SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 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-2021-41277	Metabase is an open source data analytics platform. In affected versions a security issue has been discovered with the custom GeoJSON map (`admin->settings->maps->custom maps->add a map`) support and potential local file inclusion (including environment variables). URLs were not validated prior to being loaded. This issue is fixed in a new maintenance release (0.40.5 and 1.40.5), and any subsequent release after that. If you're unable to upgrade immediately, you can mitigate this by including rules in your reverse proxy or load balancer or WAF to provide a validation filter before the application.	10.0	More Details
CVE-2021-41931	The Company's Recruitment Management System in id=2 of the parameter from view_vacancy app on-page appears to be vulnerable to SQL injection. The payloads 19424269' or '1309'='1309 and 39476597' or '2917'='2923 were each submitted in the id parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41435	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request.	9.8	More Details
CVE-2021-42784	OS Command Injection vulnerability in debug_fcgi of D-Link DWR-932C E1 firmware allows a remote attacker to perform command injection via a crafted HTTP request.	9.8	More Details
CVE-2021-42783	Missing Authentication for Critical Function vulnerability in debug_post_set.cgi of D-Link DWR-932C E1 firmware allows an unauthenticated attacker to execute administrative actions.	9.8	More Details
CVE-2021-37022	There is a Heap-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause root permission which can be escalated.	9.8	More Details
CVE-2021-44143	A flaw was found in mbsync in isync 1.4.0 through 1.4.3. Due to an unchecked condition, a malicious or compromised IMAP server could use a crafted mail message that lacks headers (i.e., one that starts with an empty line) to provoke a heap overflow, which could conceivably be exploited for remote code execution.	9.8	More Details
CVE-2021-3943	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A remote code execution risk when restoring backup files was identified.	9.8	More Details
CVE-2021-44079	In the wazuh-slack active response script in Wazuh 4.2.x before 4.2.5, untrusted user agents are passed to a curl command line, potentially resulting in remote code execution.	9.8	More Details
CVE-2021-41280	Sharetribe Go is a source available marketplace software. In affected versions operating system command injection is possible on installations of Sharetribe Go, that do not have a secret AWS Simple Notification Service (SNS) notification token configured via the `sns_notification_token` configuration parameter. This configuration parameter is unset by default. The vulnerability has been patched in version 10.2.1. Users who are unable to upgrade should set the`sns_notification_token` configuration parameter to a secret value.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40391	An out-of-bounds write vulnerability exists in the drill format T-code tool number functionality of Gerbv 2.7.0, dev (commit b5f1eacd), and the forked version of Gerbv (commit 71493260). A specially-crafted drill file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-32234	SmarterTools SmarterMail 16.x through 100.x before 100.0.7803 allows remote code execution.	9.8	More Details
CVE-2021-37592	Suricata before 5.0.8 and 6.x before 6.0.4 allows TCP evasion via a client with a crafted TCP/IP stack that can send a certain sequence of segments.	9.8	More Details
CVE-2021-42785	Buffer Overflow vulnerability in tvnviewer.exe of TightVNC Viewer allows a remote attacker to execute arbitrary instructions via a crafted FramebufferUpdate packet from a VNC server.	9.8	More Details
CVE-2021-36372	In Apache Ozone versions prior to 1.2.0, Initially generated block tokens are persisted to the metadata database and can be retrieved with authenticated users with permission to the key. Authenticated users may use them even after access is revoked.	9.8	More Details
CVE-2021-42338	4MOSAn GCB Doctor’s login page has improper validation of Cookie, which allows an unauthenticated remote attacker to bypass authentication by code injection in cookie, and arbitrarily manipulate the system or interrupt services by upload and execution of arbitrary files.	9.8	More Details
CVE-2021-44026	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to a potential SQL injection via search or search_params.	9.8	More Details
CVE-2021-27023	A flaw was discovered in Puppet Agent and Puppet Server that may result in a leak of HTTP credentials when following HTTP redirects to a different host. This is similar to CVE-2018-1000007	9.8	More Details
CVE-2021-43996	The Ignition component before 1.16.15, and 2.0.x before 2.0.6, for Laravel has a "fix variable names" feature that can lead to incorrect access control.	9.8	More Details
CVE-2021-38002	Use after free in Web Transport in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41274	solidus_auth_devise provides authentication services for the Solidus webstore framework, using the Devise gem. In affected versions solidus_auth_devise is subject to a CSRF vulnerability that allows user account takeover. All applications using any version of the frontend component of `solidus_auth_devise` are affected if `protect_from_forgery` method is both: Executed whether as: A `before_action` callback (the default) or A `prepend_before_action` (option `prepend: true` given) before the `:load_object` hook in `Spree::UserController` (most likely order to find). Configured to use `:null_session` or `:reset_session` strategies (`:null_session` is the default in case the no strategy is given, but `rails --new` generated skeleton use `:exception`). Users should promptly update to `solidus_auth_devise` version `2.5.4`. Users unable to update should if possible, change their strategy to `:exception`. Please see the linked GHSA for more workaround details.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41275	spree_auth_devise is an open source library which provides authentication and authorization services for use with the Spree storefront framework by using an underlying Devise authentication framework. In affected versions spree_auth_devise is subject to a CSRF vulnerability that allows user account takeover. All applications using any version of the frontend component of spree_auth_devise are affected if protect_from_forgery method is both: Executed whether as: A before_action callback (the default). A prepend_before_action (option prepend: true given) before the :load_object hook in Spree::UserController (most likely order to find). Configured to use :null_session or :reset_session strategies (:null_session is the default in case the no strategy is given, but rails --new generated skeleton use :exception). Users are advised to update their spree_auth_devise gem. For users unable to update it may be possible to change your strategy to :exception. Please see the linked GHSA for more workaround details. ### Impact CSRF vulnerability that allows user account takeover. All applications using any version of the frontend component of `spree_auth_devise` are affected if `protect_from_forgery` method is both: * Executed whether as: * A before_action callback (the default) * A prepend_before_action (option prepend: true given) before the :load_object hook in Spree::UserController (most likely order to find). * Configured to use :null_session or :reset_session strategies (:null_session is the default in case the no strategy is given, but rails --new generated skeleton use :exception). That means that applications that haven't been configured differently from what it's generated with Rails aren't affected. Thanks @waiting-for-dev for reporting and providing a patch ﷺ ### Patches Spree 4.3 users should update to spree_auth_devise 4.4.1 Spree 4.2 users should update to spree_auth_devise 4.2.1 ### Workarounds If possible, change your strategy to :exception: ```ruby class ApplicationController < ActionController::Base protect_from_forgery with: :exception end ``` Add the following to`config/application.rb `to at least run the `:exception` strategy on the affected controller: ```ruby config.after_initialize do Spree::UsersController.protect_from_forgery with: :exception end ``` ### References https://github.com/solidusio/solidus_auth_devise/security/advisories/GHSA-xm34-v85h-9pg2	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43409	The “WPO365	LOGIN” WordPress plugin (up to and including version 15.3) by wpo365.com is vulnerable to a persistent Cross-Site Scripting (XSS) vulnerability (also known as Stored or Second-Order XSS). Persistent XSS vulnerabilities occur when the application stores and retrieves client supplied data without proper handling of dangerous content. This type of XSS vulnerability is exploited by submitting malicious script content to the application which is then retrieved and executed by other application users. The attacker could exploit this to conduct a range of attacks against users of the affected application such as session hijacking, account take over and accessing sensitive data. In this case, the XSS payload can be submitted by any anonymous user, the payload then renders and executes when a WordPress administrator authenticates and accesses the WordPress Dashboard. The injected payload can carry out actions on behalf of the administrator including adding other administrative users and changing application settings. This flaw could be exploited to ultimately provide full control of the affected system to the attacker.	9.3	More Details
CVE-2021-39233	In Apache Ozone versions prior to 1.2.0, Container related Datanode requests of Ozone Datanode were not properly authorized and can be called by any client.	9.1	More Details
CVE-2021-36312	Dell EMC CloudLink 7.1 and all prior versions contain a Hard-coded Password Vulnerability. A remote high privileged attacker, with the knowledge of the hard-coded credentials, may potentially exploit this vulnerability to gain unauthorized access to the system.	9.1	More Details
CVE-2021-36313	Dell EMC CloudLink 7.1 and all prior versions contain an OS command injection Vulnerability. A remote high privileged attacker, may potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker. This vulnerability is considered critical as it may be leveraged to completely compromise the vulnerable application as well as the underlying operating system. Dell recommends customers to upgrade at the earliest opportunity.	9.1	More Details
CVE-2021-44144	Croatia Control Asterix 2.8.1 has a heap-based buffer over-read, with additional details to be disclosed at a later date.	9.1	More Details
CVE-2021-37016	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause Information Disclosure or Denial of Service.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39231	In Apache Ozone versions prior to 1.2.0, Various internal server-to-server RPC endpoints are available for connections, making it possible for an attacker to download raw data from Datanode and Ozone manager and modify Ratis replication configuration.	9.1	More Details
CVE-2021-22028	In versions of Greenplum database prior to 5.28.6 and 6.14.0, greenplum database contains a file path traversal vulnerability leading to information disclosure from the file system. A malicious user can read/write information from the file system using this vulnerability.	9.1	More Details
CVE-2021-23732	This affects all versions of package docker-cli-js. If the command parameter of the Docker.command method can at least be partially controlled by a user, they will be in a position to execute any arbitrary OS commands on the host system.	9.0	More Details
CVE-2021-23155	Improper validation of the cloud certificate chain in Mobile Client allows man-in-the-middle attack to impersonate the legitimate Command Centre Server. This issue affects: Gallagher Command Centre Mobile Client for Android 8.60 versions prior to 8.60.065; version 8.50 and prior versions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-0071	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2021-36307	Networking OS10, versions prior to October 2021 with RESTCONF API enabled, contains a privilege escalation vulnerability. A malicious low privileged user with specific access to the API could potentially exploit this vulnerability to gain admin privileges on the affected system.	8.8	More Details
