SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 January 2022

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-2022-21675	Bytecode Viewer (BCV) is a Java/Android reverse engineering suite. Versions of the package prior to 2.11.0 are vulnerable to Arbitrary File Write via Archive Extraction (AKA "Zip Slip"). The vulnerability is exploited using a specially crafted archive that holds directory traversal filenames (e.g. ../../evil.exe). The Zip Slip vulnerability can affect numerous archive formats, including zip, jar, tar, war, cpio, apk, rar and 7z. The attacker can then overwrite executable files and either invoke them remotely or wait for the system or user to call them, thus achieving remote command execution on the victim's machine. The impact of a Zip Slip vulnerability would allow an attacker to create or overwrite existing files on the filesystem. In the context of a web application, a web shell could be placed within the application directory to achieve code execution. All users should upgrade to BCV v2.11.0 when possible to receive a patch. There are no recommended workarounds aside from upgrading.	9.9	More Details
CVE-2021-45411	In Sourcecodetester Printable Staff ID Card Creator System 1.0 after compromising the database via SQLi, an attacker can log in and leverage an arbitrary file upload vulnerability to obtain remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22566	An incorrect setting of UXN bits within mmu_flags_to_s1_pte_attr lead to privileged executable pages being mapped as executable from an unprivileged context. This can be leveraged by an attacker to bypass executability restrictions of kernel-mode pages from user-mode. An incorrect setting of PXN bits within mmu_flags_to_s1_pte_attr lead to unprivileged executable pages being mapped as executable from a privileged context. This can be leveraged by an attacker to bypass executability restrictions of user-mode pages from kernel-mode. Typically this allows a potential attacker to circumvent a mitigation, making exploitation of potential kernel-mode vulnerabilities easier. We recommend updating kernel beyond commit 7d731b4e9599088ac3073956933559da7bca6a00 and rebuilding.	9.8	More Details
CVE-2021-4171	calibre-web is vulnerable to Business Logic Errors	9.8	More Details
CVE-2022-0239	corenlp is vulnerable to Improper Restriction of XML External Entity Reference	9.8	More Details
CVE-2022-23304	The implementations of EAP-pwd in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side-channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9495.	9.8	More Details
CVE-2022-23303	The implementations of SAE in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9494.	9.8	More Details
CVE-2022-23178	An issue was discovered on Crestron HD-MD4X2-4K-E 1.0.0.2159 devices. When the administrative web interface of the HDMI switcher is accessed unauthenticated, user credentials are disclosed that are valid to authenticate to the web interface. Specifically, aj.html sends a JSON document with uname and upassword fields.	9.8	More Details
CVE-2021-33963	China Mobile An Lianbao WF-1 v1.0.1 router web interface through /api/ZRMacClone/mac_addr_clone receives parameters by POST request, and the parameter macType has a command injection vulnerability. An attacker can use the vulnerability to execute remote commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24044	By passing invalid javascript code where await and yield were called upon non-async and non-generator getter/setter functions, Hermes would invoke generator functions and error out on invalid await/yield positions. This could result in segmentation fault as a consequence of type confusion error, with a low chance of RCE. This issue affects Hermes versions prior to v0.10.0.	9.8	More Details
CVE-2021-44530	An injection vulnerability exists in a third-party library used in UniFi Network Version 6.5.53 and earlier (Log4J CVE-2021-44228) allows a malicious actor to control the application.	9.8	More Details
CVE-2021-39623	In doRead of SimpleDecodingSource.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194105348	9.8	More Details
CVE-2022-23305	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.	9.8	More Details
CVE-2021-29215	A potential security vulnerability in HPE Ezmeral Data Fabric that may allow a remote access restriction bypass in the TEZ MapR ecosystem component was discovered in version(s): Prior to Tez-0.8: mapr-tez-0.8.201907081100-1.noarch; prior to Tez-0.9: mapr-tez-0.9.201907090334-1.noarch; prior to Tez-0.9.2: mapr-tez-0.9.2.0.201907081043-1.noarch. HPE has provided software updates to resolve the vulnerability in the TEZ MapR ecosystem component in HPE Ezmeral Data Fabric.	9.8	More Details
CVE-2021-1049	Hacker one bug ID: 1343975Product: AndroidVersions: Android SoCAndroid ID: A-204256722	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23227	NUUO NVRmini2 through 3.11 allows an unauthenticated attacker to upload an encrypted TAR archive, which can be abused to add arbitrary users because of the lack of handle_import_user.php authentication. When combined with another flaw (CVE-2011-5325), it is possible to overwrite arbitrary files under the web root and achieve code execution as root.	9.8	More Details
CVE-2022-0224	dolibarr is vulnerable to Improper Neutralization of Special Elements used in an SQL Command	9.8	More Details
CVE-2021-45468	Imperva Web Application Firewall (WAF) before 2021-12-23 allows remote unauthenticated attackers to use "Content-Encoding: gzip" to evade WAF security controls and send malicious HTTP POST requests to web servers behind the WAF.	9.8	More Details
CVE-2021-33962	China Mobile An Lianbao WF-1 router v1.0.1 is affected by an OS command injection vulnerability in the web interface /api/ZRUsb/pop_usb_device component.	9.8	More Details
CVE-2022-23219	The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.	9.8	More Details
CVE-2022-23218	The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.	9.8	More Details
CVE-2022-22056	The Le-yan dental management system contains a hard-coded credentials vulnerability in the web page source code, which allows an unauthenticated remote attacker to acquire administrator’s privilege and control the system or disrupt service.	9.8	More Details
CVE-2022-22055	The Le-yan dental management system contains an SQL-injection vulnerability. An unauthenticated remote attacker can inject SQL commands into the input field of the login page to acquire administrator’s privilege and perform arbitrary operations on the system or disrupt service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34993	This vulnerability allows remote attackers to bypass authentication on affected installations of Commvault CommCell 11.22.22. Authentication is not required to exploit this vulnerability. The specific flaw exists within the CVSearchService service. The issue results from the lack of proper validation prior to authentication. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-13706.	9.8	More Details
CVE-2022-22989	My Cloud OS 5 was vulnerable to a pre-authenticated stack overflow vulnerability on the FTP service that could be exploited by unauthenticated attackers on the network. Addressed the vulnerability by adding defenses against stack overflow issues.	9.8	More Details
CVE-2021-40722	AEM Forms Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by an XML External Entity (XXE) injection vulnerability that could be abused by an attacker to achieve RCE.	9.8	More Details
CVE-2021-33046	Some Dahua products have access control vulnerability in the password reset process. Attackers can exploit this vulnerability through specific deployments to reset device passwords.	9.8	More Details
CVE-2021-45807	jpress v4.2.0 is vulnerable to command execution via io.jpress.web.admin._AddonController::doUploadAndInstall.	9.8	More Details
CVE-2021-46013	An unrestricted file upload vulnerability exists in Sourcecodester Free school management software 1.0. An attacker can leverage this vulnerability to enable remote code execution on the affected web server. Once a php webshell containing "<?php system($_GET["cmd"]); ?>" gets uploaded it is saved into /uploads/exam_question/ directory, and is accessible by all users.	9.8	More Details
CVE-2021-38697	SoftVibe SARABAN for INFOMA 1.1 allows Unauthenticated unrestricted File Upload, that allows attackers to upload files with any file extension which can lead to arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20658	A vulnerability in the web-based management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) and Cisco Unified Contact Center Domain Manager (Unified CCDM) could allow an authenticated, remote attacker to elevate their privileges to Administrator. This vulnerability is due to the lack of server-side validation of user permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to a vulnerable system. A successful exploit could allow the attacker to create Administrator accounts. With these accounts, the attacker could access and modify telephony and user resources across all the Unified platforms that are associated to the vulnerable Cisco Unified CCMP. To successfully exploit this vulnerability, an attacker would need valid Advanced User credentials.	9.6	More Details
CVE-2021-30285	Improper validation of memory region in Hypervisor can lead to incorrect region mapping in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.3	More Details
CVE-2021-28500	An issue has recently been discovered in Arista EOS where the incorrect use of EOS's AAA API's by the OpenConfig and TerminAttr agents could result in unrestricted access to the device for local users with nopassword configuration.	9.1	More Details
CVE-2021-44757	Zoho ManageEngine Desktop Central before 10.1.2137.9 and Desktop Central MSP before 10.1.2137.9 allow attackers to bypass authentication, and read sensitive information or upload an arbitrary ZIP archive to the server.	9.1	More Details
CVE-2021-28506	An issue has recently been discovered in Arista EOS where certain gNOI APIs incorrectly skip authorization and authentication which could potentially allow a factory reset of the device.	9.1	More Details
CVE-2021-28501	An issue has recently been discovered in Arista EOS where the incorrect use of EOS's AAA API's by the OpenConfig and TerminAttr agents could result in unrestricted access to the device for local users with nopassword configuration.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23131	In the case of instances where the SAML SSO authentication is enabled (non-default), session data can be modified by a malicious actor, because a user login stored in the session was not verified. Malicious unauthenticated actor may exploit this issue to escalate privileges and gain admin access to Zabbix Frontend. To perform the attack, SAML authentication is required to be enabled and the actor has to know the username of Zabbix user (or use the guest account, which is disabled by default).	9.1	More Details
CVE-2022-23408	wolfSSL 5.x before 5.1.1 uses non-random IV values in certain situations. This affects connections (without AEAD) using AES-CBC or DES3 with TLS 1.1 or 1.2 or DTLS 1.1 or 1.2. This occurs because of misplaced memory initialization in BuildMessage in internal.c.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-34995	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Commvault CommCell 11.22.22. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the DownloadCenterUploadHandler class. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE. Was ZDI-CAN-13756.	8.8	More Details
CVE-2022-0180	Cross-site request forgery (CSRF) vulnerability in Quiz And Survey Master versions prior to 7.3.7 allows a remote attacker to hijack the authentication of administrators and conduct arbitrary operations via a specially crafted web page.	8.8	More Details
CVE-2022-20617	Jenkins Docker Commons Plugin 1.17 and earlier does not sanitize the name of an image or a tag, resulting in an OS command execution vulnerability exploitable by attackers with Item/Configure permission or able to control the contents of a previously configured job's SCM repository.	8.8	More Details
CVE-2022-23118	Jenkins Debian Package Builder Plugin 1.6.11 and earlier implements functionality that allows agents to invoke command-line `git` at an attacker-specified path on the controller, allowing attackers able to control agent processes to invoke arbitrary OS commands on the controller.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0196	phoronix-test-suite is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2022-0197	phoronix-test-suite is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2022-22113	In DayByDay CRM, versions 2.2.0 through 2.2.1 (latest) are vulnerable to Insufficient Session Expiration. When a password has been changed by the user or by an administrator, a user that was already logged in, will still have access to the application even after the password was changed.	8.8	More Details
