls hosted on Amazon AWS. Exploitation of this vulnerability enables an attacker to perform any operations allowed by the EC2 role in AWS. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20 VM-Series firewalls; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11 VM-Series firewalls; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14 VM-Series firewalls; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8 VM-Series firewalls. Prisma Access customers are not impacted by this issue. | 8.1 | More Details |
| CVE-2021-25976 | In PiranhaCMS, versions 4.0.0-alpha1 to 9.2.0 are vulnerable to cross-site request forgery (CSRF) when performing various actions supported by the management system, such as deleting a user, deleting a role, editing a post, deleting a media folder etc., when an ID is known. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34417 | The network proxy page on the web portal for the Zoom On-Premise Meeting Connector Controller before version 4.6.365.20210703, Zoom On-Premise Meeting Connector MMR before version 4.6.365.20210703, Zoom On-Premise Recording Connector before version 3.8.45.20210703, Zoom On-Premise Virtual Room Connector before version 4.4.6868.20210703, and Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5496.20210703 fails to validate input sent in requests to set the network proxy password. This could lead to remote command injection by a web portal administrator. | 7.9 | More Details |
| CVE-2020-12900 | An arbitrary write vulnerability in the AMD Radeon Graphics Driver for Windows 10 potentially allows unprivileged users to gain Escalation of Privileges and cause Denial of Service. | 7.8 | More Details |
| CVE-2021-26331 | AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. | 7.8 | More Details |
| CVE-2021-30255 | Possible buffer overflow due to improper input validation in PDM DIAG command in FTM in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 7.8 | More Details |
| CVE-2021-30254 | Possible buffer overflow due to improper input validation in factory calibration and test DIAG command in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 7.8 | More Details |
| CVE-2020-12961 | A potential vulnerability exists in AMD Platform Security Processor (PSP) that may allow an attacker to zero any privileged register on the System Management Network which may lead to bypassing SPI ROM protections. | 7.8 | More Details |
| CVE-2021-1979 | Possible buffer overflow due to improper validation of FTM command payload in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 7.8 | More Details |
| CVE-2021-26315 | When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-26323 | Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. | 7.8 | More Details |
| CVE-2021-1973 | A FTM Diag command can allow an arbitrary write into modem OS space in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 7.8 | More Details |
| CVE-2021-1921 | Possible memory corruption due to Improper handling of hypervisor unmap operations for concurrent memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 7.8 | More Details |
| CVE-2021-26335 | Improper input and range checking in the AMD Secure Processor (ASP) boot loader image header may allow an attacker to use attacker-controlled values prior to signature validation potentially resulting in arbitrary code execution. | 7.8 | More Details |
| CVE-2020-12944 | Insufficient validation of BIOS image length by ASP Firmware could lead to arbitrary code execution. | 7.8 | More Details |
| CVE-2021-42726 | Adobe Bridge version 11.1.1 (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. | 7.8 | More Details |
| CVE-2021-43013 | Adobe Media Encoder version 15.4.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2021-42721 | Acrobat Bridge versions 11.1.1 and earlier are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2021-32023 | An elevation of privilege vulnerability in the message broker of BlackBerry Protect for Windows version(s) versions 1574 and earlier could allow an attacker to potentially execute code in the context of a BlackBerry Cylance service that has admin rights on the system. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42723 | Adobe Bridge version 11.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted SGI file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2021-42725 | Adobe Bridge version 11.1.1 (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. | 7.8 | More Details |
| CVE-2021-42731 | Adobe InDesign versions 16.4 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted 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-2021-43011 | Adobe Prelude version 10.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious M4A file. | 7.8 | More Details |
| CVE-2021-32021 | A denial of service vulnerability in the message broker of BlackBerry Protect for Windows version(s) versions 1574 and earlier could allow an attacker to potentially execute code in the context of a BlackBerry Cylance service that has admin rights on the system. | 7.8 | More Details |
| CVE-2021-30259 | Possible out of bound access due to improper validation of function table entries in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 7.8 | More Details |
| CVE-2021-26326 | Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. | 7.8 | More Details |
| CVE-2020-12895 | Pool/Heap Overflow in AMD Graphics Driver for Windows 10 in Escape 0x110037 may lead to escalation of privilege, information disclosure or denial of service. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-43277 | An out-of-bounds read vulnerability exists in the U3D file reading procedure in Open Design Alliance PRC SDK before 2022.10. Crafted data in a U3D file can trigger a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. | 7.8 | More Details |
| CVE-2020-12964 | A potential privilege escalation/denial of service issue exists in the AMD Radeon Kernel Mode driver Escape 0x2000c00 Call handler. An attacker with low privilege could potentially induce a Windows BugCheck or write to leak information. | 7.8 | More Details |
| CVE-2021-42706 | This vulnerability could allow an attacker to disclose information and execute arbitrary code on affected installations of WebAccess/MHI Designer | 7.8 | More Details |
| CVE-2020-12902 | Arbitrary Decrement Privilege Escalation in AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service. | 7.8 | More Details |
| CVE-2021-43391 | An Out-of-Bounds Read vulnerability exists when reading a DXF file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DXF files. Crafted data in a DXF file (an invalid dash counter in line types) can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |
| CVE-2020-12929 | Improper parameters validation in some trusted applications of the PSP contained in the AMD Graphics Driver may allow a local attacker to bypass security restrictions and achieve arbitrary code execution . | 7.8 | More Details |
| CVE-2021-43336 | An Out-of-Bounds Write vulnerability exists when reading a DXF or DWG file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DXF and DWG files. Crafted data in a DXF or DWG file (an invalid number of properties) can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |
| CVE-2021-43280 | A stack-based buffer overflow vulnerability exists in the DWF file reading procedure in Open Design Alliance Drawings SDK before 2022.8. The issue results from the lack of proper validation of the length of user-supplied data before copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-43279 | An out-of-bounds write vulnerability exists in the U3D file reading procedure in Open Design Alliance PRC SDK before 2022.10. Crafted data in a U3D file can trigger a write past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. | 7.8 | More Details |