CVE-2021-39353	The Easy Registration Forms WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the ajax_add_form function found in the ~/includes/class-form.php file which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 2.1.1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37102	There is a command injection vulnerability in CMA service module of FusionCompute product when processing the default certificate file. The software constructs part of a command using external special input from users, but the software does not sufficiently validate the user input. Successful exploit could allow the attacker to inject certain commands to the system. Affected product versions include: FusionCompute 6.0.0, 6.3.0, 6.3.1, 6.5.0, 6.5.1, 8.0.0.	8.8	More Details
CVE-2021-22053	Applications using both `spring-cloud-netflix-hystrix-dashboard` and `spring-boot-starter-thymeleaf` expose a way to execute code submitted within the request URI path during the resolution of view templates. When a request is made at `/hystrix/monitor;[user-provided data]`, the path elements following `hystrix/monitor` are being evaluated as SpringEL expressions, which can lead to code execution.	8.8	More Details
CVE-2021-43581	An Out-of-Bounds Read vulnerability exists when reading a U3D file using Open Design Alliance PRC SDK before 2022.11. The specific issue exists within the parsing of U3D files. Incorrect use of the LibJpeg source manager inside the U3D library, and crafted data in a U3D file, 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.	8.8	More Details
CVE-2021-39236	In Apache Ozone before 1.2.0, Authenticated users with valid Ozone S3 credentials can create specific OM requests, impersonating any other user.	8.8	More Details
CVE-2021-39232	In Apache Ozone versions prior to 1.2.0, certain admin related SCM commands can be executed by any authenticated users, not just by admins.	8.8	More Details
CVE-2021-24892	Insecure Direct Object Reference in edit function of Advanced Forms (Free & Pro) before 1.6.9 allows authenticated remote attacker to change arbitrary user's email address and request for reset password, which could lead to take over of WordPress's administrator account. To exploit this vulnerability, an attacker must register to obtain a valid WordPress's user and use such user to authenticate with WordPress in order to exploit the vulnerable edit function.	8.8	More Details
CVE-2021-42362	The WordPress Popular Posts WordPress plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/src/Image.php file which makes it possible for attackers with contributor level access and above to upload malicious files that can be used to obtain remote code execution, in versions up to and including 5.3.2.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44036	Team Password Manager (aka TeamPasswordManager) before 10.135.236 has a CSRF vulnerability during import.	8.8	More Details
CVE-2021-21899	A code execution vulnerability exists in the dwgCompressor::copyCompBytes21 functionality of LibreCad libdxfrw 2.2.0-rc2-19-ge02f3580. A specially-crafted .dwg file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-21900	A code execution vulnerability exists in the dxfRW::processLType() functionality of LibreCad libdxfrw 2.2.0-rc2-19-ge02f3580. A specially-crafted .dxf file can lead to a use-after-free vulnerability. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-22966	Privilege escalation from Editor to Admin using Groups in Concrete CMS versions 8.5.6 and below. If a group is granted "view" permissions on the bulkupdate page, then users in that group can escalate to being an administrator with a specially crafted curl. Fixed by adding a check for group permissions before allowing a group to be moved. Concrete CMS Security team CVSS scoring: 7.1 AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:HCredit for discovery: "Adrian Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/)"This fix is also in Concrete version 9.0.0	8.8	More Details
CVE-2021-36908	Cross-Site Request Forgery (CSRF) vulnerability in WebFactory Ltd. WP Reset PRO plugin <= 5.98 versions.	8.8	More Details
CVE-2021-21898	A code execution vulnerability exists in the dwgCompressor::decompress18() functionality of LibreCad libdxfrw 2.2.0-rc2-19-ge02f3580. A specially-crafted .dwg file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-43559	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. The "delete related badge" functionality did not include the necessary token check to prevent a CSRF risk.	8.8	More Details
CVE-2021-37997	Use after free in Sign-In in Google Chrome prior to 95.0.4638.69 allowed a remote attacker who convinced a user to sign into Chrome to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24847	The importFromRedirection AJAX action of the SEO Redirection Plugin – 301 Redirect Manager WordPress plugin before 8.2, available to any authenticated user, does not properly sanitise the offset parameter before using it in a SQL statement, leading an SQL injection when the redirection plugin is also installed	8.8	More Details
CVE-2021-38003	Inappropriate implementation in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-24758	The Email Log WordPress plugin before 2.4.7 does not properly validate, sanitise and escape the "orderby" and "order" GET parameters before using them in SQL statement in the admin dashboard, leading to SQL injections	8.8	More Details
CVE-2021-37998	Use after free in Garbage Collection in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-28710	certain VT-d IOMMUs may not work in shared page table mode For efficiency reasons, address translation control structures (page tables) may (and, on suitable hardware, by default will) be shared between CPUs, for second-level translation (EPT), and IOMMUs. These page tables are presently set up to always be 4 levels deep. However, an IOMMU may require the use of just 3 page table levels. In such a configuration the lop level table needs to be stripped before inserting the root table's address into the hardware pagetable base register. When sharing page tables, Xen erroneously skipped this stripping. Consequently, the guest is able to write to leaf page table entries.	8.8	More Details
CVE-2021-38001	Type confusion in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-24804	The Simple JWT Login WordPress plugin before 3.2.1 does not have nonce checks when saving its settings, allowing attackers to make a logged in admin changed them. Settings such as HMAC verification secret, account registering and default user roles can be updated, which could result in site takeover.	8.8	More Details
CVE-2021-24772	The Stream WordPress plugin before 3.8.2 does not sanitise and validate the order GET parameter from the Stream Records admin dashboard before using it in a SQL statement, leading to an SQL injection issue.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36909	Authenticated Database Reset vulnerability in WordPress WP Reset PRO Premium plugin (versions <= 5.98) allows any authenticated user to wipe the entire database regardless of their authorization. It leads to a complete website reset and takeover.	8.8	More Details
CVE-2021-43775	Aim is an open-source, self-hosted machine learning experiment tracking tool. Versions of Aim prior to 3.1.0 are vulnerable to a path traversal attack. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. The vulnerability issue is resolved in Aim v3.1.0.	8.6	More Details
CVE-2021-0180	Uncontrolled resource consumption in the Intel(R) HAXM software before version 7.6.6 may allow an unauthenticated user to potentially enable privilege escalation via local access.	8.4	More Details
CVE-2021-41165	CKEditor4 is an open source WYSIWYG HTML editor. In affected version a vulnerability has been discovered in the core HTML processing module and may affect all plugins used by CKEditor 4. The vulnerability allowed to inject malformed comments HTML bypassing content sanitization, which could result in executing JavaScript code. It affects all users using the CKEditor 4 at version < 4.17.0. The problem has been recognized and patched. The fix will be available in version 4.17.0.	8.2	More Details
CVE-2021-41164	CKEditor4 is an open source WYSIWYG HTML editor. In affected versions a vulnerability has been discovered in the Advanced Content Filter (ACF) module and may affect all plugins used by CKEditor 4. The vulnerability allowed to inject malformed HTML bypassing content sanitization, which could result in executing JavaScript code. It affects all users using the CKEditor 4 at version < 4.17.0. The problem has been recognized and patched. The fix will be available in version 4.17.0.	8.2	More Details
CVE-2021-23193	Improper privilege validation vulnerability in COM Interface of Gallagher Command Centre Server allows authenticated unprivileged operators to retrieve sensitive information from the Command Centre Server. This issue affects: Gallagher Command Centre 8.50 versions prior to 8.50.2048 (MR3) ; 8.40 versions prior to 8.40.2063 (MR4); 8.30 versions prior to 8.30.1454 (MR4) ; 8.20 versions prior to 8.20.1291 (MR6); version 8.10 and prior versions.	8.1	More Details
CVE-2021-3935	When PgBouncer is configured to use "cert" authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of TLS certificate verification and encryption. This flaw affects PgBouncer versions prior to 1.16.1.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23167	Improper certificate validation vulnerability in SMTP Client allows man-in-the-middle attack to retrieve sensitive information from the Command Centre Server. This issue affects: Gallagher Command Centre 8.50 versions prior to 8.50.2048 (MR3); 8.40 versions prior to 8.40.2063 (MR4); 8.30 versions prior to 8.30.1454 (MR4) ; version 8.20 and prior versions.	8.1	More Details
CVE-2021-36306	Networking OS10, versions prior to October 2021 with RESTCONF API enabled, contains an authentication bypass vulnerability. A remote unauthenticated attacker could exploit this vulnerability to gain access and perform actions on the affected system.	8.1	More Details
CVE-2021-35535	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion 670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product. This issue affects: Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions.	8.1	More Details
CVE-2021-24641	The Images to WebP WordPress plugin before 1.9 does not have CSRF checks in place when performing some administrative actions, which could result in modification of plugin settings, Denial-of-Service, as well as arbitrary image conversion	8.1	More Details
CVE-2021-0078	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	8.1	More Details
CVE-2021-27024	A flaw was discovered in Continuous Delivery for Puppet Enterprise (CD4PE) that results in a user with lower privileges being able to access a Puppet Enterprise API token. This issue is resolved in CD4PE 4.10.0	8.1	More Details
CVE-2021-3968	vim is vulnerable to Heap-based Buffer Overflow	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43582	A Use-After-Free Remote Vulnerability exists when reading a DWG file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DWG files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-3973	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-0151	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33058	Improper access control in the installer Intel(R)Administrative Tools for Intel(R) Network Adaptersfor Windowsbefore version 1.4.0.21 may allow an unauthenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-3974	vim is vulnerable to Use After Free	7.8	More Details
CVE-2021-33062	Incorrect default permissions in the software installer for the Intel(R) VTune(TM) Profiler before version 2021.3.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33063	Uncontrolled search path in the Intel(R) RealSense(TM) D400 Series UWP driver for Windows 10 before version 6.1.160.22 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33071	Incorrect default permissions in the installer for the Intel(R) oneAPI Rendering Toolkit before version 2021.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-39976	There is a privilege escalation vulnerability in CloudEngine 5800 V200R020C00SPC600. Due to lack of privilege restrictions, an authenticated local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42737	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-33118	Improper access control in the software installer for the Intel(R) Serial IO driver for Intel(R) NUC 11 Gen before version 30.100.2104.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-40770	Adobe Prelude version 10.1 (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 in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-40757	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-40758	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-36340	Dell EMC SCG 5.00.00.10 and earlier, contain a sensitive information disclosure vulnerability. A local malicious user may exploit this vulnerability to read sensitive information and use it.	7.8	More Details