CVE-2021-45806	jpress v4.2.0 admin panel provides a function through which attackers can modify the template and inject some malicious code.	8.8	More Details
CVE-2022-23302	JMSSink in all versions of Log4j 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration or if the configuration references an LDAP service the attacker has access to. The attacker can provide a TopicConnectionFactoryBindingName configuration causing JMSSink to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-4104. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.	8.8	More Details
CVE-2022-0215	The Login/Signup Popup, Waitlist Woocommerce (Back in stock notifier), and Side Cart Woocommerce (Ajax) WordPress plugins by XootiX are vulnerable to Cross-Site Request Forgery via the save_settings function found in the ~/includes/xoo-framework/admin/class-xoo-admin-settings.php file which makes it possible for attackers to update arbitrary options on a site that can be used to create an administrative user account and grant full privileged access to a compromised site. This affects versions <= 2.2 in Login/Signup Popup, versions <= 2.5.1 in Waitlist Woocommerce (Back in stock notifier), and versions <= 2.0 in Side Cart Woocommerce (Ajax).	8.8	More Details
CVE-2022-23307	CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33828	The files_antivirus component before 1.0.0 for ownCloud mishandles the protection mechanism by which malicious files (that have been uploaded to a public share) are supposed to be deleted upon detection.	8.8	More Details
CVE-2021-25036	The All in One SEO WordPress plugin before 4.1.5.3 is affected by a Privilege Escalation issue, which was discovered during an internal audit by the Jetpack Scan team, and may grant bad actors access to protected REST API endpoints they shouldn't have access to. This could ultimately enable users with low-privileged accounts, like subscribers, to perform remote code execution on affected sites.	8.8	More Details
CVE-2021-41597	SuiteCRM through 7.11.21 is vulnerable to CSRF, with resultant remote code execution, via the UpgradeWizard functionality, if a PHP file is included in a ZIP archive.	8.8	More Details
CVE-2021-4164	calibre-web is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2022-0258	pimcore is vulnerable to Improper Neutralization of Special Elements used in an SQL Command	8.8	More Details
CVE-2021-38965	IBM FileNet Content Manager 5.5.4, 5.5.6, and 5.5.7 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 212346.	8.8	More Details
CVE-2021-33964	China Mobile An Lianbao WF-1 V1.0.1 router provides a web interface /api/ZRRuleFilter/set_firewall_level which receives parameters by POST request, and the parameter firewall_level has a command injection vulnerability. An attacker can use the vulnerability to execute remote commands.	8.8	More Details
CVE-2021-45394	An issue was discovered in Spipu HTML2PDF before 5.2.4. Attackers can trigger deserialization of arbitrary data via the injection of a malicious <link> tag in the converted HTML document.	8.8	More Details
CVE-2021-33965	China Mobile An Lianbao WF-1 V1.0.1 router provides a web interface /api/ZRMesh/set_ZRMesh which receives parameters by POST request, and the parameter mesh_enable and mesh_device have a command injection vulnerability. An attacker can use the vulnerability to execute remote commands.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43353	The Crisp Live Chat WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the crisp_plugin_settings_page function found in the ~/crisp.php file, which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 0.31.	8.8	More Details
CVE-2021-34994	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Commvault CommCell 11.22.22. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the DataProvider class. The issue results from the lack of proper validation of a user-supplied string before executing it as JavaScript code. An attacker can leverage this vulnerability to escape the JavaScript sandbox and execute Java code in the context of NETWORK SERVICE. Was ZDI-CAN-13755.	8.8	More Details
CVE-2021-32650	October CMS is a self-hosted content management system (CMS) platform based on the Laravel PHP Framework. Prior to versions 1.0.473 and 1.1.6, an attacker with access to the backend is able to execute PHP code by using the theme import feature. This will bypass the safe mode feature that prevents PHP execution in the CMS templates.The issue has been patched in Build 473 (v1.0.473) and v1.1.6. Those unable to upgrade may apply the patch to their installation manually as a workaround.	8.8	More Details
CVE-2021-32649	October CMS is a self-hosted content management system (CMS) platform based on the Laravel PHP Framework. Prior to versions 1.0.473 and 1.1.6, an attacker with "create, modify and delete website pages" privileges in the backend is able to execute PHP code by running specially crafted Twig code in the template markup. The issue has been patched in Build 473 (v1.0.473) and v1.1.6. Those unable to upgrade may apply the patch to their installation manually as a workaround.	8.8	More Details
CVE-2021-42559	An issue was discovered in CALDERA 2.8.1. It contains multiple startup "requirements" that execute commands when starting the server. Because these commands can be changed via the REST API, an authenticated user can insert arbitrary commands that will execute when the server is restarted.	8.8	More Details
CVE-2021-45406	In SalonERP 3.0.1, a SQL injection vulnerability allows an attacker to inject payload using 'sql' parameter in SQL query while generating a report. Upon successfully discovering the login admin password hash, it can be decrypted to obtain the plain-text password.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34979	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6260 1.1.0.78_1.0.1 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SOAP requests. When parsing the SOAPAction header, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13512.	8.8	More Details
CVE-2021-34996	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Commvault CommCell 11.22.22. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Demo_ExecuteProcessOnGroup workflow. By creating a workflow, an attacker can specify an arbitrary command to be executed. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-13889.	8.8	More Details
CVE-2021-44651	Zoho ManageEngine CloudSecurityPlus before Build 4117 allows remote code execution through the updatePersonalizeSettings component due to an improper security patch for CVE-2021-40175.	8.8	More Details
CVE-2021-4080	crater is vulnerable to Unrestricted Upload of File with Dangerous Type	8.8	More Details
CVE-2021-42560	An issue was discovered in CALDERA 2.9.0. The Debrief plugin receives base64 encoded "SVG" parameters when generating a PDF document. These SVG documents are parsed in an unsafe manner and can be leveraged for XXE attacks (e.g., File Exfiltration, Server Side Request Forgery, Out of Band Exfiltration, etc.).	8.8	More Details
CVE-2021-34977	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R7000 1.0.11.116_10.2.100 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of SOAP requests. The issue results from the lack of proper authentication verification before performing a password reset. An attacker can leverage this vulnerability to reset the admin password. Was ZDI-CAN-13483.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34997	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Commvault CommCell 11.22.22. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the AppStudioUploadHandler class. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE. Was ZDI-CAN-13894.	8.8	More Details
CVE-2021-34978	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6260 1.1.0.78_1.0.1 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the setupwizard.cgi page. A crafted SOAP request can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13511.	8.8	More Details
CVE-2021-42561	An issue was discovered in CALDERA 2.8.1. When activated, the Human plugin passes the unsanitized name parameter to a python "os.system" function. This allows attackers to use shell metacharacters (e.g., backticks "``" or dollar parenthesis "$()") in order to escape the current command and execute arbitrary shell commands.	8.8	More Details
CVE-2021-44648	GNOME gdk-pixbuf 2.42.6 is vulnerable to a heap-buffer overflow vulnerability when decoding the lzw compressed stream of image data in GIF files with lzw minimum code size equals to 12.	8.8	More Details
CVE-2021-34980	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6260 1.1.0.78_1.0.1 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the setupwizard.cgi page. When parsing the SOAP_LOGIN_TOKEN environment variable, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-14107.	8.8	More Details
CVE-2022-21690	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions The path parameter of the requested URL is not sanitized before being passed to the QT frontend. This path is used in all components for displaying the server access history. This leads to a rendered HTML4 Subset (QT RichText editor) in the Onionshare frontend.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39946	Improper neutralization of user input in GitLab CE/EE versions 14.3 to 14.3.6, 14.4 to 14.4.4, and 14.5 to 14.5.2 allowed an attacker to exploit XSS by abusing the generation of the HTML code related to emojis	8.7	More Details
CVE-2022-22690	Within the Umbraco CMS, a configuration element named "UmbracoApplicationUrl" (or just "ApplicationUrl") is used whenever application code needs to build a URL pointing back to the site. For example, when a user resets their password and the application builds a password reset URL or when the administrator invites users to the site. For Umbraco versions less than 9.2.0, if the Application URL is not specifically configured, the attacker can manipulate this value and store it persistently affecting all users for components where the "UmbracoApplicationUrl" is used. For example, the attacker is able to change the URL users receive when resetting their password so that it points to the attackers server, when the user follows this link the reset token can be intercepted by the attacker resulting in account takeover.	8.6	More Details
CVE-2022-0244	An issue has been discovered in GitLab CE/EE affecting all versions starting with 14.5. Arbitrary file read was possible by importing a group was due to incorrect handling of file.	8.6	More Details
CVE-2021-43860	Flatpak is a Linux application sandboxing and distribution framework. Prior to versions 1.12.3 and 1.10.6, Flatpak doesn't properly validate that the permissions displayed to the user for an app at install time match the actual permissions granted to the app at runtime, in the case that there's a null byte in the metadata file of an app. Therefore apps can grant themselves permissions without the consent of the user. Flatpak shows permissions to the user during install by reading them from the "xa.metadata" key in the commit metadata. This cannot contain a null terminator, because it is an untrusted GVariant. Flatpak compares these permissions to the *actual* metadata, from the "metadata" file to ensure it wasn't lied to. However, the actual metadata contents are loaded in several places where they are read as simple C-style strings. That means that, if the metadata file includes a null terminator, only the content of the file from *before* the terminator gets compared to xa.metadata. Thus, any permissions that appear in the metadata file after a null terminator are applied at runtime but not shown to the user. So maliciously crafted apps can give themselves hidden permissions. Users who have Flatpaks installed from untrusted sources are at risk in case the Flatpak has a maliciously crafted metadata file, either initially or in an update. This issue is patched in versions 1.12.3 and 1.10.6. As a workaround, users can manually check the permissions of installed apps by checking the metadata file or the xa.metadata key on the commit metadata.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43765	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	8.1	More Details
CVE-2022-22530	The F0743 Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104, 105, 106, does not check uploaded or downloaded files. This allows an attacker with basic user rights to inject dangerous content or malicious code which could result in critical information being modified or completely compromise the availability of the application.	8.1	More Details