| CVE-2021-43278 | An Out-of-bounds Read vulnerability exists in the OBJ file reading procedure in Open Design Alliance Drawings SDK before 2022.11. The lack of validating the input length can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |
| CVE-2021-43276 | An Out-of-bounds Read vulnerability exists in Open Design Alliance ODA Viewer before 2022.8. Crafted data in a DWF file can trigger a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process | 7.8 | More Details |
| CVE-2021-25985 | In Factor (App Framework & Headless CMS) v1.0.4 to v1.8.30, improperly invalidate a user's session even after the user logs out of the application. In addition, user sessions are stored in the browser's local storage, which by default does not have an expiration time. This makes it possible for an attacker to steal and reuse the cookies using techniques such as XSS attacks, followed by a local account takeover. | 7.8 | More Details |
| CVE-2020-12963 | An insufficient pointer validation vulnerability in the AMD Graphics Driver for Windows may allow unprivileged users to compromise the system. | 7.8 | More Details |
| CVE-2021-43275 | A Use After Free vulnerability exists in the DGN file reading procedure in Open Design Alliance Drawings SDK before 2022.8. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |
| CVE-2020-12892 | An untrusted search path in AMD Radeon settings Installer may lead to a privilege escalation or unauthorized code execution. | 7.8 | More Details |
| CVE-2021-43274 | A Use After Free Vulnerability exists in the Open Design Alliance Drawings SDK before 2022.11. The specific flaw exists within the parsing of DWF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-12898 | Stack Buffer Overflow in AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service. | 7.8 | More Details |
| CVE-2020-12893 | Stack Buffer Overflow in AMD Graphics Driver for Windows 10 in Escape 0x15002a may lead to escalation of privilege or denial of service. | 7.8 | More Details |
| CVE-2020-12903 | Out of Bounds Write and Read in AMD Graphics Driver for Windows 10 in Escape 0x6002d03 may lead to escalation of privilege or denial of service. | 7.8 | More Details |
| CVE-2020-12962 | Escape call interface in the AMD Graphics Driver for Windows may cause privilege escalation. | 7.8 | More Details |
| CVE-2021-42563 | There is an Unquoted Service Path in NI Service Locator (nisvcloc.exe) in versions prior to 18.0 on Windows. This may allow an authorized local user to insert arbitrary code into the unquoted service path and escalate privileges. | 7.8 | More Details |
| CVE-2021-43390 | An Out-of-Bounds Write vulnerability exists when reading a DGN file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DGN files. Crafted data in a DGN file and lack of proper validation of input data can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |
| CVE-2021-43012 | Adobe Prelude version 10.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious M4A file. | 7.8 | More Details |
| CVE-2021-42292 | Microsoft Excel Security Feature Bypass Vulnerability | 7.8 | More Details |
| CVE-2021-42285 | Windows Kernel Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-41370 | NTFS Elevation of Privilege Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41366 | Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-43209 | 3D Viewer Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-42298 | Microsoft Defender Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-42296 | Microsoft Word Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-40442 | Microsoft Excel Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-41367 | NTFS Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-40503 | An information disclosure vulnerability exists in SAP GUI for Windows - versions < 7.60 PL13, 7.70 PL4, which allows an attacker with sufficient privileges on the local client-side PC to obtain an equivalent of the user's password. With this highly sensitive data leaked, the attacker would be able to logon to the backend system the SAP GUI for Windows was connected to and launch further attacks depending on the authorizations of the user. | 7.8 | More Details |
| CVE-2021-42276 | Microsoft Windows Media Foundation Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-36957 | Windows Desktop Bridge Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-42322 | Visual Studio Code Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-41378 | Windows NTFS Remote Code Execution Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41377 | Windows Fast FAT File System Driver Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-43208 | 3D Viewer Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2021-31853 | DLL Search Order Hijacking Vulnerability in McAfee Drive Encryption (MDE) prior to 7.3.0 HF2 (7.3.0.183) allows local users to execute arbitrary code and escalate privileges via execution from a compromised folder. | 7.8 | More Details |
| CVE-2021-42286 | Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2021-41372 | A Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) vulnerability exists when Power BI Report Server Template file (pbix) containing HTML files is uploaded to the server and HTML files are accessed directly by the victim. Combining these 2 vulnerabilities together, an attacker is able to upload malicious Power BI templates files to the server using the victim's session and run scripts in the security context of the user and perform privilege escalation in case the victim has admin privileges when the victim access one of the HTML files present in the malicious Power BI template uploaded. The security update addresses the vulnerability by helping to ensure that Power BI Report Server properly sanitize file uploads. | 7.6 | More Details |
| CVE-2002-20001 | The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)at or D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. | 7.5 | More Details |
| CVE-2021-26558 | Deserialization of Untrusted Data vulnerability of Apache ShardingSphere-UI allows an attacker to inject outer link resources. This issue affects Apache ShardingSphere-UI Apache ShardingSphere-UI version 4.1.1 and later versions; Apache ShardingSphere-UI versions prior to 5.0.0. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-43620 | An issue was discovered in the fruity crate through 0.2.0 for Rust. Security-relevant validation of filename extensions is plausibly affected. Methods of NSString for conversion to a string may return a partial result. Because they call CStr::from_ptr on a pointer to the string buffer, the string is terminated at the first '\0' byte, which might not be the end of the string. | 7.5 | More Details |
| CVE-2021-43618 | GNU Multiple Precision Arithmetic Library (GMP) through 6.2.1 has an mpz/inp_raw.c integer overflow and resultant buffer overflow via crafted input, leading to a segmentation fault on 32-bit platforms. | 7.5 | More Details |
| CVE-2021-43494 | OpenCV-REST-API master branch as of commit 69be158c05d4dd5a4aff38fdc680a162dd6b9e49 is affected by a directory traversal vulnerability. This attack can cause the disclosure of critical secrets stored anywhere on the system and can significantly aid in getting remote code access. | 7.5 | More Details |
| CVE-2021-21528 | Dell EMC PowerScale OneFS versions 9.1.0, 9.2.0.x, 9.2.1.x contain an Exposure of Information through Directory Listing vulnerability. This vulnerability is triggered when upgrading from a previous versions. | 7.5 | More Details |