CVE-2021-40759	Adobe After Effects version 18.4.1 (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 in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-40760	Adobe After Effects version 18.4.1 (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 in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42266	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious FLA 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-2021-42267	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious FLA 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-2021-42269	Adobe Animate version 21.0.9 (and earlier) are affected by a use-after-free vulnerability in the processing of a malformed FLA file 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-2021-42707	PLC Editor Versions 1.3.8 and prior is vulnerable to an out-of-bounds write while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-42705	PLC Editor Versions 1.3.8 and prior is vulnerable to a stack-based buffer overflow while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-43019	Adobe Creative Cloud version 5.5 (and earlier) are affected by a privilege escalation vulnerability in the resources leveraged by the Setup.exe service. An unauthenticated attacker could leverage this vulnerability to remove files and escalate privileges under the context of SYSTEM . An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability on the product installer. User interaction is required before product installation to abuse this vulnerability.	7.8	More Details
CVE-2021-43015	Adobe InCopy version 16.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious GIF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-37322	GCC c++filt v2.26 was discovered to contain a use-after-free vulnerability via the component cplus-dem.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40755	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SGI file in the DoReadContinue function, 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-2021-42738	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-42727	Adobe Bridge 11.1.1 (and earlier) is affected by a stack overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file in Bridge.	7.8	More Details
CVE-2021-43997	FreeRTOS versions 10.2.0 through 10.4.5 do not prevent non-kernel code from calling the xPortRaisePrivilege internal function to raise privilege. FreeRTOS versions through 10.4.6 do not prevent a third party that has already independently gained the ability to execute injected code to achieve further privilege escalation by branching directly inside a FreeRTOS MPU API wrapper function with a manually crafted stack frame. These issues affect ARMv7-M MPU ports, and ARMv8-M ports with MPU support enabled (i.e. configENABLE_MPU set to 1). These are fixed in V10.5.0 and in V10.4.3-LTS Patch 3.	7.8	More Details
CVE-2021-29324	OpenSource Moddable v10.5.0 was discovered to contain a stack overflow via the component /moddable/xs/sources/xsScript.c.	7.8	More Details
CVE-2021-3939	Ubuntu-specific modifications to accountsservice (in patch file debian/patches/0010-set-language.patch) caused the fallback_locale variable, pointing to static storage, to be freed, in the user_change_language_authorized_cb function. This is reachable via the SetLanguage dbus function. This is fixed in versions 0.6.55-0ubuntu12~20.04.5, 0.6.55-0ubuntu13.3, 0.6.55-0ubuntu14.1.	7.8	More Details
CVE-2021-21561	Dell PowerScale OneFS version 8.1.2 contains a sensitive information exposure vulnerability. This would allow a malicious user with ISI_PRIV_LOGIN_SSH and/or ISI_PRIV_LOGIN_CONSOLE privileges to gain access to sensitive information in the log files.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33095	Unquoted search path in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33093	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Serial IO driver pack before version 30.100.2104.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33092	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit HID Event Filter driver pack before version 2.2.1.383 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33091	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit audio driver pack before version 1.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33090	Incorrect default permissionsin the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC10i3FN, NUC10i5FN, NUC10i7FN before version 1.78.2.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33089	Improper access control in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC8i3BE, NUC8i5BE, NUC8i7BE before version 1.78.4.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33088	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit Integrated Sensor Hub driver pack before version 5.4.1.4449 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0082	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0121	Improper access control in the installer for some Intel(R) Iris(R) Xe MAX Dedicated Graphics Drivers for Windows 10 before version 27.20.100.9466 may allow authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0096	Improper authentication in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33481	A stack-based buffer overflow vulnerability was discovered in gocr through 0.53-20200802 in try_to_divide_boxes() in pgm2asc.c.	7.8	More Details
CVE-2021-3962	A flaw was found in ImageMagick where it did not properly sanitize certain input before using it to invoke convert processes. This flaw allows an attacker to create a specially crafted image that leads to a use-after-free vulnerability when processed by ImageMagick. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2021-33479	A stack-based buffer overflow vulnerability was discovered in gocr through 0.53-20200802 in measure_pitch() in pgm2asc.c.	7.8	More Details
CVE-2021-42954	Zoho Remote Access Plus Server Windows Desktop Binary fixed from 10.1.2121.1 is affected by incorrect access control. The installation directory is vulnerable to weak file permissions by allowing full control for Windows Everyone user group (non-admin or any guest users), thereby allowing privilege escalation, unauthorized password reset, stealing of sensitive data, access to credentials in plaintext, access to registry values, tampering with configuration files, etc.	7.8	More Details
CVE-2021-42956	Zoho Remote Access Plus Server Windows Desktop Binary fixed in 10.1.2132.6 is affected by a sensitive information disclosure vulnerability. Due to improper privilege management, the process launches as the logged in user, so memory dump can be done by non-admin also. Remotely, an attacker can dump all sensitive information including DB Connection string, entire IT infrastructure details, commands executed by IT admin including credentials, secrets, private keys and more.	7.8	More Details
CVE-2021-42254	BeyondTrust Privilege Management prior to version 21.6 creates a Temporary File in a Directory with Insecure Permissions.	7.8	More Details
CVE-2021-44038	An issue was discovered in Quagga through 1.2.4. Unsafe chown/chmod operations in the suggested spec file allow users (with control of the non-root-owned directory /etc/quagga) to escalate their privileges to root upon package installation or update.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35033	A vulnerability in specific versions of Zyxel NBG6818, NBG7815, WSQ20, WSQ50, WSQ60, and WSR30 firmware with pre-configured password management could allow an attacker to obtain root access of the device, if the local attacker dismantles the device and uses a USB-to-UART cable to connect the device, or if the remote assistance feature had been enabled by an authenticated user.	7.8	More Details
CVE-2021-33094	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-35052	A component in Kaspersky Password Manager could allow an attacker to elevate a process Integrity level from Medium to High.	7.8	More Details
CVE-2021-33106	Integer overflow in the Safestring library maintained by Intel(R) may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-29329	OpenSource Moddable v10.5.0 was discovered to contain a stack overflow in the fxBinaryExpressionNodeDistribute function at /moddable/xs/sources/xsTree.c.	7.8	More Details
CVE-2021-29325	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow in the fx_String_prototype_repeat function at /moddable/xs/sources/xsString.c.	7.8	More Details
CVE-2021-29326	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow in the fxIDToString function at /moddable/xs/sources/xsSymbol.c.	7.8	More Details
CVE-2021-0065	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-29327	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow in the fx_ArrayBuffer function at /moddable/xs/sources/xsDataView.c.	7.8	More Details
CVE-2021-0064	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8741	Improper permissions in the installer for the Intel(R) Thunderbolt(TM) non-DCH driver, all versions, for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-23162	Improper validation of the cloud certificate chain in Mobile Connect allows man-in-the-middle attack to impersonate the legitimate Command Centre Server. This issue affects: Gallagher Command Centre Mobile Connect for Android 15 versions prior to 15.04.040; version 14 and prior versions.	7.7	More Details
CVE-2021-42360	On sites that also had the Elementor plugin for WordPress installed, it was possible for users with the edit_posts capability, which includes Contributor-level users, to import blocks onto any page using the astra-page-elementor-batch-process AJAX action. An attacker could craft and host a block containing malicious JavaScript on a server they controlled, and then use it to overwrite any post or page by sending an AJAX request with the action set to astra-page-elementor-batch-process and the url parameter pointed to their remotely-hosted malicious block, as well as an id parameter containing the post or page to overwrite. Any post or page that had been built with Elementor, including published pages, could be overwritten by the imported block, and the malicious JavaScript in the imported block would then be executed in the browser of any visitors to that page.	7.6	More Details
CVE-2020-7882	Using the parameter of getPFXFolderList function, attackers can see the information of authorization certification and delete the files. It occurs because the parameter contains path traversal characters(ie. '../../../')	7.5	More Details
CVE-2021-22965	A vulnerability in Pulse Connect Secure before 9.1R12.1 could allow an unauthenticated administrator to causes a denial of service when a malformed request is sent to the device.	7.5	More Details
CVE-2021-36320	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID.	7.5	More Details
CVE-2021-20601	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23201	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller, which may allow a user with elevated privileges to generate valid microcode by identifying, exploiting, and loading vulnerable microcode. Such an attack could lead to information disclosure, data corruption, or denial of service of the device. The scope may extend to other components.	7.5	More Details
CVE-2021-23217	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller, which may allow a user with elevated privileges to instantiate a DMA write operation only within a specific time window timed to corrupt code execution, which may impact confidentiality, integrity, or availability. The scope impact may extend to other components.	7.5	More Details
CVE-2021-39925	Buffer overflow in the Bluetooth SDP dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-43669	A vulnerability has been detected in HyperLedger Fabric v1.4.0, v2.0.0, v2.0.1, v2.3.0. It can easily break down as many orderers as the attacker wants. This bug can be leveraged by constructing a message whose header is invalid to the interface Order. This bug has been admitted and fixed by the developers of Fabric.	7.5	More Details
CVE-2021-38146	The File Download API in Wipro Holmes Orchestrator 20.4.1 (20.4.1_02_11_2020) allows remote attackers to read arbitrary files via absolute path traversal in the SearchString JSON field in /home/download POST data.	7.5	More Details