CVE-2021-38690	A stack buffer overflow vulnerability has been reported to affect QNAP device running QVR Elite, QVR Pro, QVR Guard. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QVR Elite, QVR Pro, QVR Guard: QuTS hero h5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QuTS hero h4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 4.5.4: QVR Guard 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Guard 2.1.3.0 (2021/12/06) and later	8.1	More Details
CVE-2021-46255	eyouCMS V1.5.5-UTF8-SP3_1 suffers from Arbitrary file deletion due to insufficient filtering of the parameter filename.	8.1	More Details
CVE-2021-42562	An issue was discovered in CALDERA 2.8.1. It does not properly segregate user privileges, resulting in non-admin users having access to read and modify configuration or other components that should only be accessible by admin users.	8.1	More Details
CVE-2021-38691	A stack buffer overflow vulnerability has been reported to affect QNAP device running QVR Elite, QVR Pro, QVR Guard. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QVR Elite, QVR Pro, QVR Guard: QuTS hero h5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QuTS hero h4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 4.5.4: QVR Guard 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Guard 2.1.3.0 (2021/12/06) and later	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38682	A stack buffer overflow vulnerability has been reported to affect QNAP device running QVR Elite, QVR Pro, QVR Guard. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QVR Elite, QVR Pro, QVR Guard: QuTS hero h5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QuTS hero h4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 4.5.4: QVR Guard 2.1.3.0 and later QTS 5.0.0: QVR Guard 2.1.3.0 and later	8.1	More Details
CVE-2021-38689	A stack buffer overflow vulnerability has been reported to affect QNAP device running QVR Elite, QVR Pro, QVR Guard. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QVR Elite, QVR Pro, QVR Guard: QuTS hero h5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QuTS hero h4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 4.5.4: QVR Guard 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Guard 2.1.3.0 (2021/12/06) and later	8.1	More Details
CVE-2022-22531	The F0743 Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104, 105, 106, does not check uploaded or downloaded files. This allows an attacker with basic user rights to run arbitrary script code, resulting in sensitive information being disclosed or modified.	8.1	More Details
CVE-2022-0130	Tenable.sc versions 5.14.0 through 5.19.1 were found to contain a remote code execution vulnerability which could allow a remote, unauthenticated attacker to execute code under special circumstances. An attacker would first have to stage a specific file type in the web server root of the Tenable.sc host prior to remote exploitation.	8.1	More Details
CVE-2021-44177	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	8.1	More Details
CVE-2021-44176	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23107	Jenkins Warnings Next Generation Plugin 9.10.2 and earlier does not restrict the name of a file when configuring custom ID, allowing attackers with Item/Configure permission to write and read specific files with a hard-coded suffix on the Jenkins controller file system.	8.1	More Details
CVE-2021-38692	A stack buffer overflow vulnerability has been reported to affect QNAP device running QVR Elite, QVR Pro, QVR Guard. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QVR Elite, QVR Pro, QVR Guard: QuTS hero h5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QuTS hero h4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 4.5.4: QVR Guard 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Guard 2.1.3.0 (2021/12/06) and later	8.1	More Details
CVE-2021-43764	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	8.0	More Details
CVE-2021-43761	AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	8.0	More Details
CVE-2021-34942	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-15041.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14110	AX3600 router sensitive information leaked.There is an unauthorized interface through luci to obtain sensitive information and log in to the web background.	7.8	More Details
CVE-2021-34941	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15040.	7.8	More Details
CVE-2021-34940	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15039.	7.8	More Details
CVE-2021-34939	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14996.	7.8	More Details
CVE-2021-34891	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14844.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34945	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15054.	7.8	More Details
CVE-2021-34933	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14911.	7.8	More Details
CVE-2021-34885	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-14838.	7.8	More Details
CVE-2021-34946	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-15055.	7.8	More Details
CVE-2021-34892	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14845.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34880	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. Crafted data in a 3DS 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. Was ZDI-CAN-14833.	7.8	More Details
CVE-2021-34879	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14832.	7.8	More Details
CVE-2021-34878	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14830.	7.8	More Details
CVE-2021-34877	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14829.	7.8	More Details
CVE-2021-34876	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14828.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34875	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. Crafted data in a 3DS file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14827.	7.8	More Details
CVE-2021-34874	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14736.	7.8	More Details
CVE-2021-34873	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. Crafted data in a PDF file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14696.	7.8	More Details
CVE-2021-34872	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SKP files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14737.	7.8	More Details
CVE-2021-34871	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14695.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34938	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14995.	7.8	More Details
CVE-2021-34898	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14865.	7.8	More Details
CVE-2021-34893	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14846.	7.8	More Details
CVE-2021-34923	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14901.	7.8	More Details
CVE-2021-34914	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14892.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34915	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14893.	7.8	More Details
CVE-2021-34917	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14895.	7.8	More Details
CVE-2021-34918	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. Crafted data in a JP2 file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14896.	7.8	More Details
CVE-2021-34919	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14897.	7.8	More Details
CVE-2021-34920	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14898.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34921	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14899.	7.8	More Details
CVE-2021-34922	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14900.	7.8	More Details
CVE-2021-34924	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14902.	7.8	More Details
CVE-2021-34912	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-14885.	7.8	More Details
CVE-2021-34925	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14903.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34926	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14904.	7.8	More Details
CVE-2021-34927	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-14905.	7.8	More Details
CVE-2021-34928	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14906.	7.8	More Details
CVE-2021-34929	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14907.	7.8	More Details
CVE-2021-34930	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-14908.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34931	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14909.	7.8	More Details
CVE-2021-34998	This vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Free Antivirus 20.2.0.0. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the use of named pipes. The issue results from allowing an untrusted process to impersonate the client of a pipe. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-14208.	7.8	More Details
CVE-2021-34913	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT 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. Was ZDI-CAN-14831.	7.8	More Details
CVE-2021-34911	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14884.	7.8	More Details
CVE-2021-34894	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14847.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34936	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14914.	7.8	More Details
CVE-2021-34895	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14862.	7.8	More Details
CVE-2021-34896	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14863.	7.8	More Details
CVE-2021-34897	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14864.	7.8	More Details
CVE-2021-34934	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14912.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34899	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14866.	7.8	More Details
CVE-2021-34900	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14867.	7.8	More Details
CVE-2021-34937	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14915.	7.8	More Details
CVE-2022-0263	Unrestricted Upload of File with Dangerous Type in Packagist pimcore/pimcore prior to 10.2.7.	7.8	More Details
CVE-2021-34935	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14913.	7.8	More Details
CVE-2022-0261	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34903	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. Crafted data in a BMP file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14876.	7.8	More Details
CVE-2022-22991	A malicious user on the same LAN could use DNS spoofing followed by a command injection attack to trick a NAS device into loading through an unsecured HTTP call. Addressed this vulnerability by disabling checks for internet connectivity using HTTP.	7.8	More Details
CVE-2021-34904	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14877.	7.8	More Details
CVE-2021-34905	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14878.	7.8	More Details
CVE-2021-34906	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14879.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34907	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14880.	7.8	More Details
CVE-2021-34908	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14881.	7.8	More Details
CVE-2021-34909	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14882.	7.8	More Details
CVE-2021-34858	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TeamViewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TVS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13606.	7.8	More Details
CVE-2021-34932	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14910.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22990	A limited authentication bypass vulnerability was discovered that could allow an attacker to achieve remote code execution and escalate privileges on the My Cloud devices. Addressed this vulnerability by changing access token validation logic and rewriting rule logic on PHP scripts.	7.8	More Details
CVE-2021-39678	In <TBD> of <TBD>, there is a possible bypass of Factory Reset Protection due to <TBD>. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171742549References: N/A	7.8	More Details
CVE-2021-39681	In delete_protocol of main.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-200251074References: N/A	7.8	More Details
CVE-2021-39682	In mgm_alloc_page of memory_group_manager.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-201677538References: N/A	7.8	More Details
CVE-2021-34401	NVIDIA Linux kernel distributions contain a vulnerability in nvmap NVGPU_IOCTL_CHANNEL_SET_ERROR_NOTIFIER, where improper access control may lead to code execution, compromised integrity, or denial of service.	7.8	More Details