| CVE-2021-41356 | Windows Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2021-43610 | Belledonne Belle-sip before 5.0.20 can crash applications such as Linphone via an invalid From header (request URI without a parameter) in an unauthenticated SIP message, a different issue than CVE-2021-33056. | 7.5 | More Details |
| CVE-2021-40873 | An issue was discovered in Softing Industrial Automation OPC UA C++ SDK before 5.66, and uaToolkit Embedded before 1.40. Remote attackers to cause a denial of service (DoS) by sending crafted messages to a client or server. The server process may crash unexpectedly because of a double free, and must be restarted. | 7.5 | More Details |
| CVE-2021-42773 | Broadcom Emulex HBA Manager/One Command Manager versions before 11.4.425.0 and 12.8.542.31, if not installed in Strictly Local Management mode, could allow a user to retrieve an arbitrary file from a remote host with the GetDumpFile command. In non-secure mode, the user is unauthenticated. | 7.5 | More Details |
| CVE-2021-26338 | Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3934 | ohmyzsh is vulnerable to Improper Neutralization of Special Elements used in an OS Command | 7.5 | More Details |
| CVE-2021-34598 | In Phoenix Contact FL MGUARD 1102 and 1105 in Versions 1.4.0, 1.4.1 and 1.5.0 the remote logging functionality is impaired by the lack of memory release for data structures from syslog-ng when remote logging is active | 7.5 | More Details |
| CVE-2021-1981 | Possible buffer over read due to improper IE size check of Bearer capability IE in MT setup request from network in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 7.5 | More Details |
| CVE-2021-1982 | Possible denial of service scenario due to improper input validation of received NAS OTA message in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 7.5 | More Details |
| CVE-2021-43564 | An issue was discovered in the jobfair (aka Job Fair) extension before 1.0.13 and 2.x before 2.0.2 for TYPO3. The extension fails to protect or obfuscate filenames of uploaded files. This allows unauthenticated users to download files with sensitive data by simply guessing the filename of uploaded files (e.g., uploads/tx_jobfair/cv.pdf). | 7.5 | More Details |
| CVE-2021-43611 | Belledonne Belle-sip before 5.0.20 can crash applications such as Linphone via " \ " in the display name of a From header. | 7.5 | More Details |
| CVE-2021-40872 | An issue was discovered in Softing Industrial Automation uaToolkit Embedded before 1.40. Remote attackers to cause a denial of service (DoS) or login as an anonymous user (bypassing security checks) by sending crafted messages to a OPC/UA server. The server process may crash unexpectedly because of an invalid type cast, and must be restarted. | 7.5 | More Details |
| CVE-2021-40871 | An issue was discovered in Softing Industrial Automation OPC UA C++ SDK before 5.66. Remote attackers to cause a denial of service (DoS) by sending crafted messages to a OPC/UA client. The client process may crash unexpectedly because of a wrong type cast, and must be restarted. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3063 | An improper handling of exceptional conditions vulnerability exists in Palo Alto Networks GlobalProtect portal and gateway interfaces that enables an unauthenticated network-based attacker to send specifically crafted traffic to a GlobalProtect interface that causes the service to stop responding. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.21; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14-h4; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11-h3; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8-h4; PAN-OS 10.1 versions earlier than PAN-OS 10.1.3. Prisma Access customers are not impacted by this issue. | 7.5 | More Details |
| CVE-2021-36323 | 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-2021-36324 | 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-2020-23872 | A NULL pointer dereference in the function TextPage::restoreState of pdf2xml v2.0 allows attackers to cause a denial of service (DoS). | 7.5 | More Details |
| CVE-2020-23876 | pdf2xml v2.0 was discovered to contain a memory leak in the function TextPage::testLinkedText. | 7.5 | More Details |
| CVE-2020-23879 | pdf2json v0.71 was discovered to contain a NULL pointer dereference in the component ObjectStream::getObject. | 7.5 | More Details |
| CVE-2021-42278 | Active Directory Domain Services Elevation of Privilege Vulnerability | 7.5 | More Details |
| CVE-2021-38984 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 212793. | 7.5 | More Details |
| CVE-2021-38983 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 212792. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-36325 | 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-2021-38979 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 uses a one-way cryptographic hash against an input that should not be reversible, such as a password, but the software does not also use a salt as part of the input. IBM X-Force ID: 212785. | 7.5 | More Details |
| CVE-2021-43046 | The Interior Server and Gateway Server components of TIBCO Software Inc.'s TIBCO PartnerExpress contain an easily exploitable vulnerability that allows an unauthenticated attacker with network access to obtain session tokens for the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: versions 6.2.1 and below. | 7.5 | More Details |
| CVE-2021-26322 | Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. | 7.5 | More Details |
| CVE-2021-42282 | Active Directory Domain Services Elevation of Privilege Vulnerability | 7.5 | More Details |
| CVE-2020-21627 | Ruijie RG-UAC commit 9071227 was discovered to contain a vulnerability in the component /current_action.php?action=reboot, which allows attackers to cause a denial of service (DoS) via unspecified vectors. | 7.5 | More Details |
| CVE-2021-43493 | ServerManagement master branch as of commit 49491cc6f94980e6be7791d17be947c27071eb56 is affected by a directory traversal vulnerability. This vulnerability can be used to extract credentials which can in turn be used to execute code. | 7.5 | More Details |
| CVE-2021-42287 | Active Directory Domain Services Elevation of Privilege Vulnerability | 7.5 | More Details |
| CVE-2021-43492 | AlquistManager branch as of commit 280d99f43b11378212652e75f6f3159cde9c1d36 is affected by a directory traversal vulnerability. This attack can cause the disclosure of critical secrets stored anywhere on the system andcan significantly aid in getting remote code access. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-43496 | Clustering master branch as of commit 53e663e259bcfc8cdecb56c0bb255bd70bfcaa70 is affected by a directory traversal vulnerability. This attack can cause the disclosure of critical secrets stored anywhere on the system and can significantly aid in getting remote code access. | 7.5 | More Details |
| CVE-2021-42291 | Active Directory Domain Services Elevation of Privilege Vulnerability | 7.5 | More Details |
| CVE-2021-43495 | AlquistManager branch as of commit 280d99f43b11378212652e75f6f3159cde9c1d36 is affected by a directory traversal vulnerability in alquist/IO/input.py. This attack can cause the disclosure of critical secrets stored anywhere on the system and can significantly aid in getting remote code access. | 7.5 | More Details |
| CVE-2021-30284 | Possible information exposure and denial of service due to NAS not dropping messages when integrity check fails in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 7.5 | More Details |
| CVE-2021-38665 | Remote Desktop Protocol Client Information Disclosure Vulnerability | 7.4 | More Details |