CVE-2021-22970	Concrete CMS (formerly concrete5) versions 8.5.6 and below and version 9.0.0 allow local IP importing causing the system to be vulnerable toa. SSRF attacks on the private LAN servers by reading files from the local LAN. An attacker can pivot in the private LAN and exploit local network appsandb. SSRF Mitigation Bypass through DNS RebindingConcrete CMS security team gave this a CVSS score of 3.5 AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:NConcrete CMS is maintaining Concrete version 8.5.x until 1 May 2022 for security fixes.This CVE is shared with HackerOne Reports https://hackerone.com/reports/1364797 and https://hackerone.com/reports/1360016Reporters: Adrian Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/) and Bipul Jaiswal	7.5	More Details
CVE-2021-39924	Large loop in the Bluetooth DHT dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41436	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet.	7.5	More Details
CVE-2021-22967	In Concrete CMS (formerly concrete 5) below 8.5.7, IDOR Allows Unauthenticated User to Access Restricted Files If Allowed to Add Message to a Conversation.To remediate this, a check was added to verify a user has permissions to view files before attaching the files to a message in "add / edit message".Concrete CMS security team gave this a CVSS v3.1 score of 4.3 AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:NCredit for discovery Adrian H	7.5	More Details
CVE-2021-41569	SAS/Intrnet 9.4 build 1520 and earlier allows Local File Inclusion. The samples library (included by default) in the appstart.sas file, allows end-users of the application to access the sample.webcsf1.sas program, which contains user-controlled macro variables that are passed to the DS2CSF macro. Users can escape the context of the configured user-controllable variable and append additional functions native to the macro but not included as variables within the library. This includes a function that retrieves files from the host OS.	7.5	More Details
CVE-2021-22951	Unauthorized individuals could view password protected files using view_inline in Concrete CMS (previously concrete 5) prior to version 8.5.7. Concrete CMS now checks to see if a file has a password in view_inline and, if it does, the file is not rendered.For version 8.5.6, the following mitigations were put in place a. restricting file types for view_inline to images only b. putting a warning in the file manager to advise users.Credit for discovery: "Solar Security Research Team"Concrete CMS security team CVSS scoring is 5.3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:NThis fix is also in Concrete version 9.0.0	7.5	More Details
CVE-2021-39921	NULL pointer exception in the Modbus dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-44150	The client in tusdotnet through 2.5.0 relies on SHA-1 to prevent spoofing of file content.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44037	Team Password Manager (aka TeamPasswordManager) before 10.135.236 allows password-reset poisoning.	7.5	More Details
CVE-2021-39923	Large loop in the PNRP dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-26614	ius_get.cgi in IpTime C200 camera allows remote code execution. A remote attacker may send a crafted parameters to the exposed vulnerable web service interface which invokes the arbitrary shell command.	7.5	More Details
CVE-2021-38448	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software.	7.5	More Details
CVE-2021-39922	Buffer overflow in the C12.22 dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-39929	Uncontrolled Recursion in the Bluetooth DHT dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-39920	NULL pointer exception in the IPPUSB dissector in Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-39928	NULL pointer exception in the IEEE 802.11 dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-43557	The uri-block plugin in Apache APISIX before 2.10.2 uses $request_uri without verification. The $request_uri is the full original request URI without normalization. This makes it possible to construct a URI to bypass the block list on some occasions. For instance, when the block list contains "^/internal/", a URI like `//internal/` can be used to bypass it. Some other plugins also have the same issue. And it may affect the developer's custom plugin.	7.5	More Details
CVE-2021-39926	Buffer overflow in the Bluetooth HCI_ISO dissector in Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-37007	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37003	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37012	There is a Data Processing Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37017	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37018	There is a Data Processing Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37019	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37024	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37025	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37026	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37030	There is an Improper permission vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	7.5	More Details
CVE-2021-37031	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly.	7.5	More Details
CVE-2021-37033	There is an Injection attack vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	7.5	More Details
CVE-2021-37034	There is an Unstandardized field names in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37035	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly.	7.5	More Details
CVE-2021-24644	The Images to WebP WordPress plugin before 1.9 does not validate or sanitise the tab parameter before passing it to the include() function, which could lead to a Local File Inclusion issue	7.5	More Details
CVE-2021-0013	Improper input validation for Intel(R) EMA before version 1.5.0 may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2021-40745	Adobe Campaign version 21.2.1 (and earlier) is affected by a Path Traversal vulnerability that could lead to reading arbitrary server files. By leveraging an exposed XML file, an unauthenticated attacker can enumerate other files on the server.	7.5	More Details
CVE-2021-38890	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 209507.	7.5	More Details
CVE-2021-38891	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 209508.	7.5	More Details
CVE-2021-41281	Synapse is a package for Matrix homeservers written in Python 3/Twisted. Prior to version 1.47.1, Synapse instances with the media repository enabled can be tricked into downloading a file from a remote server into an arbitrary directory. No authentication is required for the affected endpoint. The last 2 directories and file name of the path are chosen randomly by Synapse and cannot be controlled by an attacker, which limits the impact. Homeservers with the media repository disabled are unaffected. Homeservers with a federation whitelist are also unaffected, since Synapse will check the remote hostname, including the trailing `../`s, against the whitelist. Server administrators should upgrade to 1.47.1 or later. Server administrators using a reverse proxy could, at the expense of losing media functionality, may block the certain endpoints as a workaround. Alternatively, non-containerized deployments can be adapted to use the hardened systemd config.	7.5	More Details
CVE-2021-37015	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36321	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service.	7.5	More Details
CVE-2021-43667	A vulnerability has been detected in HyperLedger Fabric v1.4.0, v2.0.0, v2.1.0. This bug can be leveraged by constructing a message whose payload is nil and sending this message with the method 'forwardToLeader'. This bug has been admitted and fixed by the developers of Fabric. If leveraged, any leader node will crash.	7.5	More Details
CVE-2021-37005	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37004	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-37010	There is a Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the confidentiality of users is affected.	7.5	More Details
CVE-2021-37006	There is a Improper Preservation of Permissions vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the confidentiality of users is affected.	7.5	More Details
CVE-2021-37009	There is a Configuration vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the confidentiality of users is affected.	7.5	More Details
CVE-2021-37008	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash.	7.5	More Details
CVE-2021-42955	Zoho Remote Access Plus Server Windows Desktop binary fixed in version 10.1.2132 is affected by an unauthorized password reset vulnerability. Because of the designed password reset mechanism, any non-admin Windows user can reset the password of the Remote Access Plus Server Admin account.	7.3	More Details
CVE-2021-43555	mySCADA myDESIGNER Versions 8.20.0 and prior fails to properly validate contents of an imported project file, which may make the product vulnerable to a path traversal payload. This vulnerability may allow an attacker to plant files on the file system in arbitrary locations or overwrite existing files, resulting in remote code execution.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24877	The MainWP Child WordPress plugin before 4.1.8 does not validate the orderby and order parameter before using them in a SQL statement, leading to an SQL injection exploitable by high privilege users such as admin when the Backup and Staging by WP Time Capsule plugin is installed	7.2	More Details
CVE-2021-35534	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions.	7.2	More Details
CVE-2021-22968	A bypass of adding remote files in Concrete CMS (previously concrete5) File Manager leads to remote code execution in Concrete CMS (concrete5) versions 8.5.6 and below.The external file upload feature stages files in the public directory even if they have disallowed file extensions. They are stored in a directory with a random name, but it's possible to stall the uploads and brute force the directory name. You have to be an admin with the ability to upload files, but this bug gives you the ability to upload restricted file types and execute them depending on server configuration.To fix this, a check for allowed file extensions was added before downloading files to a tmp directory.Concrete CMS Security Team gave this a CVSS v3.1 score of 5.4 AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:NThis fix is also in Concrete version 9.0.0	7.2	More Details
CVE-2021-35528	Improper Access Control vulnerability in the application authentication and authorization of Hitachi Energy Retail Operations, Counterparty Settlement and Billing (CSB) allows an attacker to execute a modified signed Java Applet JAR file. A successful exploitation may lead to data extraction or modification of data inside the application. This issue affects: Hitachi Energy Retail Operations 5.7.3 and prior versions. Hitachi Energy Counterparty Settlement and Billing (CSB) 5.7.3 prior versions.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36299	Dell iDRAC9 versions 4.40.00.00 and later, but prior to 4.40.29.00 and 5.00.00.00 contain an SQL injection vulnerability. A remote authenticated malicious user with low privileges may potentially exploit this vulnerability to cause information disclosure or denial of service by supplying specially crafted input data to the affected application.	7.1	More Details
CVE-2021-36314	Dell EMC CloudLink 7.1 and all prior versions contain an Arbitrary File Creation Vulnerability. A remote unauthenticated attacker, may potentially exploit this vulnerability, leading to the execution of arbitrary files on the end user system.	7.1	More Details
CVE-2021-29328	OpenSource Moddable v10.5.0 was discovered to contain buffer over-read in the fxDebugThrow function at /moddable/xs/sources/xsDebug.c.	7.1	More Details
CVE-2021-23146	An Incomplete Comparison with Missing Factors vulnerability in the Gallagher Controller allows an attacker to bypass PIV verification. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1359 (MR3); 8.20 versions prior to 8.20.1259 (MR5); 8.10 versions prior to 8.10.1284 (MR7); version 8.00 and prior versions.	7.1	More Details
CVE-2021-43549	A remote authenticated attacker with write access to a PI Server could trick a user into interacting with a PI Web API endpoint and redirect them to a malicious website. As a result, a victim may disclose sensitive information to the attacker or be provided with false information.	6.9	More Details
CVE-2021-0146	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2021-44033	In Ionic Identity Vault before 5.0.5, the protection mechanism for invalid unlock attempts can be bypassed.	6.8	More Details
CVE-2021-39234	In Apache Ozone versions prior to 1.2.0, Authenticated users knowing the ID of an existing block can craft specific request allowing access those blocks, bypassing other security checks like ACL.	6.8	More Details