CVE-2021-39684	In target_init of gs101/abl/target/slider/target.c, there is a possible allocation of RWX memory due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-203250788References: N/A	7.8	More Details
CVE-2021-44701	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44703	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a stack buffer overflow vulnerability due to insecure handling of a crafted file, potentially resulting 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-2021-44704	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-44705	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-44706	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-44707	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (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 file.	7.8	More Details
CVE-2021-44708	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a heap overflow vulnerability due to insecure handling of a crafted file, potentially resulting 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 Number	Description	Base Score	Reference
CVE-2021-44709	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a heap overflow vulnerability due to insecure handling of a crafted file, potentially resulting 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-2021-44710	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-44711	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Integer Overflow or Wraparound 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 file.	7.8	More Details
CVE-2021-44828	Arm Mali GPU Kernel Driver (Midgard r26p0 through r30p0, Bifrost r0p0 through r34p0, and Valhall r19p0 through r34p0) allows a non-privileged user to achieve write access to read-only memory, and possibly obtain root privileges, corrupt memory, and modify the memory of other processes.	7.8	More Details
CVE-2021-34403	NVIDIA Linux distributions contain a vulnerability in nvmap ioctl, which allows any user with a local account to exploit a use-after-free condition, leading to code privilege escalation, loss of confidentiality and integrity, or denial of service.	7.8	More Details
CVE-2021-39634	In fs/eventpoll.c, there is a possible use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-204450605References: Upstream kernel	7.8	More Details
CVE-2021-45061	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (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 file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39632	In inotify_cb of events.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-202159709	7.8	More Details
CVE-2021-0959	In jit_memory_region.cc, there is a possible bypass of memory restrictions due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-200284993	7.8	More Details
CVE-2021-1035	In setLaunchIntent of BluetoothDevicePickerPreferenceController.java, there is a possible way to invoke an arbitrary broadcast receiver due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-12Android ID: A-195668284	7.8	More Details
CVE-2021-1036	In LocationSettingsActivity of AndroidManifest.xml, there is a possible EoP due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-182812255	7.8	More Details
CVE-2021-44652	Zoho ManageEngine O365 Manager Plus before Build 4416 allows remote code execution via BCP file overwrite through the ChangeDBAPI component.	7.8	More Details
CVE-2021-23138	WECON LeviStudioU Versions 2019-09-21 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute code.	7.8	More Details
CVE-2021-23157	WECON LeviStudioU Versions 2019-09-21 and prior are vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute code.	7.8	More Details
CVE-2021-39618	In multiple methods of EuiccNotificationManager.java, there is a possible way to install existing packages without user consent due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-196855999	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39620	In ipcSetDataReference of Parcel.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-203847542	7.8	More Details
CVE-2021-39621	In sendLegacyVoicemailNotification of LegacyModeSmsHandler.java, there is a possible permissions bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-185126319	7.8	More Details
CVE-2021-39622	In GBoard, there is a possible way to bypass Factory Reset Protection due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-192663648	7.8	More Details
CVE-2022-0015	A local privilege escalation (PE) vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables an authenticated local user to execute programs with elevated privileges. This issue impacts: Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.12; Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.9.	7.8	More Details
CVE-2021-39626	In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194695497	7.8	More Details
CVE-2021-36417	A heap-based buffer overflow vulnerability exists in GPAC v1.0.1 in the gf_isom_dovi_config_get function in MP4Box, which causes a denial of service or execute arbitrary code via a crafted file.	7.8	More Details
CVE-2021-39627	In sendLegacyVoicemailNotification of LegacyModeSmsHandler.java, there is a possible permissions bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-185126549	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39630	In executeRequest of OverlayManagerService.java, there is a possible way to control fabricated overlays from adb shell due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-202768292	7.8	More Details
CVE-2021-45060	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-44743	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (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 file.	7.8	More Details
CVE-2021-45062	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-44049	CyberArk Endpoint Privilege Manager (EPM) through 11.5.3.328 before 2021-12-20 allows a local user to gain elevated privileges via a Trojan horse Procmon64.exe in the user's Temp directory.	7.8	More Details
CVE-2021-45058	Adobe InDesign version 16.4 (and earlier) is 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 JPEG file.	7.8	More Details
CVE-2021-45057	Adobe InDesign version 16.4 (and earlier) is 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 JPEG2000 file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45056	Adobe InCopy version 16.4 (and earlier) is 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 file.	7.8	More Details
CVE-2021-45055	Adobe InCopy version 16.4 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-23222	kernel/bpf/verifier.c in the Linux kernel through 5.15.14 allows local users to gain privileges because of the availability of pointer arithmetic via certain *_OR_NULL pointer types.	7.8	More Details
CVE-2021-45053	Adobe InCopy version 16.4 (and earlier) is 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 file.	7.8	More Details
CVE-2021-40574	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the gf_text_get_utf8_line function in load_text.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	7.8	More Details
CVE-2021-40571	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the ilst_box_read function in box_code_apple.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	7.8	More Details
CVE-2021-40570	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the avc_compute_poc function in av_parsers.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	7.8	More Details
CVE-2021-40568	A buffer overflow vulnerability exists in Gpac through 1.0.1 via a malformed MP4 file in the svc_parse_slice function in av_parsers.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45064	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-23095	Open Design Alliance Drawings SDK before 2022.12.1 mishandles the loading of JPG files. Unchecked input data from a crafted JPG file leads to memory corruption. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-44537	ownCloud owncloud/client before 2.9.2 allows Resource Injection by a server into the desktop client via a URL, leading to remote code execution.	7.8	More Details
CVE-2021-45068	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (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 file.	7.8	More Details
CVE-2021-30311	Possible heap overflow due to lack of index validation before allocating and writing to heap buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2022-21137	Omron CX-One Versions 4.60 and prior are vulnerable to a stack-based buffer overflow while processing specific project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-30308	Possible buffer overflow while printing the HARQ memory partition detail due to improper validation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2021-30319	Possible integer overflow due to improper validation of command length parameters while processing WMI command in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21682	Flatpak is a Linux application sandboxing and distribution framework. A path traversal vulnerability affects versions of Flatpak prior to 1.12.3 and 1.10.6. flatpak-builder applies `finish-args` last in the build. At this point the build directory will have the full access that is specified in the manifest, so running `flatpak build` against it will gain those permissions. Normally this will not be done, so this is not problem. However, if `--mirror-screenshots-url` is specified, then flatpak-builder will launch `flatpak build --nofilesystem=host appstream-utils mirror-screenshots` after finalization, which can lead to issues even with the `--nofilesystem=host` protection. In normal use, the only issue is that these empty directories can be created wherever the user has write permissions. However, a malicious application could replace the `appstream-util` binary and potentially do something more hostile. This has been resolved in Flatpak 1.12.3 and 1.10.6 by changing the behaviour of `--nofilesystem=home` and `--nofilesystem=host`.	7.7	More Details
CVE-2022-22988	File and directory permissions have been corrected to prevent unintended users from modifying or accessing resources. It would be more difficult for an authenticated attacker to now traverse through the files and directories. This can only be exploited once an attacker has already found a way to get authenticated access to the device.	7.7	More Details
CVE-2021-3965	Certain HP DesignJet products may be vulnerable to unauthenticated HTTP requests which allow viewing and downloading of print job previews.	7.5	More Details
CVE-2021-38785	There is a NULL pointer deference in the Allwinner R818 SoC Android Q SDK V1.0 camera driver /dev/cedar_dev that could use the ioctl cmd IOCTL_GET_IOMMU_ADDR to cause a system crash.	7.5	More Details
CVE-2022-20698	A vulnerability in the OOXML parsing module in Clam AntiVirus (ClamAV) Software version 0.104.1 and LTS version 0.103.4 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper checks that may result in an invalid pointer read. An attacker could exploit this vulnerability by sending a crafted OOXML file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to crash, resulting in a denial of service condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20612	Lack of administrator control over security vulnerability in MELSEC-F series FX3U-ENET Firmware version 1.14 and prior, FX3U-ENET-L Firmware version 1.14 and prior and FX3U-ENET-P502 Firmware version 1.14 and prior allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition in communication function of the product or other unspecified effects by sending specially crafted packets to an unnecessary opening of TCP port. Control by MELSEC-F series PLC is not affected by this vulnerability, but system reset is required for recovery.	7.5	More Details
CVE-2021-20613	Improper initialization vulnerability in MELSEC-F series FX3U-ENET Firmware version 1.16 and prior, FX3U-ENET-L Firmware version 1.16 and prior and FX3U-ENET-P502 Firmware version 1.16 and prior allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition in communication function of the product by sending specially crafted packets. Control by MELSEC-F series PLC is not affected by this vulnerability, but system reset is required for recovery.	7.5	More Details
CVE-2021-45769	A NULL pointer dereference in AcseConnection_parseMessage at src/mms/iso_acse/acse.c of libiec61850 v1.5.0 can lead to a segmentation fault or application crash.	7.5	More Details
CVE-2021-45773	A NULL pointer dereference in CS104_IPAddress_setFromString at src/iec60870/cs104/cs104_slave.c of lib60870 commit 0d5e76e can lead to a segmentation fault or application crash.	7.5	More Details