| CVE-2021-3907 | OctoRPKI does not escape a URI with a filename containing "..", this allows a repository to create a file, (ex. rsync://example.org/repo/../../etc/cron.daily/evil.roa), which would then be written to disk outside the base cache folder. This could allow for remote code execution on the host machine OctoRPKI is running on. | 7.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41258 | Kirby is an open source file structured CMS. In affected versions Kirby's blocks field stores structured data for each block. This data is then used in block snippets to convert the blocks to HTML for use in your templates. We recommend to escape HTML special characters to protect against cross-site scripting (XSS) attacks. The default snippet for the image block unfortunately did not use our escaping helper. This made it possible to include malicious HTML code in the source, alt and link fields of the image block, which would then be displayed on the site frontend and executed in the browsers of site visitors and logged in users who are browsing the site. Attackers must be in your group of authenticated Panel users in order to exploit this weakness. Users who do not make use of the blocks field are not affected. This issue has been patched in Kirby version 3.5.8 by escaping special HTML characters in the output from the default image block snippet. Please update to this or a later version to fix the vulnerability. | 7.3 | More Details |
| CVE-2021-41252 | Kirby is an open source file structured CMS ### Impact Kirby's writer field stores its formatted content as HTML code. Unlike with other field types, it is not possible to escape HTML special characters against cross-site scripting (XSS) attacks, otherwise the formatting would be lost. If the user is logged in to the Panel, a harmful script can for example trigger requests to Kirby's API with the permissions of the victim. Because the writer field did not securely sanitize its contents on save, it was possible to inject malicious HTML code into the content file by sending it to Kirby's API directly without using the Panel. This malicious HTML code would then be displayed on the site frontend and executed in the browsers of site visitors and logged in users who are browsing the site. Attackers must be in your group of authenticated Panel users in order to exploit this weakness. Users who do not make use of the writer field are not affected. This issue has been patched in Kirby 3.5.8 by sanitizing all writer field contents on the backend whenever the content is modified via Kirby's API. Please update to this or a later version to fix the vulnerability. | 7.3 | More Details |
| CVE-2021-42384 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the handle_special function | 7.2 | More Details |
| CVE-2021-34422 | The Keybase Client for Windows before version 5.7.0 contains a path traversal vulnerability when checking the name of a file uploaded to a team folder. A malicious user could upload a file to a shared folder with a specially crafted file name which could allow a user to execute an application which was not intended on their host machine. If a malicious user leveraged this issue with the public folder sharing feature of the Keybase client, this could lead to remote code execution. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42385 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function | 7.2 | More Details |
| CVE-2021-42381 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the hash_init function | 7.2 | More Details |
| CVE-2021-42382 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_s function | 7.2 | More Details |
| CVE-2021-42383 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function | 7.2 | More Details |
| CVE-2021-42379 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the next_input_file function | 7.2 | More Details |
| CVE-2021-3723 | A command injection vulnerability was reported in the Integrated Management Module (IMM) of legacy IBM System x 3550 M3 and IBM System x 3650 M3 servers that could allow the execution of operating system commands over an authenticated SSH or Telnet session. | 7.2 | More Details |
| CVE-2021-42380 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the clrvar function | 7.2 | More Details |
| CVE-2021-42386 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the nvalloc function | 7.2 | More Details |
| CVE-2021-39474 | Vulnerability in the product Docsis 3.0 UBC1319BA00 Router supported affected version 1319010201r009. The vulnerability allows an attacker with privileges and network access through the ping.cmd component to execute commands on the device. | 7.2 | More Details |
| CVE-2021-42378 | A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_i function | 7.2 | More Details |
| CVE-2021-43577 | Jenkins OWASP Dependency-Check Plugin 5.1.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41057 | In WIBU CodeMeter Runtime before 7.30a, creating a crafted CmDongles symbolic link will overwrite the linked file without checking permissions. | 7.1 | More Details |
| CVE-2020-12899 | Arbitrary Read in AMD Graphics Driver for Windows 10 may lead to KASLR bypass or denial of service. | 7.1 | More Details |
| CVE-2020-12894 | Arbitrary Write in AMD Graphics Driver for Windows 10 in Escape 0x40010d may lead to arbitrary write to kernel memory or denial of service. | 7.1 | More Details |
| CVE-2020-12946 | Insufficient input validation in ASP firmware for discrete TPM commands could allow a potential loss of integrity and denial of service. | 7.1 | More Details |
| CVE-2020-12951 | Race condition in ASP firmware could allow less privileged x86 code to perform ASP SMM (System Management Mode) operations. | 7.0 | More Details |
| CVE-2021-34357 | A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running QmailAgent. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of QmailAgent: QmailAgent 3.0.2 ( 2021/08/25 ) and later | 6.9 | More Details |
| CVE-2021-3788 | An exposed debug interface was reported in some Motorola-branded Binatone Hubble Cameras that could allow an attacker with physical access unauthorized access to the device. | 6.8 | More Details |
| CVE-2021-42274 | Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability | 6.8 | More Details |
| CVE-2021-42284 | Windows Hyper-V Denial of Service Vulnerability | 6.8 | More Details |
| CVE-2021-36315 | Dell EMC PowerScale Nodes contain a hardware design flaw. This may allow a local unauthenticated user to escalate privileges. This also affects Compliance mode and for Compliance mode clusters, is a critical vulnerability. Dell EMC recommends applying the workaround at your earliest opportunity. | 6.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3719 | A potential vulnerability in the SMI callback function that saves and restore boot script tables used for resuming from sleep state in some ThinkCentre and ThinkStation models may allow an attacker with local access and elevated privileges to execute arbitrary code. | 6.7 | More Details |
| CVE-2021-30264 | Possible use after free due improper validation of reference from call back to internal store table in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 6.7 | More Details |
| CVE-2021-3843 | A potential vulnerability in the SMI function to access EEPROM in some ThinkPad models may allow an attacker with local access and elevated privileges to execute arbitrary code. | 6.7 | More Details |
| CVE-2021-30265 | Possible memory corruption due to improper validation of memory address while processing user-space IOCTL for clearing Filter and Route statistics in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 6.7 | More Details |
| CVE-2021-41374 | Azure Sphere Information Disclosure Vulnerability | 6.7 | More Details |