CVE-2021-34358	We have already fixed this vulnerability in the following versions of QmailAgent: QmailAgent 3.0.2 (2021/08/25) and later	6.8	More Details
CVE-2021-0135	Improper input validation in the Intel(R) Ethernet Diagnostic Driver for Windows before version 1.4.0.10 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0658	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107.	6.7	More Details
CVE-2021-0158	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-43975	In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-of-bounds write via a crafted length value.	6.7	More Details
CVE-2021-0186	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	6.7	More Details
CVE-2021-0157	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0671	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273.	6.7	More Details
CVE-2021-0667	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581.	6.7	More Details
CVE-2021-0657	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103.	6.7	More Details
CVE-2021-0656	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376.	6.7	More Details
CVE-2021-0655	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0629	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625.	6.7	More Details
CVE-2021-0664	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158.	6.7	More Details
CVE-2021-0668	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521.	6.7	More Details
CVE-2021-0669	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550.	6.7	More Details
CVE-2021-0670	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663.	6.7	More Details
CVE-2021-33059	Improper input validation in the Intel(R) Administrative Tools for Intel(R) Network Adapters driver for Windows before version 1.4.0.15, may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0200	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access.	6.7	More Details
CVE-2021-33097	Time-of-check time-of-use vulnerability in the Crypto API Toolkit for Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via network access.	6.6	More Details
CVE-2021-33491	OX App Suite through 7.10.5 allows Directory Traversal via ../ in an OOXML or ODF ZIP archive, because of the mishandling of relative paths in mail addresses in conjunction with auto-configuration DNS records.	6.5	More Details
CVE-2021-36300	iDRAC9 versions prior to 5.00.00.00 contain an improper input validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability by sending a specially crafted malicious request to crash the webserver or cause information disclosure.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43337	SchedMD Slurm 21.08.* before 21.08.4 has Incorrect Access Control. On sites using the new AccountingStoreFlags=job_script and/or job_env options, the access control rules in SlurmDBD may permit users to request job scripts and environment files to which they should not have access.	6.5	More Details
CVE-2021-24852	The MouseWheel Smooth Scroll WordPress plugin before 5.7 does not have CSRF check in place on its settings page, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2021-24802	The Colorful Categories WordPress plugin before 2.0.15 does not enforce nonce checks which could allow attackers to make a logged in admin or editor change taxonomy colors via a CSRF attack	6.5	More Details
CVE-2021-42250	Improper output neutralization for Logs. A specific Apache Superset HTTP endpoint allowed for an authenticated user to forge log entries or inject malicious content into logs.	6.5	More Details
CVE-2021-38875	IBM MQ 8.0, 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.1 CD, and 9.2 CD is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 208398.	6.5	More Details
CVE-2021-24894	The Reviews Plus WordPress plugin before 1.2.14 does not validate the submitted rating, allowing submission of long integer, causing a Denial of Service in the review section when an authenticated user submit such rating and the reviews are set to be displayed on the post/page	6.5	More Details
CVE-2021-23718	The package ssrf-agent before 1.0.5 are vulnerable to Server-side Request Forgery (SSRF) via the defaultIpChecker function. It fails to properly validate if the IP requested is private.	6.5	More Details
CVE-2021-43551	A remote attacker with write access to PI Vision could inject code into a display. Unauthorized information disclosure, modification, or deletion is possible if a victim views or interacts with the infected display using Microsoft Internet Explorer. The impact affects PI System data and other data accessible with victim's user permissions.	6.5	More Details
CVE-2021-0079	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-37023	There is a Improper Access Control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause media files which can be reads and writes in non-distributed directories on any device on the network..	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39235	In Apache Ozone before 1.2.0, Ozone Datanode doesn't check the access mode parameter of the block token. Authenticated users with valid READ block token can do any write operation on the same block.	6.5	More Details
CVE-2021-3976	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF)	6.5	More Details
CVE-2021-27025	A flaw was discovered in Puppet Agent where the agent may silently ignore Augeas settings or may be vulnerable to a Denial of Service condition prior to the first 'pluginsync'.	6.5	More Details
CVE-2021-43408	The "Duplicate Post" WordPress plugin up to and including version 1.1.9 is vulnerable to SQL Injection. SQL injection vulnerabilities occur when client supplied data is included within an SQL Query insecurely. SQL Injection can typically be exploited to read, modify and delete SQL table data. In many cases it also possible to exploit features of SQL server to execute system commands and/or access the local file system. This particular vulnerability can be exploited by any authenticated user who has been granted access to use the Duplicate Post plugin. By default, this is limited to Administrators, however the plugin presents the option to permit access to the Editor, Author, Contributor and Subscriber roles.	6.5	More Details
CVE-2021-22030	In versions of Greenplum database prior to 5.28.14 and 6.17.0, certain statements execution led to the storage of sensitive(credential) information in the logs of the database. A malicious user with access to logs can read sensitive(credentials) information about users	6.5	More Details
CVE-2021-0069	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-0063	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40829	Connections initialized by the AWS IoT Device SDK v2 for Java (versions prior to 1.4.2), Python (versions prior to 1.6.1), C++ (versions prior to 1.12.7) and Node.js (versions prior to 1.5.3) did not verify server certificate hostname during TLS handshake when overriding Certificate Authorities (CA) in their trust stores on MacOS. This issue has been addressed in aws-c-io submodule versions 0.10.5 onward. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.4.2 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.6.1 on macOS. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on macOS. Amazon Web Services AWS-C-IO 0.10.4 on macOS.	6.3	More Details
CVE-2021-40828	Connections initialized by the AWS IoT Device SDK v2 for Java (versions prior to 1.3.3), Python (versions prior to 1.5.18), C++ (versions prior to 1.12.7) and Node.js (versions prior to 1.5.1) did not verify server certificate hostname during TLS handshake when overriding Certificate Authorities (CA) in their trust stores on Windows. This issue has been addressed in aws-c-io submodule versions 0.9.13 onward. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.3.3 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.5.18 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on Microsoft Windows.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40831	The AWS IoT Device SDK v2 for Java, Python, C++ and Node.js appends a user supplied Certificate Authority (CA) to the root CAs instead of overriding it on macOS systems. Additionally, SNI validation is also not enabled when the CA has been “overridden”. TLS handshakes will thus succeed if the peer can be verified either from the user-supplied CA or the system’s default trust-store. Attackers with access to a host’s trust stores or are able to compromise a certificate authority already in the host's trust store (note: the attacker must also be able to spoof DNS in this case) may be able to use this issue to bypass CA pinning. An attacker could then spoof the MQTT broker, and either drop traffic and/or respond with the attacker's data, but they would not be able to forward this data on to the MQTT broker because the attacker would still need the user's private keys to authenticate against the MQTT broker. The 'aws_tls_ctx_options_override_default_trust_store_*' function within the aws-c-io submodule has been updated to address this behavior. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.5.0 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.7.0 on macOS. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.14.0 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.6.0 on macOS. Amazon Web Services AWS-C-IO 0.10.7 on macOS.	6.3	More Details
CVE-2021-40830	The AWS IoT Device SDK v2 for Java, Python, C++ and Node.js appends a user supplied Certificate Authority (CA) to the root CAs instead of overriding it on Unix systems. TLS handshakes will thus succeed if the peer can be verified either from the user-supplied CA or the system’s default trust-store. Attackers with access to a host’s trust stores or are able to compromise a certificate authority already in the host's trust store (note: the attacker must also be able to spoof DNS in this case) may be able to use this issue to bypass CA pinning. An attacker could then spoof the MQTT broker, and either drop traffic and/or respond with the attacker's data, but they would not be able to forward this data on to the MQTT broker because the attacker would still need the user's private keys to authenticate against the MQTT broker. The 'aws_tls_ctx_options_override_default_trust_store_*' function within the aws-c-io submodule has been updated to override the default trust store. This corrects this issue. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.5.0 on Linux/Unix. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.6.1 on Linux/Unix. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on Linux/Unix. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on Linux/Unix. Amazon Web Services AWS-C-IO 0.10.4 on Linux/Unix.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0182	Uncontrolled resource consumption in the Intel(R) HAXM software before version 7.6.6 may allow an unauthenticated user to potentially enable information disclosure via local access.	6.2	More Details
CVE-2021-29861	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in EFS to expose sensitive information. IBM X-Force ID: 206085.	6.2	More Details
CVE-2021-42744	Philips MRI 1.5T and MRI 3T Version 5.x.x exposes sensitive information to an actor not explicitly authorized to have access.	6.2	More Details
CVE-2021-26262	Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an unauthorized actor.	6.2	More Details
CVE-2021-26248	Philips MRI 1.5T and MRI 3T Version 5.x.x assigns an owner who is outside the intended control sphere to a resource.	6.2	More Details
CVE-2021-29860	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the libc.a library to expose sensitive information. IBM X-Force ID: 206084.	6.2	More Details
CVE-2021-33495	OX App Suite 7.10.5 allows XSS via an OX Chat system message.	6.1	More Details
CVE-2021-31851	A Reflected Cross-Site Scripting vulnerability in McAfee Policy Auditor prior to 6.5.2 allows a remote unauthenticated attacker to inject arbitrary web script or HTML via the profileNodeID request parameters. The malicious script is reflected unmodified into the Policy Auditor web-based interface which could lead to the extraction of end user session token or login credentials. These may be used to access additional security-critical applications or conduct arbitrary cross-domain requests.	6.1	More Details
CVE-2021-38000	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 95.0.4638.69 allowed a remote attacker to arbitrarily browser to a malicious URL via a crafted HTML page.	6.1	More Details