CVE-2021-23567	The package colors after 1.4.0 are vulnerable to Denial of Service (DoS) that was introduced through an infinite loop in the americanFlag module. Unfortunately this appears to have been a purposeful attempt by a maintainer of colors to make the package unusable, other maintainers' controls over this package appear to have been revoked in an attempt to prevent them from fixing the issue. Vulnerable Code js for (let i = 666; i < Infinity; i++;) { Alternative Remediation Suggested * Pin dependancy to 1.4.0	7.5	More Details
CVE-2021-46020	An untrusted pointer dereference in mrb_vm_exec() of mruby v3.0.0 can lead to a segmentation fault or application crash.	7.5	More Details
CVE-2021-38783	There is a Out-of-Bound Write in the Allwinner R818 SoC Android Q SDK V1.0 camera driver "/dev/cedar_dev" through iotcl cmd IOCTL_SET_PROC_INFO and IOCTL_COPY_PROC_INFO, which could cause a system crash or EoP.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38784	There is a NULL pointer dereference in the syscall open_exec function of Allwinner R818 SoC Android Q SDK V1.0 that could executable a malicious file to cause a system crash.	7.5	More Details
CVE-2021-38696	SoftVibe SARABAN for INFOMA 1.1 has Incorrect Access Control vulnerability, that allows attackers to access signature files on the application without any authentication.	7.5	More Details
CVE-2021-46170	An issue was discovered in JerryScript commit a6ab5e9. There is an Use-After-Free in lexer_compare_identifier_to_string in js-lexer.c file.	7.5	More Details
CVE-2022-0240	mruby is vulnerable to NULL Pointer Dereference	7.5	More Details
CVE-2022-21681	Marked is a markdown parser and compiler. Prior to version 4.0.10, the regular expression `inline.reflinkSearch` may cause catastrophic backtracking against some strings and lead to a denial of service (DoS). Anyone who runs untrusted markdown through a vulnerable version of marked and does not use a worker with a time limit may be affected. This issue is patched in version 4.0.10. As a workaround, avoid running untrusted markdown through marked or run marked on a worker thread and set a reasonable time limit to prevent draining resources.	7.5	More Details
CVE-2022-21680	Marked is a markdown parser and compiler. Prior to version 4.0.10, the regular expression `block.def` may cause catastrophic backtracking against some strings and lead to a regular expression denial of service (ReDoS). Anyone who runs untrusted markdown through a vulnerable version of marked and does not use a worker with a time limit may be affected. This issue is patched in version 4.0.10. As a workaround, avoid running untrusted markdown through marked or run marked on a worker thread and set a reasonable time limit to prevent draining resources.	7.5	More Details
CVE-2022-23094	Libreswan 4.2 through 4.5 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted IKEv1 packet because pluto/ikev1.c wrongly expects that a state object exists. This is fixed in 4.6.	7.5	More Details
CVE-2021-42555	Pexip Infinity before 26.2 allows temporary remote Denial of Service (abort) because of missing call-setup input validation.	7.5	More Details
CVE-2021-35969	Pexip Infinity before 26 allows temporary remote Denial of Service (abort) because of missing call-setup input validation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33499	Pexip Infinity before 26 allows remote denial of service because of missing H.264 input validation (issue 2 of 2).	7.5	More Details
CVE-2021-33498	Pexip Infinity before 26 allows remote denial of service because of missing H.264 input validation (issue 1 of 2).	7.5	More Details
CVE-2021-32545	Pexip Infinity before 26 allows remote denial of service because of missing RTMP input validation.	7.5	More Details
CVE-2021-38694	SoftVibe SARABAN for INFOMA 1.1 allows SQL Injection.	7.5	More Details
CVE-2021-45761	ROPium v3.1 was discovered to contain an invalid memory address dereference via the find() function.	7.5	More Details
CVE-2022-21689	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions the receive mode limits concurrent uploads to 100 per second and blocks other uploads in the same second, which can be triggered by a simple script. An adversary with access to the receive mode can block file upload for others. There is no way to block this attack in public mode due to the anonymity properties of the tor network.	7.5	More Details
CVE-2021-30300	Possible denial of service due to incorrectly decoding hex data for the SIB2 OTA message and assigning a garbage value to choice when processing the SRS configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2022-0154	An issue has been discovered in GitLab affecting all versions starting from 7.7 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to a Cross-Site Request Forgery attack that allows a malicious user to have their GitHub project imported on another GitLab user account.	7.5	More Details
CVE-2021-45445	Unisys ClearPath MCP TCP/IP Networking Services 59.1, 60.0, and 62.0 has an Infinite Loop.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21676	Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the `engine.io` package starting from version `4.0.0`, including those who uses depending packages like `socket.io`. Versions prior to `4.0.0` are not impacted. A fix has been released for each major branch, namely `4.1.2` for the `4.x.x` branch, `5.2.1` for the `5.x.x` branch, and `6.1.1` for the `6.x.x` branch. There is no known workaround except upgrading to a safe version.	7.5	More Details
CVE-2021-30301	Possible denial of service due to out of memory while processing RRC and NAS OTA message in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-30307	Possible denial of service due to improper validation of DNS response when DNS client requests with PTR, NAPTR or SRV query type in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	7.5	More Details
CVE-2021-41807	Lack of rate limiting in M-Files Server and M-Files Web products with versions before 21.12.10873.0 in certain type of user accounts allows unlimited amount of attempts and therefore makes brute-forcing login accounts easier.	7.5	More Details
CVE-2021-29632	In FreeBSD 13.0-STABLE before n247428-9352de39c3dc, 12.2-STABLE before r370674, 13.0-RELEASE before p6, and 12.2-RELEASE before p12, certain conditions involving use of the highlight buffer while text is scrolling on the console, console data may overwrite data structures associated with the system console or other kernel memory.	7.5	More Details
CVE-2020-14107	A stack overflow in the HTTP server of Cast can be exploited to make the app crash in LAN.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21688	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. Affected versions of the desktop application were found to be vulnerable to denial of service via an undisclosed vulnerability in the QT image parsing. Roughly 20 bytes lead to 2GB memory consumption and this can be triggered multiple times. To be abused, this vulnerability requires rendering in the history tab, so some user interaction is required. An adversary with knowledge of the Onion service address in public mode or with authentication in private mode can perform a Denial of Service attack, which quickly results in out-of-memory for the server. This requires the desktop application with rendered history, therefore the impact is only elevated. This issue has been patched in version 2.5.	7.5	More Details
CVE-2022-0236	The WP Import Export WordPress plugin (both free and premium versions) is vulnerable to unauthenticated sensitive data disclosure due to a missing capability check on the download function wpie_process_file_download found in the ~/includes/classes/class-wpie-general.php file. This made it possible for unauthenticated attackers to download any imported or exported information from a vulnerable site which can contain sensitive information like user data. This affects versions up to, and including, 3.9.15.	7.5	More Details
CVE-2021-3852	growi is vulnerable to Authorization Bypass Through User-Controlled Key	7.5	More Details
CVE-2021-30330	Possible null pointer dereference due to improper validation of APE clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2021-30353	Improper validation of function pointer type with actual function signature can lead to assertion in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2022-23116	Jenkins Conjur Secrets Plugin 1.0.9 and earlier implements functionality that allows attackers able to control agent processes to decrypt secrets stored in Jenkins obtained through another method.	7.5	More Details
CVE-2022-23117	Jenkins Conjur Secrets Plugin 1.0.9 and earlier implements functionality that allows attackers able to control agent processes to retrieve all username/password credentials stored on the Jenkins controller.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30287	Possible assertion due to improper validation of symbols configured for PDCCH monitoring in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-39625	In showCarrierAppInstallationNotification of EuiccNotificationManager.java, there is a possible way to gain an access to MediaProvider content due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194695347	7.3	More Details
CVE-2022-0242	Unrestricted Upload of File with Dangerous Type in GitHub repository crater-invoice/crater prior to 6.0.	7.2	More Details
CVE-2021-33827	The files_antivirus component before 1.0.0 for ownCloud allows OS Command Injection via the administration settings.	7.2	More Details
CVE-2021-44650	Zoho ManageEngine M365 Manager Plus before Build 4419 allows remote command execution when updating proxy settings through the Admin ProxySettings and Tenant ProxySettings components.	7.2	More Details
CVE-2021-41550	Leostream Connection Broker 9.0.40.17 allows administrator to upload and execute Perl code.	7.2	More Details
CVE-2022-0198	corenlp is vulnerable to Improper Restriction of XML External Entity Reference	7.1	More Details
CVE-2021-34404	Android images for T210 provided by NVIDIA contain a vulnerability in BROM, where failure to limit access to AHB-DMA when BROM fails may allow an unprivileged attacker with physical access to cause denial of service or impact integrity and confidentiality beyond the security scope of BROM.	7.1	More Details
CVE-2022-20619	A cross-site request forgery (CSRF) vulnerability in Jenkins Bitbucket Branch Source Plugin 737.vdf9dc06105be and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4083	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.	7.0	More Details
CVE-2021-39629	In phTmlNfc_Init and phTmlNfc_CleanUp of phTmlNfc.cc, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-197353344	7.0	More Details
CVE-2021-39679	In init of vendor_graphicbuffer_meta.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-188745089References: N/A	7.0	More Details
CVE-2022-22691	The password reset component deployed within Umbraco uses the hostname supplied within the request host header when building a password reset URL. It may be possible to manipulate the URL sent to Umbraco users when so that it points to the attackers server thereby disclosing the password reset token if/when the link is followed. A related vulnerability (CVE-2022-22690) could allow this flaw to become persistent so that all password reset URLs are affected persistently following a successful attack. See the AppCheck advisory for further information and associated caveats.	6.8	More Details
CVE-2021-39683	In copy_from_mbox of sss_ice_util.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-202003354References: N/A	6.7	More Details
CVE-2022-0014	An untrusted search path vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables a local attacker with file creation privilege in the Windows root directory (such as C:\) to store a program that can then be unintentionally executed by another local user when that user utilizes a Live Terminal session. This issue impacts: Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.12; Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.9; Cortex XDR agent 7.2 versions earlier than Cortex XDR agent 7.2.4; Cortex XDR agent 7.3 versions earlier than Cortex XDR agent 7.3.2.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30313	Use after free condition can occur in wired connectivity due to a race condition while creating and deleting folders in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2021-34402	NVIDIA Tegra kernel driver contains a vulnerability in NVIDIA NVDEC, where a user with high privileges might be able to read from or write to a memory location that is outside the intended boundary of the buffer, which may lead to denial of service, Information disclosure, loss of Integrity, or possible escalation of privileges.	6.7	More Details
CVE-2022-0213	vim is vulnerable to Heap-based Buffer Overflow	6.6	More Details