| CVE-2021-30263 | Possible race condition can occur due to lack of synchronization mechanism when On-Device Logging node open twice concurrently in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music | 6.7 | More Details |
| CVE-2021-30266 | Possible use after free due to improper memory validation when initializing new interface via Interface add command in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking | 6.7 | More Details |
| CVE-2021-3599 | A potential vulnerability in the SMI callback function used to access flash device in some ThinkPad models may allow an attacker with local access and elevated privileges to execute arbitrary code. | 6.7 | More Details |
| CVE-2021-42303 | Azure RTOS Elevation of Privilege Vulnerability | 6.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42304 | Azure RTOS Elevation of Privilege Vulnerability | 6.6 | More Details |
| CVE-2021-42302 | Azure RTOS Elevation of Privilege Vulnerability | 6.6 | More Details |
| CVE-2021-36305 | Dell PowerScale OneFS contains an Unsynchronized Access to Shared Data in a Multithreaded Context in SMB CA handling. An authenticated user of SMB on a cluster with CA could potentially exploit this vulnerability, leading to a denial of service over SMB. | 6.5 | More Details |
| CVE-2021-3683 | showdoc is vulnerable to Cross-Site Request Forgery (CSRF) | 6.5 | More Details |
| CVE-2021-42305 | Microsoft Exchange Server Spoofing Vulnerability | 6.5 | More Details |
| CVE-2021-22959 | The parser in accepts requests with a space (SP) right after the header name before the colon. This can lead to HTTP Request Smuggling (HRS) in llhttp < v2.1.4 and < v6.0.6. | 6.5 | More Details |
| CVE-2021-38974 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 could allow an authenticated user to cause a denial of service using specially crafted HTTP requests. IBM X-Force ID: 212779. | 6.5 | More Details |
| CVE-2021-38975 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 could allow an authenticated user to to obtain sensitive information from a specially crafted HTTP request. IBM X-Force ID: 212780. | 6.5 | More Details |
| CVE-2021-3793 | An improper access control vulnerability was reported in some Motorola-branded Binatone Hubble Cameras which could allow an unauthenticated attacker on the same network as the device to access administrative pages that could result in information disclosure or device firmware update with verified firmware. | 6.5 | More Details |
| CVE-2021-3380 | Insecure direct object reference (IDOR) vulnerability in ICREM H8 SSRMS allows attackers to disclose sensitive information via the Print Invoice Functionality. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3791 | An information disclosure vulnerability was reported in some Motorola-branded Binatone Hubble Cameras that could allow an unauthenticated attacker on the same subnet to download an encrypted log file containing sensitive information such as WiFi SSID and password. | 6.5 | More Details |
| CVE-2021-41349 | Microsoft Exchange Server Spoofing Vulnerability | 6.5 | More Details |
| CVE-2021-21701 | Jenkins Performance Plugin 3.20 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. | 6.5 | More Details |
| CVE-2020-28137 | Cross site request forgery (CSRF) in Genexis Platinum 4410 V2-1.28, allows attackers to cause a denial of service by continuously restarting the router. | 6.5 | More Details |
| CVE-2021-3790 | A buffer overflow was reported in the local web server of some Motorola-branded Binatone Hubble Cameras that could allow an unauthenticated attacker on the same network to perform a denial-of-service attack against the device. | 6.5 | More Details |
| CVE-2021-38887 | IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information from application response requests that could be used in further attacks against the system. IBM X-Force ID: 209401. | 6.5 | More Details |
| CVE-2021-43576 | Jenkins pom2config Plugin 1.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks, allowing attackers with Overall/Read and Item/Read permissions to have Jenkins parse a crafted XML file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery. | 6.5 | More Details |
| CVE-2021-40518 | Airangel HSMX Gateway devices through 5.2.04 allow CSRF. | 6.5 | More Details |
| CVE-2021-41972 | Apache Superset up to and including 1.3.1 allowed for database connections password leak for authenticated users. This information could be accessed in a non-trivial way. | 6.5 | More Details |
| CVE-2021-43332 | In GNU Mailman before 2.1.36, the CSRF token for the Cgi/admindb.py admindb page contains an encrypted version of the list admin password. This could potentially be cracked by a moderator via an offline brute-force attack. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22870 | A path traversal vulnerability was identified in GitHub Pages builds on GitHub Enterprise Server that could allow an attacker to read system files. 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 3.3 and was fixed in versions 3.0.19, 3.1.11, and 3.2.3. This vulnerability was reported via the GitHub Bug Bounty program. | 6.5 | More Details |
| CVE-2021-3519 | A vulnerability was reported in some Lenovo Desktop models that could allow unauthorized access to the boot menu, when the "BIOS Password At Boot Device List" BIOS setting is Yes. | 6.4 | More Details |
| CVE-2021-3061 | An OS command injection vulnerability in the Palo Alto Networks PAN-OS command line interface (CLI) enables an authenticated administrator with access to the CLI to execute arbitrary OS commands to escalate privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20-h1; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14-h3; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11-h2; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8; PAN-OS 10.1 versions earlier than PAN-OS 10.1.3. Prisma Access customers that have Prisma Access 2.1 firewalls are impacted by this issue. | 6.4 | More Details |
| CVE-2021-39222 | Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Talk application was vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, a user would need to right-click on a malicious file and open the file in a new tab. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Talk application is upgraded to patched versions 10.0.7, 10.1.4, 11.1.2, 11.2.0 or 12.0.0. As a workaround, use a browser that has support for Content-Security-Policy. | 6.4 | More Details |
| CVE-2021-3787 | A vulnerability was reported in some Motorola-branded Binatone Hubble Cameras that could allow an attacker with local access to obtain the MQTT credentials that could result in unauthorized access to backend Hubble services. | 6.4 | More Details |
| CVE-2021-41289 | ASUS P453UJ contains the Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability. With a general user's permission, local attackers can modify the BIOS by replacing or filling in the content of the designated Memory DataBuffer, which causing a failure of integrity verification and further resulting in a failure to boot. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-25982 | In Factor (App Framework & Headless CMS) forum plugin, versions 1.3.5 to 1.8.30, are vulnerable to reflected Cross-Site Scripting (XSS) at the “search” parameter in the URL. An unauthenticated attacker can execute malicious JavaScript code and steal the session cookies. | 6.1 | More Details |
| CVE-2021-41368 | Microsoft Access Remote Code Execution Vulnerability | 6.1 | More Details |
| CVE-2020-14424 | Cacti before 1.2.18 allows remote attackers to trigger XSS via template import for the midwinter theme. | 6.1 | More Details |