CVE-2021-37999	Insufficient data validation in New Tab Page in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to inject arbitrary scripts or HTML in a new browser tab via a crafted HTML page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43558	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A URL parameter in the filetype site administrator tool required extra sanitizing to prevent a reflected XSS risk.	6.1	More Details
CVE-2021-24875	The eCommerce Product Catalog Plugin for WordPress plugin before 3.0.39 does not escape the ic-settings-search parameter before outputting it back in the page in an attribute, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-24873	The Tutor LMS WordPress plugin before 1.9.11 does not sanitise and escape user input before outputting back in attributes in the Student Registration page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-31852	A Reflected Cross-Site Scripting vulnerability in McAfee Policy Auditor prior to 6.5.2 allows a remote unauthenticated attacker to inject arbitrary web script or HTML via the UID request parameter. The malicious script is reflected unmodified into the Policy Auditor web-based interface which could lead to the extract of end user session token or login credentials. These may be used to access additional security-critical applications or conduct arbitrary cross-domain requests.	6.1	More Details
CVE-2021-24891	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.	6.1	More Details
CVE-2021-33489	OX App Suite through 7.10.5 allows XSS via JavaScript code in a shared XCF file.	6.1	More Details
CVE-2021-33490	OX App Suite through 7.10.5 allows XSS via a crafted snippet in a shared mail signature.	6.1	More Details
CVE-2021-33494	OX App Suite 7.10.5 allows XSS via an OX Chat room title during typing rendering.	6.1	More Details
CVE-2021-33492	OX App Suite 7.10.5 allows XSS via an OX Chat room name.	6.1	More Details
CVE-2021-38375	OX App Suite through 7.10.5 allows XSS via the alt attribute of an IMG element in a truncated e-mail message.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38377	OX App Suite through 7.10.5 allows XSS via JavaScript code in an anchor HTML comment within truncated e-mail, because there is a predictable UUID with HTML transformation results.	6.1	More Details
CVE-2021-33488	chat in OX App Suite 7.10.5 has Improper Input Validation. A user can be redirected to a rogue OX Chat server via a development-related hook.	6.1	More Details
CVE-2021-36322	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections.	6.1	More Details
CVE-2021-44025	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to XSS in handling an attachment's filename extension when displaying a MIME type warning message.	6.1	More Details
CVE-2021-24796	The My Tickets WordPress plugin before 1.8.31 does not properly sanitise and escape the Email field of booked tickets before outputting it in the Payment admin dashboard, which could allow unauthenticated users to perform Cross-Site Scripting attacks against admins	6.1	More Details
CVE-2021-43977	SmarterTools SmarterMail 16.x through 100.x before 100.0.7803 allows XSS.	6.1	More Details
CVE-2021-42363	The Preview E-Mails for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the search_order parameter found in the ~/views/form.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.6.8.	6.1	More Details
CVE-2021-36311	Dell EMC Networker versions prior to 19.5 contain an Improper Authorization vulnerability. Any local malicious user with networker user privileges may exploit this vulnerability to upload malicious file to unauthorized locations and execute it.	6.0	More Details
CVE-2021-33493	The middleware component in OX App Suite through 7.10.5 allows Code Injection via Java classes in a YAML format.	6.0	More Details
CVE-2021-23433	The package algoliasearch-helper before 3.6.2 are vulnerable to Prototype Pollution due to use of the merge function in src/SearchParameters/index.jsSearchParameters._parseNumbers without any protection against prototype properties. Note that this vulnerability is only exploitable if the implementation allows users to define arbitrary search patterns.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36334	Dell EMC CloudLink 7.1 and all prior versions contain a CSV formula Injection Vulnerability. A remote high privileged attacker, may potentially exploit this vulnerability, leading to arbitrary code execution on end user machine	5.9	More Details
CVE-2021-36301	Dell iDRAC 9 prior to version 4.40.40.00 and iDRAC 8 prior to version 2.80.80.80 contain a Stack Buffer Overflow in Racadm. An authenticated remote attacker may potentially exploit this vulnerability to control process execution and gain access to the underlying operating system.	5.9	More Details
CVE-2021-22356	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200.	5.9	More Details
CVE-2021-36308	Networking OS10, versions prior to October 2021 with Smart Fabric Services enabled, contains an authentication bypass vulnerability. A remote unauthenticated attacker could exploit this vulnerability to gain access and perform actions on the affected system.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41278	Functions SDK for EdgeX is meant to provide all the plumbing necessary for developers to get started in processing/transforming/exporting data out of the EdgeX IoT platform. In affected versions broken encryption in app-functions-sdk “AES” transform in EdgeX Foundry releases prior to Jakarta allows attackers to decrypt messages via unspecified vectors. The app-functions-sdk exports an “aes” transform that user scripts can optionally call to encrypt data in the processing pipeline. No decrypt function is provided. Encryption is not enabled by default, but if used, the level of protection may be less than the user may expects due to a broken implementation. Version v2.1.0 (EdgeX Foundry Jakarta release and later) of app-functions-sdk-go/v2 deprecates the “aes” transform and provides an improved “aes256” transform in its place. The broken implementation will remain in a deprecated state until it is removed in the next EdgeX major release to avoid breakage of existing software that depends on the broken implementation. As the broken transform is a library function that is not invoked by default, users who do not use the AES transform in their processing pipelines are unaffected. Those that are affected are urged to upgrade to the Jakarta EdgeX release and modify processing pipelines to use the new "aes256" transform.	5.7	More Details
CVE-2021-24703	The Download Plugin WordPress plugin before 1.6.1 does not have capability and CSRF checks in the dpwap_plugin_activate AJAX action, allowing any authenticated users, such as subscribers, to activate plugins that are already installed.	5.7	More Details
CVE-2021-0053	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access.	5.7	More Details
CVE-2021-3672	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability.	5.6	More Details
CVE-2021-33087	Improper authentication in the installer for the Intel(R) NUC M15 Laptop Kit Management Engine driver pack before version 15.0.10.1508 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40761	Adobe After Effects version 18.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-0623	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817.	5.5	More Details
CVE-2021-36333	Dell EMC CloudLink 7.1 and all prior versions contain a Buffer Overflow Vulnerability. A local low privileged attacker, may potentially exploit this vulnerability, leading to an application crash.	5.5	More Details
CVE-2021-33098	Improper input validation in the Intel(R) Ethernet ixgbe driver for Linux before version 3.17.3 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-0622	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388.	5.5	More Details
CVE-2021-44147	An XML External Entity issue in Claris FileMaker Pro and Server (including WebDirect) before 19.4.1 allows a remote attacker to disclose local files via a crafted XML/Excel document and perform server-side request forgery attacks.	5.5	More Details
CVE-2021-42268	Adobe Animate version 21.0.9 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted FLA file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40756	Adobe After Effects version 18.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0620	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381.	5.5	More Details
CVE-2021-38959	IBM SPSS Statistics for Windows 24.0, 25.0, 26.0, 27.0, 27.0.1, and 28.0 could allow a local user to cause a denial of service by writing arbitrary files to admin protected directories on the system. IBM X-Force ID: 212046.	5.5	More Details
CVE-2021-0619	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395.	5.5	More Details
CVE-2021-0621	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383.	5.5	More Details
CVE-2021-37036	There is an information leakage vulnerability in FusionCompute 6.5.1, eCNS280_TD V100R005C00 and V100R005C10. Due to the improperly storage of specific information in the log file, the attacker can obtain the information when a user logs in to the device. Successful exploit may cause the information leak.	5.5	More Details
CVE-2021-33073	Uncontrolled resource consumption in the Intel(R) Distribution of OpenVINOâ„¢ Toolkit before version 2021.4 may allow an unauthenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-0672	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-199678035	5.5	More Details
CVE-2021-33480	An use-after-free vulnerability was discovered in gocr through 0.53-20200802 in context_correction() in pgm2asc.c.	5.5	More Details
CVE-2021-43668	Go-Ethereum 1.10.9 nodes crash (denial of service) after receiving a serial of messages and cannot be recovered. They will crash with "runtime error: invalid memory address or nil pointer dereference" and arise a SEGV signal.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33086	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-43016	Adobe InCopy version 16.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-42733	Adobe Bridge version 11.1.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-0624	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988.	5.5	More Details
CVE-2021-40131	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input that is processed by the web-based management interface. An attacker could exploit this vulnerability by adding malicious code to the configuration by using the web-based management interface. A successful exploit could allow the attacker to execute arbitrary code in the context of the interface or access sensitive, browser-based information.	5.5	More Details
CVE-2021-0075	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-40774	Adobe Prelude version 10.1 (and earlier) is affected by a null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40773	Adobe Prelude version 10.1 (and earlier) is affected by a null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-0120	Improper initialization in the installer for some Intel(R) Graphics DCH Drivers for Windows 10 before version 27.20.100.9316 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-0110	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-0152	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-29323	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow via the component /modules/network/wifi/esp/modwifi.c.	5.5	More Details
CVE-2021-36003	Adobe Audition version 14.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-25986	In Django-wiki, versions 0.0.20 to 0.7.8 are vulnerable to Stored Cross-Site Scripting (XSS) in Notifications Section. An attacker who has access to edit pages can inject JavaScript payload in the title field. When a victim gets a notification regarding the changes made in the application, the payload in the notification panel renders and loads external JavaScript.	5.4	More Details
CVE-2021-33850	There is a Cross-Site Scripting vulnerability in Microsoft Clarity version 0.3. The XSS payload executes whenever the user changes the clarity configuration in Microsoft Clarity version 0.3. The payload is stored on the configuring project Id page.	5.4	More Details
CVE-2021-22410	There is a XSS injection vulnerability in iMaster NCE-Fabric V100R019C10. A module of the client does not verify the input sufficiently. Attackers can exploit this vulnerability by modifying input after logging onto the client. This may compromise the normal service of the client.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38374	OX App Suite through through 7.10.5 allows XSS via a crafted snippet that has an app loader reference within an app loader URL.	5.4	More Details