CVE-2021-44839	An issue was discovered in Delta RM 1.2. It is possible to request a new password for any other account using the account ID. Using the /listes/DTsendmaildata/adm_utilisateur/send-mail.json endpoint, a user can send a JSON array with user IDs that will have their passwords reset (and new ones sent to their respective e-mail addresses).	6.5	More Details
CVE-2021-23824	This affects the package Crow before 0.3+4. When using attributes without quotes in the template, an attacker can manipulate the input to introduce additional attributes, potentially executing code. This may lead to a Cross-site Scripting (XSS) vulnerability, assuming an attacker can influence the value entered into the template. If the template is used to render user-generated content, this vulnerability may escalate to a persistent XSS vulnerability.	6.5	More Details
CVE-2022-21685	Frontier is Substrate's Ethereum compatibility layer. Prior to commit number `8a93fdc6c9f4eb1d2f2a11b7ff1d12d70bf5a664`, a bug in Frontier's MODEXP precompile implementation can cause an integer underflow in certain conditions. This will cause a node crash for debug builds. For release builds (and production WebAssembly binaries), the impact is limited as it can only cause a normal EVM out-of-gas. Users who do not use MODEXP precompile in their runtime are not impacted. A patch is available in pull request #549.	6.5	More Details
CVE-2022-0151	An issue has been discovered in GitLab affecting all versions starting from 12.10 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not correctly handling requests to delete existing packages which could result in a Denial of Service under specific conditions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46225	A buffer overflow in the GmfOpenMesh() function of libMeshb v7.61 allows attackers to cause a Denial of Service (DoS) via a crafted MESH file.	6.5	More Details
CVE-2021-25037	The All in One SEO WordPress plugin before 4.1.5.3 is affected by an authenticated SQL injection issue, which was discovered during an internal audit by the Jetpack Scan team, and could grant attackers access to privileged information from the affected site's database (e.g., usernames and hashed passwords).	6.5	More Details
CVE-2022-0152	An issue has been discovered in GitLab affecting all versions starting from 13.10 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to unauthorized access to some particular fields through the GraphQL API.	6.5	More Details
CVE-2021-39056	The IBM i 7.1, 7.2, 7.3, and 7.4 Extended Dynamic Remote SQL server (EDRSQL) could allow a remote authenticated user to send a specially crafted request and cause a denial of service. IBM X-Force ID: 214537.	6.5	More Details
CVE-2021-23514	This affects the package Crow before 0.3+4. It is possible to traverse directories to fetch arbitrary files from the server.	6.5	More Details
CVE-2022-22054	ASUS RT-AX56U's login function contains a path traversal vulnerability due to its inadequate filtering for special characters in URL parameters, which allows an unauthenticated local area network attacker to access restricted system paths and download arbitrary files.	6.5	More Details
CVE-2022-23109	Jenkins HashiCorp Vault Plugin 3.7.0 and earlier does not mask Vault credentials in Pipeline build logs or in Pipeline step descriptions when Pipeline: Groovy Plugin 2.85 or later is installed.	6.5	More Details
CVE-2022-23105	Jenkins Active Directory Plugin 2.25 and earlier does not encrypt the transmission of data between the Jenkins controller and Active Directory servers in most configurations.	6.5	More Details
CVE-2022-22290	Incorrect download source UI in Downloads in Samsung Internet prior to 16.0.6.23 allows attackers to perform domain spoofing via a crafted HTML page.	6.5	More Details
CVE-2021-43762	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a dispatcher bypass vulnerability that could be abused to evade security controls. Sensitive areas of the web application may be exposed through exploitation of the vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23112	A missing permission check in Jenkins Publish Over SSH Plugin 1.22 and earlier allows attackers with Overall/Read access to connect to an attacker-specified SSH server using attacker-specified credentials.	6.5	More Details
CVE-2022-0090	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab is configured in a way that it doesn't ignore replacement references with git sub-commands, allowing a malicious user to spoof the contents of their commits in the UI.	6.5	More Details
CVE-2022-0231	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	6.5	More Details
CVE-2022-0233	The ProfileGrid – User Profiles, Memberships, Groups and Communities WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the pm_user_avatar and pm_cover_image parameters found in the ~/admin/class-profile-magic-admin.php file which allows attackers with authenticated user access, such as subscribers, to inject arbitrary web scripts into their profile, in versions up to and including 1.2.7.	6.4	More Details
CVE-2021-4074	The WHMCS Bridge WordPress plugin is vulnerable to Stored Cross-Site Scripting via the cc_whmcs_bridge_url parameter found in the ~/whmcs-bridge/bridge_cp.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.1. Due to missing authorization checks on the cc_whmcs_bridge_add_admin function, low-level authenticated users such as subscribers can exploit this vulnerability.	6.4	More Details
CVE-2021-35500	The Data Virtualization Server component of TIBCO Software Inc.'s TIBCO Data Virtualization, TIBCO Data Virtualization, TIBCO Data Virtualization, and TIBCO Data Virtualization for AWS Marketplace contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to download arbitrary files outside of the scope of the user's permissions on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Data Virtualization: versions 8.3.0 and below, TIBCO Data Virtualization: version 8.4.0, TIBCO Data Virtualization: version 8.5.0, and TIBCO Data Virtualization for AWS Marketplace: versions 8.5.0 and below.	6.3	More Details
CVE-2022-0178	Missing Authorization vulnerability in snipe snipe/snipe-it.This issue affects snipe/snipe-i before 5.3.8.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23133	An authenticated user can create a hosts group from the configuration with XSS payload, which will be available for other users. When XSS is stored by an authenticated malicious actor and other users try to search for groups during new host creation, the XSS payload will fire and the actor can steal session cookies and perform session hijacking to impersonate users or take over their accounts.	6.3	More Details
CVE-2022-21693	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions an adversary with a primitive that allows for filesystem access from the context of the Onionshare process can access sensitive files in the entire user home folder. This could lead to the leaking of sensitive data. Due to the automatic exclusion of hidden folders, the impact is reduced. This can be mitigated by usage of the flatpak release.	6.3	More Details
CVE-2021-30314	Lack of validation for third party application accessing the service can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.2	More Details
CVE-2022-0235	node-fetch is vulnerable to Exposure of Sensitive Information to an Unauthorized Actor	6.1	More Details
CVE-2022-23083	NetMaster 12.2 Network Management for TCP/IP and NetMaster File Transfer Management contain a XSS (Cross-Site Scripting) vulnerability in ReportCenter UI due to insufficient input validation that could potentially allow an attacker to execute code on the affected machine.	6.1	More Details
CVE-2022-22529	SAP Enterprise Threat Detection (ETD) - version 2.0, does not sufficiently encode user-controlled inputs which may lead to an unauthorized attacker possibly exploit XSS vulnerability. The UIs in ETD are using SAP UI5 standard controls, the UI5 framework provides automated output encoding for its standard controls. This output encoding prevents stored malicious user input from being executed when it is reflected in the UI.	6.1	More Details
CVE-2021-3853	chaskiq is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2022-0181	Reflected cross-site scripting vulnerability in Quiz And Survey Master versions prior to 7.3.7 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0087	keystone is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2022-20645	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20636	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20638	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20635	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-0262	Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.2.7.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38678	An open redirect vulnerability has been reported to affect QNAP device running QcalAgent. If exploited, this vulnerability allows attackers to redirect users to an untrusted page that contains malware. We have already fixed this vulnerability in the following versions of QcalAgent: QcalAgent 1.1.7 and later	6.1	More Details
CVE-2022-20639	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20640	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20641	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20642	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20643	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20644	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2021-24838	The AnyComment WordPress plugin before 0.3.5 has an API endpoint which passes user input via the redirect parameter to the wp_redirect() function without being validated first, leading to an Open Redirect issue, which according to the vendor, is a feature.	6.1	More Details
CVE-2022-20646	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20647	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42551	Cross-site Scripting (XSS) vulnerability in the search functionality of AlCoda NetBiblio WebOPAC allows an unauthenticated user to craft a reflected Cross-Site Scripting attack. This issue affects: AlCoda NetBiblio WebOPAC versions prior to 4.0.0.320; versions later than 4.0.0.328. This issue does not affect: AlCoda NetBiblio WebOPAC version 4.0.0.335 and later versions.	6.1	More Details
CVE-2021-45422	Reprise License Manager 14.2 is affected by a reflected cross-site scripting vulnerability in the /goform/activate_process "count" parameter via GET. No authentication is required.	6.1	More Details
CVE-2022-20637	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2021-44217	In Ericsson CodeChecker through 6.18.0, a Stored Cross-site scripting (XSS) vulnerability in the comments component of the reports viewer allows remote attackers to inject arbitrary web script or HTML via the POST JSON data of the /CodeCheckerService API.	6.1	More Details
CVE-2021-38126	Potential vulnerabilities have been identified in Micro Focus ArcSight Enterprise Security Manager, affecting versions 7.4.x and 7.5.x. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS).	6.1	More Details
CVE-2021-38127	Potential vulnerabilities have been identified in Micro Focus ArcSight Enterprise Security Manager, affecting versions 7.4.x and 7.5.x. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS).	6.1	More Details
CVE-2022-0012	An improper link resolution before file access vulnerability exists in the Palo Alto Networks Cortex XDR agent on Windows platforms that enables a local user to delete arbitrary system files and impact the system integrity or cause a denial of service condition. This issue impacts: Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.12; Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.9; Cortex XDR agent 7.2 versions earlier than Cortex XDR agent 7.2.4; Cortex XDR agent 7.3 versions earlier than Cortex XDR agent 7.3.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42357	When using Apache Knox SSO prior to 1.6.1, a request could be crafted to redirect a user to a malicious page due to improper URL parsing. A request that included a specially crafted request parameter could be used to redirect the user to a page controlled by an attacker. This URL would need to be presented to the user outside the normal request flow through a XSS or phishing campaign.	6.1	More Details
CVE-2021-33040	managers/views/iframe.js in FuturePress EPub.js before 0.3.89 allows XSS.	6.1	More Details
CVE-2021-42558	An issue was discovered in CALDERA 2.8.1. It contains multiple reflected, stored, and self XSS vulnerabilities that may be exploited by authenticated and unauthenticated attackers.	6.1	More Details
CVE-2021-25024	The EventCalendar WordPress plugin before 1.1.51 does not escape some user input before outputting it back in attributes, leading to Reflected Cross-SIte Scripting issues	6.1	More Details