| CVE-2021-41951 | ResourceSpace before 9.6 rev 18290 is affected by a reflected Cross-Site Scripting vulnerability in plugins/wordpress_sso/pages/index.php via the wordpress_user parameter. If an attacker is able to persuade a victim to visit a crafted URL, malicious JavaScript content may be executed within the context of the victim's browser. | 6.1 | More Details |
| CVE-2021-42838 | Grand Vice info Co. webopac7 book search field parameter does not properly restrict the input of special characters, thus unauthenticated attackers can inject JavaScript syntax remotely, and further perform reflective XSS attacks. | 6.1 | More Details |
| CVE-2021-25984 | In Factor (App Framework & Headless CMS) forum plugin, versions v1.3.3 to v1.8.30, are vulnerable to stored Cross-Site Scripting (XSS) at the “post reply” section. An unauthenticated attacker can execute malicious JavaScript code and steal the session cookies. | 6.1 | More Details |
| CVE-2021-25983 | In Factor (App Framework & Headless CMS) forum plugin, versions v1.3.8 to v1.8.30, are vulnerable to reflected Cross-Site Scripting (XSS) at the “tags” and “category” parameters in the URL. An unauthenticated attacker can execute malicious JavaScript code and steal the session cookies. | 6.1 | More Details |
| CVE-2021-3945 | django-helpdesk is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 6.1 | More Details |
| CVE-2021-33618 | Dolibarr ERP and CRM 13.0.2 allows XSS via object details, as demonstrated by > and < characters in the onpointermove attribute of a BODY element to the user-management feature. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-21639 | Ruijie RG-UAC 6000-E50 commit 9071227 was discovered to contain a cross-site scripting (XSS) vulnerability via the rule_name parameter. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload. | 6.1 | More Details |
| CVE-2021-43574 | WebAdmin Control Panel in Atmail 6.5.0 (a version released in 2012) allows XSS via the format parameter to the default URI. NOTE: This vulnerability only affects products that are no longer supported by the maintainer | 6.1 | More Details |
| CVE-2021-43331 | In GNU Mailman before 2.1.36, a crafted URL to the Cgi/options.py user options page can execute arbitrary JavaScript for XSS. | 6.1 | More Details |
| CVE-2021-41038 | In versions of the @theia/plugin-ext component of Eclipse Theia prior to 1.18.0, Webview contents can be hijacked via postMessage(). | 6.1 | More Details |
| CVE-2021-41427 | Beeline Smart Box 2.0.38 is vulnerable to Cross Site Scripting (XSS) via the choose_mac parameter to setup.cgi. | 6.1 | More Details |
| CVE-2021-42300 | Azure Sphere Tampering Vulnerability | 6.0 | More Details |
| CVE-2021-3908 | OctoRPKI does not limit the depth of a certificate chain, allowing for a CA to create children in an ad-hoc fashion, thereby making tree traversal never end. | 5.9 | More Details |
| CVE-2021-38978 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 212783. | 5.9 | More Details |
| CVE-2021-42288 | Windows Hello Security Feature Bypass Vulnerability | 5.7 | More Details |
| CVE-2021-3572 | A flaw was found in python-pip in the way it handled Unicode separators in git references. A remote attacker could possibly use this issue to install a different revision on a repository. The highest threat from this vulnerability is to data integrity. This is fixed in python-pip version 21.1. | 5.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3915 | bookstack is vulnerable to Unrestricted Upload of File with Dangerous Type | 5.7 | More Details |
| CVE-2020-23884 | A buffer overflow in Nomacs v3.15.0 allows attackers to cause a denial of service (DoS) via a crafted MNG file. | 5.5 | More Details |
| CVE-2020-23888 | A User Mode Write AV in Editor!TMethodImplementationIntercept+0x53f6c3 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted psd file. | 5.5 | More Details |
| CVE-2020-23894 | A User Mode Write AV in ntdll!RtlpCoalesceFreeBlocks+0x268 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tiff file. | 5.5 | More Details |
| CVE-2020-23893 | A User Mode Write AV in Editor!TMethodImplementationIntercept+0x3c3682 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tiff file. | 5.5 | More Details |
| CVE-2021-38976 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 stores user credentials in plain clear text which can be read by a local user. X-Force ID: 212781. | 5.5 | More Details |
| CVE-2020-23891 | A User Mode Write AV in Editor+0x5cd7 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tiff file. | 5.5 | More Details |
| CVE-2021-42373 | A NULL pointer dereference in Busybox's man applet leads to denial of service when a section name is supplied but no page argument is given | 5.5 | More Details |
| CVE-2020-23890 | A buffer overflow in WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted JPG file. Related to Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at JPGCodec+0x753648. | 5.5 | More Details |
| CVE-2020-23889 | A User Mode Write AV starting at Editor!TMethodImplementationIntercept+0x4189c6 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted ico file. | 5.5 | More Details |
| CVE-2021-32022 | A low privileged delete vulnerability using CEF RPC server of BlackBerry Protect for Windows version(s) versions 1574 and earlier could allow an attacker to potentially execute code in the context of a BlackBerry Cylance service that has admin rights on the system and gaining the ability to delete data from the local system. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-23887 | XnView MP v0.96.4 was discovered to contain a heap overflow which allows attackers to cause a denial of service (DoS) via a crafted ico file. Related to a Read Access Violation starting at USER32!SmartStretchDIBits+0x33. | 5.5 | More Details |
| CVE-2021-42277 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability | 5.5 | More Details |
| CVE-2021-41379 | Windows Installer Elevation of Privilege Vulnerability | 5.5 | More Details |
| CVE-2020-23886 | XnView MP v0.96.4 was discovered to contain a heap overflow which allows attackers to cause a denial of service (DoS) via a crafted pict file. Related to a User Mode Write AV starting at ntdll!RtlpLowFragHeapFree. | 5.5 | More Details |
| CVE-2020-12960 | AMD Graphics Driver for Windows 10, amdfender.sys may improperly handle input validation on InputBuffer which may result in a denial of service (DoS). | 5.5 | More Details |
| CVE-2020-12905 | Out of Bounds Read in AMD Graphics Driver for Windows 10 in Escape 0x3004403 may lead to arbitrary information disclosure. | 5.5 | More Details |
| CVE-2020-12901 | Arbitrary Free After Use in AMD Graphics Driver for Windows 10 may lead to KASLR bypass or information disclosure. | 5.5 | More Details |
| CVE-2021-42280 | Windows Feedback Hub Elevation of Privilege Vulnerability | 5.5 | More Details |
| CVE-2021-42111 | An issue was discovered in the RCDevs OpenOTP app 1.4.13 and 1.4.14 for iOS. If it is installed on a jailbroken device, it is possible to retrieve the PIN code used to access the application. The IOS app version 1.4.1631262629 resolves this issue by storing a hash PIN code. | 5.5 | More Details |
| CVE-2020-23895 | A User Mode Write AV in Editor+0x76af of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tiff file. | 5.5 | More Details |
| CVE-2020-23906 | FFmpeg N-98388-g76a3ee996b allows attackers to cause a denial of service (DoS) via a crafted audio file due to insufficient verification of data authenticity. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-23896 | A User Mode Write AV in Editor+0x576b of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tiff file. | 5.5 | More Details |
| CVE-2020-23897 | A User Mode Write AV in Editor!TMethodImplementationIntercept+0x54dcec of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tga file. | 5.5 | More Details |