CVE-2021-24834	The YOP Poll WordPress plugin before 6.3.1 is affected by a stored Cross-Site Scripting vulnerability which exists in the Create Poll - Options module where a user with a role as low as author is allowed to execute arbitrary script code within the context of the application. This vulnerability is due to insufficient validation of custom label parameters - vote button label , results link label and back to vote caption label.	5.4	More Details
CVE-2021-24833	The YOP Poll WordPress plugin before 6.3.1 is affected by a stored Cross-Site Scripting vulnerability, which exists in the Admin preview module where a user with a role as low as author is allowed to execute arbitrary script code within the context of the application. This vulnerability is due to insufficient validation of question and answer text parameters in Create Poll module.	5.4	More Details
CVE-2021-24729	The Logo Showcase with Slick Slider WordPress plugin before 1.2.4 does not sanitise the Grid Settings, which could allow users with a role as low as Author to perform stored Cross-Site Scripting attacks via post metadata of Grid logo showcase.	5.4	More Details
CVE-2021-24812	The BetterLinks WordPress plugin before 1.2.6 does not sanitise and escape some of imported link fields, which could lead to Stored Cross-Site Scripting issues when an admin import a malicious CSV.	5.4	More Details
CVE-2021-3920	grav-plugin-admin is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-24850	The Insert Pages WordPress plugin before 3.7.0 adds a shortcode that prints out other pages' content and custom fields. It can be used by users with a role as low as Contributor to perform Cross-Site Scripting attacks by storing the payload/s in another post's custom fields.	5.4	More Details
CVE-2021-23673	This affects all versions of package pekeupload. If an attacker induces a user to upload a file whose name contains javascript code, the javascript code will be executed.	5.4	More Details
CVE-2020-22719	Shimo Document v2.0.1 contains a cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the table content text field.	5.4	More Details
CVE-2021-3961	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24854	The QR Redirector WordPress plugin before 1.6.1 does not sanitise and escape some of the QR Redirect fields, which could allow users with a role as low as Contributor perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2021-3950	django-helpdesk is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-36332	Dell EMC CloudLink 7.1 and all prior versions contain a HTML and Javascript Injection Vulnerability. A remote low privileged attacker, may potentially exploit this vulnerability, directing end user to arbitrary and potentially malicious websites.	5.4	More Details
CVE-2021-37032	There is a Bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Digital Balance to fail to work.	5.3	More Details
CVE-2021-37029	There is an Identity verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	5.3	More Details
CVE-2021-43560	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. Insufficient capability checks made it possible to fetch other users' calendar action events.	5.3	More Details
CVE-2021-38681	A reflected cross-site scripting (XSS) vulnerability has been reported to affect QNAP NAS running Ragic Cloud DB. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already disabled and removed Ragic Cloud DB from the QNAP App Center, pending a security patch from Ragic.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22969	Concrete CMS (formerly concrete5) versions below 8.5.7 has a SSRF mitigation bypass using DNS Rebind attack giving an attacker the ability to fetch cloud IAAS (ex AWS) IAM keys.To fix this Concrete CMS no longer allows downloads from the local network and specifies the validated IP when downloading rather than relying on DNS.Discoverer: Adrian Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/)The Concrete CMS team gave this a CVSS 3.1 score of 3.5 AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N . Please note that Cloud IAAS provider mis-configurations are not Concrete CMS vulnerabilities. A mitigation for this vulnerability is to make sure that the IMDS configurations are according to a cloud provider's best practices.This fix is also in Concrete version 9.0.0	5.3	More Details
CVE-2021-38376	OX App Suite through 7.10.5 has Incorrect Access Control for retrieval of session information via the rampup action of the login API call.	5.3	More Details
CVE-2021-41532	In Apache Ozone before 1.2.0, Recon HTTP endpoints provide access to OM, SCM and Datanode metadata. Due to a bug, any unauthenticated user can access the data from these endpoints.	5.3	More Details
CVE-2021-43979	Styra Open Policy Agent (OPA) Gatekeeper through 3.7.0 mishandles concurrency, sometimes resulting in incorrect access control. The data replication mechanism allows policies to access the Kubernetes cluster state. During data replication, OPA/Gatekeeper does not wait for the replication to finish before processing a request, which might cause inconsistencies between the replicated resources in OPA/Gatekeeper and the resources actually present in the cluster. Inconsistency can later be reflected in a policy bypass. NOTE: the vendor disagrees that this is a vulnerability, because Kubernetes states are only eventually consistent	5.3	More Details
CVE-2021-38980	IBM Tivoli Key Lifecycle Manager (IBM Security Guardium 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: 212786.	5.3	More Details
CVE-2021-37013	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the availability of users is affected.	5.3	More Details
CVE-2021-23197	Unquoted service path vulnerability in the Gallagher Controller Service allows an unprivileged user to execute arbitrary code as the account that runs the Controller Service. This issue affects: Gallagher Command Centre 8.50 versions prior to 8.50.2048 (MR3) ;	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32600	An exposure of sensitive information to an unauthorized actor vulnerability in FortiOS CLI 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, 6.0.x and 5.6.x may allow a local and authenticated user assigned to a specific VDOM to retrieve other VDOMs information such as the admin account list and the network interface list.	5.0	More Details
CVE-2021-40129	A vulnerability in the configuration dashboard of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to submit a SQL query through the CSPC configuration dashboard. This vulnerability is due to insufficient input validation of uploaded files. An attacker could exploit this vulnerability by uploading a file containing a SQL query to the configuration dashboard. A successful exploit could allow the attacker to read restricted information from the CSPC SQL database.	4.9	More Details
CVE-2021-40130	A vulnerability in the web application of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to specify non-log files as sources for syslog reporting. This vulnerability is due to improper restriction of the syslog configuration. An attacker could exploit this vulnerability by configuring non-log files as sources for syslog reporting through the web application. A successful exploit could allow the attacker to read non-log files on the CSPC.	4.9	More Details
CVE-2021-36310	Dell Networking OS10, versions 10.4.3.x, 10.5.0.x, 10.5.1.x & 10.5.2.x, contain an uncontrolled resource consumption flaw in its API service. A high-privileged API user may potentially exploit this vulnerability, leading to a denial of service.	4.9	More Details
CVE-2021-24830	The Advanced Access Manager WordPress plugin before 6.8.0 does not escape some of its settings when outputting them, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24841	The Helpful WordPress plugin before 4.4.59 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24598	The Testimonial WordPress plugin before 1.6.0 does not escape some testimonial fields which could allow high privilege users to perform Cross Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24713	The Video Lessons Manager WordPress plugin before 1.7.2 and Video Lessons Manager Pro WordPress plugin before 3.5.9 do not properly sanitize and escape values when updating their settings, which could allow high privilege users to perform Cross-Site Scripting attacks	4.8	More Details
CVE-2021-24888	The ImageBoss WordPress plugin before 3.0.6 does not sanitise and escape its Source Name setting, which could allow high privilege users to perform Cross-Site Scripting attacks	4.8	More Details
CVE-2021-24882	The Slideshow Gallery WordPress plugin before 1.7.4 does not sanitise and escape the Slide "Title", "Description", and Gallery "Title" fields, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-24856	The Shared Files WordPress plugin before 1.6.61 does not sanitise and escape the Download Counter Text settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24787	The Client Invoicing by Sprout Invoices WordPress plugin before 19.9.7 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24700	The Forminator WordPress plugin before 1.15.4 does not sanitize and escape the email field label, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-42361	The Contact Form Email WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via the name parameter found in the ~/trunk/cp-admin-int-list.inc.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.3.24. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	4.8	More Details
CVE-2021-24815	The Accept Donations with PayPal WordPress plugin before 1.3.2 does not escape the Amount Menu Name field of created Buttons, which could allow a high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-36884	Authenticated Persistent Cross-Site Scripting (XSS) vulnerability discovered in WordPress Backup Migration plugin <= 1.1.5 versions.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43976	In the Linux kernel through 5.15.2, mwifiex_usb_recv in drivers/net/wireless/marvell/mwifiex/usb.c allows an attacker (who can connect a crafted USB device) to cause a denial of service (skb_over_panic).	4.6	More Details
CVE-2021-0659	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559.	4.4	More Details
CVE-2021-0148	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2021-0665	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113.	4.4	More Details
CVE-2021-0197	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local access.	4.4	More Details
CVE-2021-0198	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2021-0199	Improper input validation in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2021-27026	A flaw was divered in Puppet Enterprise and other Puppet products where sensitive plan parameters may be logged	4.4	More Details
CVE-2021-0666	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086.	4.4	More Details
CVE-2021-24851	The Insert Pages WordPress plugin before 3.7.0 allows users with a role as low as Contributor to access content and metadata from arbitrary posts/pages regardless of their author and status (ie private), using a shortcode. Password protected posts/pages are not affected by such issue.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36335	Dell EMC CloudLink 7.1 and all prior versions contain an Improper Input Validation Vulnerability. A remote low privileged attacker, may potentially exploit this vulnerability, leading to execution of arbitrary files on the server	4.3	More Details
CVE-2021-24776	The WP Performance Score Booster WordPress plugin before 2.1 does not have CSRF check when saving its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	4.3	More Details
CVE-2021-24853	The QR Redirector WordPress plugin before 1.6 does not have capability and CSRF checks when saving bulk QR Redirector settings via the qr_save_bulk AJAX action, which could allow any authenticated user, such as subscriber to change the redirect response status code of arbitrary QR Redirects	4.3	More Details
CVE-2021-38004	Insufficient policy enforcement in Autofill in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-24668	The MAZ Loader WordPress plugin before 1.4.1 does not enforce nonce checks, which allows attackers to make administrators delete arbitrary loaders via a CSRF attack	4.3	More Details
CVE-2021-41273	Pterodactyl is an open-source game server management panel built with PHP 7, React, and Go. Due to improperly configured CSRF protections on two routes, a malicious user could execute a CSRF-based attack against the following endpoints: Sending a test email and Generating a node auto-deployment token. At no point would any data be exposed to the malicious user, this would simply trigger email spam to an administrative user, or generate a single auto-deployment token unexpectedly. This token is not revealed to the malicious user, it is simply created unexpectedly in the system. This has been addressed in release `1.6.6`. Users may optionally manually apply the fixes released in v1.6.6 to patch their own systems.	4.3	More Details