CVE-2021-24909	The ACF Photo Gallery Field WordPress plugin before 1.7.5 does not sanitise and escape the post parameter in the includes/acf_photo_gallery_metabox_edit.php file before outputing back in an attribute, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-40327	Trusted Firmware-M (TF-M) 1.4.0, when Profile Small is used, has incorrect access control. NSPE can access a secure key (held by the Crypto service) based solely on knowledge of its key ID. For example, there is no authorization check associated with the relationship between a caller and a key owner.	5.9	More Details
CVE-2021-36781	A Incorrect Default Permissions vulnerability in the parsec package of openSUSE Factory allows local attackers to imitate the service leading to DoS or clients talking to an imposter service. This issue affects: openSUSE Factory parsec versions prior to 0.8.1-1.1.	5.9	More Details
CVE-2021-37529	A double-free vulnerability exists in fig2dev through 3.28a is affected by: via the free_stream function in readpics.c, which could cause a denial of service (context-dependent).	5.5	More Details
CVE-2021-45763	GPAC v1.1.0 was discovered to contain an invalid call in the function gf_node_changed(). This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44713	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in application denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-44712	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Access of Memory Location After End of Buffer vulnerability that could lead to application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-45762	GPAC v1.1.0 was discovered to contain an invalid memory address dereference via the function gf_sg_vrml_mf_reset(). This vulnerability allows attackers to cause a Denial of Service (DoS).	5.5	More Details
CVE-2021-39633	In gre_handle_offloads of ip_gre.c, there is a possible page fault due to an invalid memory access. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150694665References: Upstream kernel	5.5	More Details
CVE-2022-20621	Jenkins Metrics Plugin 4.0.2.8 and earlier stores an access key unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	5.5	More Details
CVE-2021-44700	Adobe Illustrator versions 25.4.2 (and earlier) and 26.0.1 (and earlier) are 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.	5.5	More Details
CVE-2021-44234	SAP Business One - version 10.0, extended log stores information that can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.	5.5	More Details
CVE-2021-28507	An issue has recently been discovered in Arista EOS where, under certain conditions, the service ACL configured for OpenConfig gNOI and OpenConfig RESTCONF might be bypassed, which results in the denied requests being forwarded to the agent.	5.5	More Details
CVE-2021-40559	A null pointer deference vulnerability exists in gpac through 1.0.1 via the naludmx_parse_nal_avc function in reframe_nalu, which allows a denail of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45449	Docker Desktop version 4.3.0 and 4.3.1 has a bug that may log sensitive information (access token or password) on the user's machine during login. This only affects users if they are on Docker Desktop 4.3.0, 4.3.1 and the user has logged in while on 4.3.0, 4.3.1. Gaining access to this data would require having access to the user's local files.	5.5	More Details
CVE-2021-39659	In sortSimPhoneAccountsForEmergency of CreateConnectionProcessor.java, there is a possible prevention of access to emergency calling due to an unhandled exception. In rare instances, this could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-208267659	5.5	More Details
CVE-2021-34405	NVIDIA Linux distributions contain a vulnerability in TrustZone's TEE_Malloc function, where an unchecked return value causing a null pointer dereference may lead to denial of service.	5.5	More Details
CVE-2021-39032	IBM Sterling Gentran:Server for Microsoft Windows 5.3 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 213962.	5.5	More Details
CVE-2021-37530	A denial of service vulnerabiity exists in fig2dev through 3.28a due to a segfault in the open_stream function in readpics.c.	5.5	More Details
CVE-2021-34985	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley ContextCapture 10.18.0.232. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OBJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14785.	5.5	More Details
CVE-2021-40562	A Segmentation fault caused by a floating point exception exists in Gpac through 1.0.1 using mp4box via the naludmx_enqueue_or_dispatch function in reframe_nalu.c, which causes a denial of service.	5.5	More Details
CVE-2021-46022	An Use-After-Free vulnerability in rec_mset_elem_destroy() at rec-mset.c of GNU Recutils v1.8.90 can lead to a segmentation fault or application crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45760	GPAC v1.1.0 was discovered to contain an invalid memory address dereference via the function gf_list_last(). This vulnerability allows attackers to cause a Denial of Service (DoS).	5.5	More Details
CVE-2021-40576	The binary MP4Box in Gpac 1.0.1 has a null pointer dereference vulnerability in the gf_isom_get_payt_count function in hint_track.c, which allows attackers to cause a denial of service.	5.5	More Details
CVE-2021-40575	The binary MP4Box in Gpac 1.0.1 has a null pointer dereference vulnerability in the mpgviddmx_process function in reframe_mpgvid.c, which allows attackers to cause a denial of service. This vulnerability is possibly due to an incomplete fix for CVE-2021-40566.	5.5	More Details
CVE-2021-40573	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the gf_list_del function in list.c, which allows attackers to cause a denial of service.	5.5	More Details
CVE-2021-40572	The binary MP4Box in Gpac 1.0.1 has a double-free bug in the av1dmx_finalize function in reframe_av1.c, which allows attackers to cause a denial of service.	5.5	More Details
CVE-2022-22703	In Stormshield SSO Agent 2.x before 2.1.1 and 3.x before 3.0.2, the cleartext user password and PSK are contained in the log file of the .exe installer.	5.5	More Details
CVE-2021-40569	The binary MP4Box in Gpac through 1.0.1 has a double-free vulnerability in the iloc_entry_del funciton in box_code_meta.c, which allows attackers to cause a denial of service.	5.5	More Details
CVE-2021-40567	Segmentation fault vulnerability exists in Gpac through 1.0.1 via the gf_odf_size_descriptor function in desc_private.c when using mp4box, which causes a denial of service.	5.5	More Details
CVE-2021-45063	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions 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.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34984	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley ContextCapture 10.18.0.232. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OBJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14784.	5.5	More Details
CVE-2021-46169	Modex v2.11 was discovered to contain an Use-After-Free vulnerability via the component tcache.	5.5	More Details
CVE-2021-46168	Spin v6.5.1 was discovered to contain an out-of-bounds write in lex() at spinlex.c.	5.5	More Details
CVE-2021-46195	GCC v12.0 was discovered to contain an uncontrolled recursion via the component libiberty/rust-demangle.c. This vulnerability allows attackers to cause a Denial of Service (DoS) by consuming excessive CPU and memory resources.	5.5	More Details
CVE-2021-46171	Modex v2.11 was discovered to contain a NULL pointer dereference in set_create_id() at xtract.c.	5.5	More Details
CVE-2021-46021	An Use-After-Free vulnerability in rec_record_destroy() at rec-record.c of GNU Recutils v1.8.90 can lead to a segmentation fault or application crash.	5.5	More Details
CVE-2021-46019	An untrusted pointer dereference in rec_db_destroy() at rec-db.c of GNU Recutils v1.8.90 can lead to a segmentation fault or application crash.	5.5	More Details
CVE-2021-40563	A Segmentation fault exists casued by null pointer dereference exists in Gpac through 1.0.1 via the naludmx_create_avc_decoder_config function in reframe_nalu.c when using mp4box, which causes a denial of service.	5.5	More Details
CVE-2021-45764	GPAC v1.1.0 was discovered to contain an invalid memory address dereference via the function shift_chunk_offsets.isra().	5.5	More Details
CVE-2021-45767	GPAC 1.1.0 was discovered to contain an invalid memory address dereference via the function lsr_read_id(). This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40565	A Segmentation fault caused by a null pointer dereference vulnerability exists in Gpac through 1.0.1 via the gf_avc_parse_nalu function in av_parsers.c when using mp4box, which causes a denial of service.	5.5	More Details
CVE-2021-40564	A Segmentation fault caused by null pointer dereference vulnerability eists in Gpac through 1.0.2 via the avc_parse_slice function in av_parsers.c when using mp4box, which causes a denial of service.	5.5	More Details
CVE-2021-45067	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Access of Memory Location After End of Buffer 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.	5.5	More Details
CVE-2021-40566	A Segmentation fault casued by heap use after free vulnerability exists in Gpac through 1.0.1 via the mpgviddmx_process function in reframe_mpgvid.c when using mp4box, which causes a denial of service.	5.5	More Details
CVE-2021-23227	Cross-Site Request Forgery (CSRF) vulnerability in Alexander Fuchs PHP Everywhere plugin <= 2.0.2 versions.	5.4	More Details
CVE-2022-23115	Cross-site request forgery (CSRF) vulnerabilities in Jenkins batch task Plugin 1.19 and earlier allows attackers with Overall/Read access to retrieve logs, build or delete a batch task.	5.4	More Details
CVE-2021-44178	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a reflected Cross-Site Scripting (XSS) vulnerability via the itemResourceType parameter. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser	5.4	More Details
CVE-2022-0159	orchardcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-38695	SoftVibe SARABAN for INFOMA 1.1 is vulnerable to stored cross-site scripting (XSS) that allows users to store scripts in certain fields (e.g. subject, description) of the document form.	5.4	More Details
CVE-2021-43436	MartDevelopers Inc iResturant v1.0 allows Stored XSS by placing a payload in the username field during a login attempt. When an administrator looks at the log of failed logins, the XSS payload will be executed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29872	IBM Cloud Pak for Automation 21.0.1 and 21.0.2 - Business Automation Studio Component is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. By sending a specially crafted HTTP request, a remote attacker could exploit this vulnerability to inject HTTP HOST header, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 206228.	5.4	More Details
CVE-2021-44649	Django CMS 3.7.3 does not validate the plugin_type parameter while generating error messages for an invalid plugin type, resulting in a Cross Site Scripting (XSS) vulnerability. The vulnerability allows an attacker to execute arbitrary JavaScript code in the web browser of the affected user.	5.4	More Details
CVE-2022-0260	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.2.7.	5.4	More Details
CVE-2022-0179	snipe-it is vulnerable to Missing Authorization	5.4	More Details
CVE-2021-40813	A cross-site scripting (XSS) vulnerability in the "Zip content" feature in Element-IT HTTP Commander 3.1.9 allows remote authenticated users to inject arbitrary web script or HTML via filenames.	5.4	More Details
CVE-2022-0257	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2022-22112	In DayByDay CRM, versions 1.1 through 2.2.1 (latest) suffer from an application-wide Client-Side Template Injection (CSTI). A low privileged attacker can input template injection payloads in the application at various locations to execute JavaScript on the client browser.	5.4	More Details
CVE-2022-0182	Stored cross-site scripting vulnerability in Quiz And Survey Master versions prior to 7.3.7 allows a remote authenticated attacker to inject an arbitrary script via an website that uses Quiz And Survey Master.	5.4	More Details
CVE-2022-23108	Jenkins Badge Plugin 1.9 and earlier does not escape the description and does not check for allowed protocols when creating a badge, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2020-28919	A stored cross site scripting (XSS) vulnerability in Checkmk 1.6.0x prior to 1.6.0p19 allows an authenticated remote attacker to inject arbitrary JavaScript via a javascript: URL in a view title.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20615	Jenkins Matrix Project Plugin 1.19 and earlier does not escape HTML metacharacters in node and label names, and label descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Agent/Configure permission.	5.4	More Details