| CVE-2021-26329 | AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. | 5.5 | More Details |
| CVE-2021-3720 | An information disclosure vulnerability was reported in the Time Weather system widget on Legion Phone Pro (L79031) and Legion Phone2 Pro (L70081) that could allow other applications to access device GPS data. | 5.5 | More Details |
| CVE-2021-42376 | A NULL pointer dereference in Busybox's hush applet leads to denial of service when processing a crafted shell command, due to missing validation after a \x03 delimiter character. This may be used for DoS under very rare conditions of filtered command input. | 5.5 | More Details |
| CVE-2020-12954 | A side effect of an integrated chipset option may be able to be used by an attacker to bypass SPI ROM protections, allowing unauthorized SPI ROM modification. | 5.5 | More Details |
| CVE-2021-26312 | Failure to flush the Translation Lookaside Buffer (TLB) of the I/O memory management unit (IOMMU) may lead an IO device to write to memory it should not be able to access, resulting in a potential loss of integrity. | 5.5 | More Details |
| CVE-2021-38949 | IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. | 5.5 | More Details |
| CVE-2021-41373 | FSLogix Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2021-26320 | Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP | 5.5 | More Details |
| CVE-2021-26321 | Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-12488 | The attacker can access the sensitive information stored within the jovi Smart Scene module by entering carefully constructed commands without requesting permission. | 5.5 | More Details |
| CVE-2021-26325 | Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. | 5.5 | More Details |
| CVE-2021-26327 | Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. | 5.5 | More Details |
| CVE-2021-26330 | AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. | 5.5 | More Details |
| CVE-2021-26336 | Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. | 5.5 | More Details |
| CVE-2021-26337 | Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. | 5.5 | More Details |
| CVE-2020-23904 | A stack buffer overflow in speexenc.c of Speex v1.2 allows attackers to cause a denial of service (DoS) via a crafted WAV file. NOTE: the vendor states "I cannot reproduce it" and it "is a demo program. | 5.5 | More Details |
| CVE-2020-23903 | A Divide by Zero vulnerability in the function static int read_samples of Speex v1.2 allows attackers to cause a denial of service (DoS) via a crafted WAV file. | 5.5 | More Details |
| CVE-2020-23902 | A buffer overflow in WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tga file. Related to Data from Faulting Address may be used as a return value starting at Editor!TMethodImplementationIntercept+0x528a3. | 5.5 | More Details |
| CVE-2020-23901 | A User Mode Write AV in Editor+0x5d15 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tga file. | 5.5 | More Details |
| CVE-2020-12897 | Kernel Pool Address disclosure in AMD Graphics Driver for Windows 10 may lead to KASLR bypass. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-23900 | A buffer overflow in WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tga file. Related to Data from Faulting Address controls Code Flow starting at Editor!TMethodImplementationIntercept+0x57a3b. | 5.5 | More Details |
| CVE-2020-23899 | A User Mode Write AV in Editor+0x5f91 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tga file. | 5.5 | More Details |
| CVE-2020-23898 | A User Mode Write AV in Editor+0x5ea2 of WildBit Viewer v6.6 allows attackers to cause a denial of service (DoS) via a crafted tga file. | 5.5 | More Details |
| CVE-2020-12904 | Out of Bounds Read in AMD Graphics Driver for Windows 10 in Escape 0x3004203 may lead to arbitrary information disclosure. | 5.5 | More Details |
| CVE-2020-12920 | A potential denial of service issue exists in the AMD Display driver Escape 0x130007 Call handler. An attacker with low privilege could potentially induce a Windows BugCheck. | 5.5 | More Details |
| CVE-2021-42375 | An incorrect handling of a special element in Busybox's ash applet leads to denial of service when processing a crafted shell command, due to the shell mistaking specific characters for reserved characters. This may be used for DoS under rare conditions of filtered command input. | 5.5 | More Details |
| CVE-2021-3938 | snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 5.4 | More Details |
| CVE-2021-25974 | In Publify, versions v8.0 to v9.2.4 are vulnerable to stored XSS. A user with a “publisher” role is able to inject and execute arbitrary JavaScript code while creating a page/article. | 5.4 | More Details |
| CVE-2021-3776 | showdoc is vulnerable to Cross-Site Request Forgery (CSRF) | 5.4 | More Details |
| CVE-2021-43561 | An XSS issue was discovered in the google_for_jobs (aka Google for Jobs) extension before 1.5.1 and 2.x before 2.1.1 for TYPO3. The extension fails to properly encode user input for output in HTML context. A TYPO3 backend user account is required to exploit the vulnerability. | 5.4 | More Details |
| CVE-2021-21699 | Jenkins Active Choices Plugin 2.5.6 and earlier does not escape the parameter name of reactive parameters and dynamic reference parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42703 | This vulnerability could allow an attacker to send malicious Javascript code resulting in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage, and performing unintended browser action. | 5.4 | More Details |
| CVE-2021-21700 | Jenkins Scriptler Plugin 3.3 and earlier does not escape the name of scripts on the UI when asking to confirm their deletion, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by exploitable by attackers able to create Scriptler scripts. | 5.4 | More Details |
| CVE-2020-4140 | IBM Security SiteProtector System 3.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174052. | 5.4 | More Details |
| CVE-2021-25975 | In publify, versions v8.0 to v9.2.4 are vulnerable to stored XSS as a result of an unrestricted file upload. This issue allows a user with "publisher" role to inject malicious JavaScript via the uploaded html file. | 5.4 | More Details |
| CVE-2021-38982 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 212791. | 5.4 | More Details |
| CVE-2021-40517 | Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. | 5.4 | More Details |
| CVE-2021-3775 | showdoc is vulnerable to Cross-Site Request Forgery (CSRF) | 5.4 | More Details |
| CVE-2021-1903 | Possible denial of service scenario can occur due to lack of length check on Channel Switch Announcement IE in beacon or probe response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking | 5.3 | More Details |
| CVE-2021-3792 | Some device communications in some Motorola-branded Binatone Hubble Cameras with backend Hubble services are not encrypted which could lead to the communication channel being accessible by an attacker. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42374 | An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when crafted LZMA-compressed input is decompressed. This can be triggered by any applet/format that | 5.3 | More Details |
| CVE-2020-4146 | IBM Security SiteProtector System 3.1.1 could allow a remote attacker to obtain sensitive information, caused by missing 'HttpOnly' flag. A remote attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 174129. | 5.3 | More Details |
| CVE-2021-38981 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 212788. | 5.3 | More Details |
| CVE-2021-40504 | A certain template role in SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, contains transport authorizations, which exceed expected display only permissions. | 4.9 | More Details |