CVE-2021-37938	It was discovered that on Windows operating systems specifically, Kibana was not validating a user supplied path, which would load .pbf files. Because of this, a malicious user could arbitrarily traverse the Kibana host to load internal files ending in the .pbf extension. Thanks to Dominic Couture for finding this vulnerability.	4.3	More Details
CVE-2021-3963	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3957	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-38378	OX App Suite 7.10.5 allows Information Exposure because a caching mechanism can caused a Modified By response to show a person's name.	4.3	More Details
CVE-2021-39198	OroCRM is an open source Client Relationship Management (CRM) application. Affected versions we found to suffer from a vulnerability which could an attacker is able to disqualify any Lead with a Cross-Site Request Forgery (CSRF) attack. There are no workarounds that address this vulnerability and all users are advised to update their package.	4.2	More Details
CVE-2021-43017	Adobe Creative Cloud version 5.5 (and earlier) are affected by an Application denial of service vulnerability in the Creative Cloud Desktop installer. An authenticated attacker with root privileges could leverage this vulnerability to achieve denial of service by planting a malicious file on the victim's local machine. User interaction is required before product installation to abuse this vulnerability.	4.2	More Details
CVE-2021-1088	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure.	4.1	More Details
CVE-2021-1105	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure.	4.1	More Details
CVE-2021-1125	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data.	4.1	More Details
CVE-2021-23219	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller, which may allow a user with elevated privileges to access protected information by identifying, exploiting, and loading vulnerable microcode. Such an attack may lead to information disclosure.	4.1	More Details
CVE-2021-34399	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34400	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	4.1	More Details
CVE-2021-32004	This issue affects: Secomea GateManager All versions prior to 9.6. Improper Check of host header in web server of Secomea GateManager allows attacker to cause browser cache poisoning.	3.7	More Details
CVE-2021-36319	Dell Networking OS10 versions 10.4.3.x, 10.5.0.x and 10.5.1.x contain an information exposure vulnerability. A low privileged authenticated malicious user can gain access to SNMP authentication failure messages.	3.3	More Details
CVE-2019-5640	Rapid7 Nexpose versions prior to 6.6.114 suffer from an information exposure issue whereby, when the user's session has ended due to inactivity, an attacker can use the inspect element browser feature to remove the login panel and view the details available in the last webpage visited by previous user	3.3	More Details
CVE-2021-43553	PI Vision could disclose information to a user with insufficient privileges for an AF attribute that is the child of another attribute and is configured as a Limits property.	3.1	More Details
CVE-2021-41190	The OCI Distribution Spec project defines an API protocol to facilitate and standardize the distribution of content. In the OCI Distribution Specification version 1.0.0 and prior, the Content-Type header alone was used to determine the type of document during push and pull operations. Documents that contain both “manifests” and “layers” fields could be interpreted as either a manifest or an index in the absence of an accompanying Content-Type header. If a Content-Type header changed between two pulls of the same digest, a client may interpret the resulting content differently. The OCI Distribution Specification has been updated to require that a mediaType value present in a manifest or index match the Content-Type header used during the push and pull operations. Clients pulling from a registry may distrust the Content-Type header and reject an ambiguous document that contains both “manifests” and “layers” fields or “manifests” and “config” fields if they are unable to update to version 1.0.1 of the spec.	3.0	More Details
CVE-2021-37939	It was discovered that Kibana’s JIRA connector & IBM Resilient connector could be used to return HTTP response data on internal hosts, which may be intentionally hidden from public view. Using this vulnerability, a malicious user with the ability to create connectors, could utilize these connectors to view limited HTTP response data on hosts accessible to the cluster.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13926	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13928	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13929	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13923	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13931	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13930	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13936	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13932	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13933	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13934	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13935	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13921	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13937	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13922	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13915	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13892	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13891	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13890	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13883	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13882	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13881	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13880	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13939	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12007	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12002	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13938	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13948	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13940	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13956	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13969	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13968	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13967	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13966	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13965	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13964	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13963	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13962	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13961	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13960	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13959	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13958	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13957	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13955	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13941	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13954	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13953	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13952	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13951	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13950	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13949	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11997	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13947	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13946	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13945	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13944	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13943	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13942	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-12000	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11944	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11992	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2015-9086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9080	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9081	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9082	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9083	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-9078	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9089	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9090	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9091	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9092	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9093	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9079	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9077	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2018-11991	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42271	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious BMP file.	N/A	More Details
CVE-2021-40733	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .psd file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-40751	Adobe After Effects version 18.4 (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 in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-40752	Adobe After Effects version 18.4 (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 in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-40753	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-40754	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-42270	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious BMP file.	N/A	More Details
CVE-2021-42272	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious GIF file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-9076	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2021-42524	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious BMP file.	N/A	More Details
CVE-2021-42525	Acrobat Animate versions 21.0.9 (and earlier)is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-40775	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-40772	Adobe Prelude version 10.1 (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 in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-40771	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2015-9075	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9094	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-9117	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2018-11896	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11841	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11844	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11848	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11885	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11887	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11890	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11900	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2015-9121	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2018-11901	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11915	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-11926	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11957	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11979	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11990	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11839	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11835	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11834	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11833	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11831	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11829	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11306	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11303	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-8249	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8232	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-14874	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2015-9225	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9214	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9168	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9155	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9154	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-9074	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details