| CVE-2021-41271 | Discourse is a platform for community discussion. In affected versions a maliciously crafted request could cause an error response to be cached by intermediate proxies. This could cause a loss of confidentiality for some content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. | 4.8 | More Details |
| CVE-2021-34582 | In Phoenix Contact FL MGUARD 1102 and 1105 in Versions 1.4.0, 1.4.1 and 1.5.0 a user with high privileges can inject HTML code (XSS) through web-based management or the REST API with a manipulated certificate file. | 4.8 | More Details |
| CVE-2021-42319 | Visual Studio Elevation of Privilege Vulnerability | 4.7 | More Details |
| CVE-2021-34420 | The Zoom Client for Meetings for Windows installer before version 5.5.4 does not properly verify the signature of files with .msi, .ps1, and .bat extensions. This could lead to a malicious actor installing malicious software on a customer’s computer. | 4.7 | More Details |
| CVE-2021-38882 | IBM Spectrum Scale 5.1.0 through 5.1.1.1 could allow a privileged admin to destroy filesystem audit logging records before expiration time. IBM X-Force ID: 209164. | 4.4 | More Details |
| CVE-2021-38631 | Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability | 4.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41375 | Azure Sphere Information Disclosure Vulnerability | 4.4 | More Details |
| CVE-2021-41371 | Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability | 4.4 | More Details |
| CVE-2021-3909 | OctoRPKI does not limit the length of a connection, allowing for a slowloris DOS attack to take place which makes OctoRPKI wait forever. Specifically, the repository that OctoRPKI sends HTTP requests to will keep the connection open for a day before a response is returned, but does keep drip feeding new bytes to keep the connection alive. | 4.4 | More Details |
| CVE-2021-3910 | OctoRPKI crashes when encountering a repository that returns an invalid ROA (just an encoded NUL (\0) character). | 4.4 | More Details |
| CVE-2021-3786 | A potential vulnerability in the SMI callback function used in CSME configuration of some Lenovo Notebook and ThinkPad systems could be used to leak out data out of the SMRAM range. | 4.4 | More Details |
| CVE-2021-3718 | A denial of service vulnerability was reported in some ThinkPad models that could cause a system to crash when the Enhanced Biometrics setting is enabled in BIOS. | 4.3 | More Details |
| CVE-2021-42062 | SAP ERP HCM Portugal does not perform necessary authorization checks for a report that reads the payroll data of employees in a certain area. Since the affected report only reads the payroll information, the attacker can neither modify any information nor cause availability impacts. | 4.3 | More Details |
| CVE-2021-42337 | The permission control of AIFU cashier management salary query function can be bypassed, thus after obtaining general user’s permission, the remote attacker can access account information except passwords by crafting URL parameters. | 4.3 | More Details |
| CVE-2021-38985 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. | 4.3 | More Details |
| CVE-2021-38972 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-41229 | BlueZ is a Bluetooth protocol stack for Linux. In affected versions a vulnerability exists in sdp_cstate_alloc_buf which allocates memory which will always be hung in the singly linked list of cstates and will not be freed. This will cause a memory leak over time. The data can be a very large object, which can be caused by an attacker continuously sending sdp packets and this may cause the service of the target device to crash. | 4.3 | More Details |
| CVE-2021-3921 | firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) | 4.3 | More Details |
| CVE-2021-41351 | Microsoft Edge (Chrome based) Spoofing on IE Mode | 4.3 | More Details |
| CVE-2021-3931 | snipe-it is vulnerable to Cross-Site Request Forgery (CSRF) | 4.3 | More Details |
| CVE-2021-38977 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 212782. | 4.3 | More Details |
| CVE-2021-3932 | twill is vulnerable to Cross-Site Request Forgery (CSRF) | 4.3 | More Details |
| CVE-2021-3911 | If the ROA that a repository returns contains too many bits for the IP address then OctoRPKI will crash. | 4.2 | More Details |
| CVE-2021-3912 | OctoRPKI tries to load the entire contents of a repository in memory, and in the case of a GZIP bomb, unzip it in memory, making it possible to create a repository that makes OctoRPKI run out of memory (and thus crash). | 4.2 | More Details |
| CVE-2021-42279 | Chakra Scripting Engine Memory Corruption Vulnerability | 4.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3789 | An information disclosure vulnerability was reported in some Motorola-branded Binatone Hubble Cameras that could allow an attacker with physical access to obtain the encryption key used to decrypt firmware update packages. | 4.2 | More Details |
| CVE-2021-34418 | The login routine of the web console in the Zoom On-Premise Meeting Connector before version 4.6.239.20200613, Zoom On-Premise Meeting Connector MMR before version 4.6.239.20200613, Zoom On-Premise Recording Connector before version 3.8.42.20200905, Zoom On-Premise Virtual Room Connector before version 4.4.6344.20200612, and Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5492.20200616 fails to validate that a NULL byte was sent while authenticating. This could lead to a crash of the login service. | 4.0 | More Details |
| CVE-2021-34421 | The Keybase Client for Android before version 5.8.0 and the Keybase Client for iOS before version 5.8.0 fails to properly remove exploded messages initiated by a user if the receiving user places the chat session in the background while the sending user explodes the messages. This could lead to disclosure of sensitive information which was meant to be deleted from the customer's device. | 3.7 | More Details |
| CVE-2021-37910 | ASUS routers Wi-Fi protected access protocol (WPA2 and WPA3-SAE) has improper control of Interaction frequency vulnerability, an unauthenticated attacker can remotely disconnect other users' connections by sending specially crafted SAE authentication frames. | 3.7 | More Details |
| CVE-2021-34419 | In the Zoom Client for Meetings for Ubuntu Linux before version 5.1.0, there is an HTML injection flaw when sending a remote control request to a user in the process of in-meeting screen sharing. This could allow meeting participants to be targeted for social engineering attacks. | 3.7 | More Details |
| CVE-2021-42301 | Azure RTOS Information Disclosure Vulnerability | 3.3 | More Details |
| CVE-2021-43273 | An Out-of-bounds Read vulnerability exists in the DGN file reading procedure in Open Design Alliance Drawings SDK before 2022.11. Crafted data in a DGN file and lack of verification of input data can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 3.3 | More Details |
| CVE-2021-26444 | Azure RTOS Information Disclosure Vulnerability | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42323 | Azure RTOS Information Disclosure Vulnerability | 3.3 | More Details |
| CVE-2021-38973 | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. | 2.7 | More Details |
| CVE-2021-41376 | Azure Sphere Information Disclosure Vulnerability | 2.3 | More Details |
| CVE-2021-41259 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: None. Reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. Notes: None. | N/A | More Details |
| CVE-2021-30216 | 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 in a customer-controlled product. Notes: none | N/A | More Details |