CVE-2022-22123	In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the article title. An authenticated attacker can inject arbitrary javascript code that will execute on a victim’s server.	5.4	More Details
CVE-2021-4170	calibre-web is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2022-0256	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2022-22124	In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the profile image. An authenticated attacker can upload a carefully crafted SVG file that will trigger arbitrary javascript to run on a victim’s browser.	5.4	More Details
CVE-2021-3857	chaskiq is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-25061	The WP Booking System WordPress plugin before 2.0.15 was affected by a reflected xss in wp-booking-system on the wpbs-calendars admin page.	5.4	More Details
CVE-2021-25065	The Smash Balloon Social Post Feed WordPress plugin before 4.1.1 was affected by a reflected XSS in custom-facebook-feed in cff-top admin page.	5.4	More Details
CVE-2021-25067	The Landing Page Builder WordPress plugin before 1.4.9.6 was affected by a reflected XSS in page-builder-add on the ulpb_post admin page.	5.4	More Details
CVE-2022-0253	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-46005	Sourcecodester Car Rental Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via vehicalorcview parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25046	The Modern Events Calendar Lite WordPress plugin before 6.2.0 alloed any logged-in user, even a subscriber user, may add a category whose parameters are incorrectly escaped in the admin panel, leading to stored XSS.	5.4	More Details
CVE-2021-36199	Running a vulnerability scanner against VideoEdge NVRs can cause some functionality to stop.	5.3	More Details
CVE-2021-1037	The broadcast that DevicePickerFragment sends when a new device is paired doesn't have any permission checks, so any app can register to listen for it. This lets apps keep track of what devices are paired without requesting BLUETOOTH permissions.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-162951906	5.3	More Details
CVE-2022-0172	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.3. Under certain conditions it was possible to bypass the IP restriction for public projects through GraphQL allowing unauthorised users to read titles of issues, merge requests and milestones.	5.3	More Details
CVE-2021-24046	A logic flaw in Ray-Ban® Stories device software allowed some parameters like video capture duration limit to be modified through the Facebook View application. This issue affected versions of device software before 2107460.6810.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21700	Micronaut is a JVM-based, full stack Java framework designed for building JVM web applications with support for Java, Kotlin and the Groovy language. In affected versions sending an invalid Content Type header leads to memory leak in DefaultArgumentConversionContext as this type is erroneously used in static state. ### Impact Sending an invalid Content Type header leads to memory leak in `DefaultArgumentConversionContext` as this type is erroneously used in static state. ### Patches The problem is patched in Micronaut 3.2.7 and above. ### Workarounds The default content type binder can be replaced in an existing Micronaut application to mitigate the issue: ```java package example; import java.util.List; import io.micronaut.context.annotation.Replaces; import io.micronaut.core.convert.ConversionService; import io.micronaut.http.MediaType; import io.micronaut.http.bind.DefaultRequestBinderRegistry; import io.micronaut.http.bind.binders.RequestArgumentBinder; import jakarta.inject.Singleton; @Singleton @Replaces(DefaultRequestBinderRegistry.class) class FixedRequestBinderRegistry extends DefaultRequestBinderRegistry { public FixedRequestBinderRegistry(ConversionService conversionService, List<RequestArgumentBinder> binders) { super(conversionService, binders); } @Override protected void registerDefaultConverters(ConversionService<?> conversionService) { super.registerDefaultConverters(conversionService); conversionService.addConverter(CharSequence.class, MediaType.class, charSequence -> { try { return MediaType.of(charSequence); } catch (IllegalArgumentException e) { return null; } }); } } ``` ### References Commit that introduced the vulnerability https://github.com/micronaut-projects/micronaut-core/commit/b8ec32c311689667c69ae7d9f9c3b3a8abc96fe3 ### For more information If you have any questions or comments about this advisory: * Open an issue in [Micronaut Core] (https://github.com/micronaut-projects/micronaut-core/issues) * Email us at info@micronaut.io	5.3	More Details
CVE-2021-38677	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running QcalAgent. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of QcalAgent: QcalAgent 1.1.7 and later	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23106	Jenkins Configuration as Code Plugin 1.55 and earlier used a non-constant time comparison function when validating an authentication token allowing attackers to use statistical methods to obtain a valid authentication token.	5.3	More Details
CVE-2021-28377	ChronoForums 2.0.11 allows av Directory Traversal to read arbitrary files.	5.3	More Details
CVE-2022-0013	A file information exposure vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables a local attacker to read the contents of arbitrary files on the system with elevated privileges when generating a support file. This issue impacts: Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.12; Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.9; Cortex XDR agent 7.2 versions earlier than Cortex XDR agent 7.2.4; Cortex XDR agent 7.3 versions earlier than Cortex XDR agent 7.3.2.	5.0	More Details
CVE-2021-41551	Leostream Connection Broker 9.0.40.17 allows administrators to conduct directory traversal attacks by uploading z ZIP file that contains a symbolic link.	4.9	More Details
CVE-2021-36920	Authenticated Reflected Cross-Site Scripting (XSS) vulnerability discovered in WordPress plugin Download Monitor (versions <= 4.4.6).	4.8	More Details
CVE-2022-23110	Jenkins Publish Over SSH Plugin 1.22 and earlier does not escape the SSH server name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Administer permission.	4.8	More Details
CVE-2022-0232	The User Registration, Login & Landing Pages WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the loader_text parameter found in the ~/includes/templates/landing-page.php file which allows attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.2.7. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	4.8	More Details
CVE-2021-25005	The SEUR Oficial WordPress plugin before 1.7.0 does not sanitize and escape some of its settings allowing 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-2022-0210	The Random Banner WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the category parameter found in the ~/include/models/model.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	4.8	More Details
CVE-2021-3862	icecoder is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	4.8	More Details
CVE-2022-22125	In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the article tag. An authenticated admin attacker can inject arbitrary javascript code that will execute on a victim’s server.	4.8	More Details
CVE-2021-43960	Lorensbergs Connect2 3.13.7647.20190 is affected by an XSS vulnerability. Exploitation requires administrator privileges and is performed through the Wizard editor of the application. The attack requires an administrator to go into the Wizard editor and enter an XSS payload within the Page title, Page Instructions, Text before, Text after, or Text on side box. Once this has been done, the administrator must click save and finally wait until any user of the application performs a booking for rental items in the booking area of the application, where the XSS triggers. NOTE: another perspective is that the administrator may require JavaScript to customize any aspect of the page rendering. There is no effective way for the product to defend users in the face of a malicious administrator	4.8	More Details
CVE-2021-34406	NVIDIA Tegra kernel driver contains a vulnerability in NVHost, where a specific race condition can lead to a null pointer dereference, which may lead to a system reboot.	4.7	More Details
CVE-2021-37866	Mattermost Boards plugin v0.10.0 and earlier fails to invalidate a session on the server-side when a user logged out of Boards, which allows an attacker to reuse old session token for authorization.	4.7	More Details
CVE-2022-20660	A vulnerability in the information storage architecture of several Cisco IP Phone models could allow an unauthenticated, physical attacker to obtain confidential information from an affected device. This vulnerability is due to unencrypted storage of confidential information on an affected device. An attacker could exploit this vulnerability by physically extracting and accessing one of the flash memory chips. A successful exploit could allow the attacker to obtain confidential information from the device, which could be used for subsequent attacks.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0183	Missing encryption of sensitive data vulnerability in 'MIRUPASS' PW10 firmware all versions and 'MIRUPASS' PW20 firmware all versions allows an attacker who can physically access the device to obtain the stored passwords.	4.6	More Details
CVE-2021-39680	In sec_SHA256_Transform of sha256_core.c, there is a possible way to read heap data due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-197965864References: N/A	4.4	More Details
CVE-2022-21677	Discourse is an open source discussion platform. Discourse groups can be configured with varying visibility levels for the group as well as the group members. By default, a newly created group has its visibility set to public and the group's members visibility set to public as well. However, a group's visibility and the group's members visibility can be configured such that it is restricted to logged on users, members of the group or staff users. A vulnerability has been discovered in versions prior to 2.7.13 and 2.8.0.beta11 where the group advanced search option does not respect the group's visibility and members visibility level. As such, a group with restricted visibility or members visibility can be revealed through search with the right search option. This issue is patched in `stable` version 2.7.13, `beta` version 2.8.0.beta11, and `tests-passed` version 2.8.0.beta11 versions of Discourse. There are no workarounds aside from upgrading.	4.3	More Details
CVE-2022-21684	Discourse is an open source discussion platform. Versions prior to 2.7.13 in `stable`, 2.8.0.beta11 in `beta`, and 2.8.0.beta11 in `tests-passed` allow some users to log in to a community before they should be able to do so. A user invited via email to a forum with `must_approve_users` enabled is going to be automatically logged in, bypassing the check that does not allow unapproved users to sign in. They will be able to do everything an approved user can do. If they logout, they cannot log back in. This issue is patched in the `stable` version 2.7.13, `beta` version 2.8.0.beta11, and `tests-passed` version 2.8.0.beta11. One may disable invites as a workaround. Administrators can increase `min_trust_level_to_allow_invite` to reduce the attack surface to more trusted users.	4.3	More Details
CVE-2022-0238	phoronix-test-suite is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0124	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. Gitlab's Slack integration is incorrectly validating user input and allows to craft malicious URLs that are sent to slack.	4.3	More Details
CVE-2022-0125	An issue has been discovered in GitLab affecting all versions starting from 12.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not verifying that a maintainer of a project had the right access to import members from a target project.	4.3	More Details
CVE-2022-21678	Discourse is an open source discussion platform. Prior to version 2.8.0.beta11 in the `tests-passed` branch, version 2.8.0.beta11 in the `beta` branch, and version 2.7.13 in the `stable` branch, the bios of users who made their profiles private were still visible in the `<meta>` tags on their users' pages. The problem is patched in `tests-passed` version 2.8.0.beta11, `beta` version 2.8.0.beta11, and `stable` version 2.7.13 of Discourse.	4.3	More Details
CVE-2021-4146	Business Logic Errors in GitHub repository pimcore/pimcore prior to 10.2.6.	4.3	More Details
CVE-2021-44702	Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must visit an attacker controlled web page.	4.3	More Details
CVE-2021-39942	A denial of service vulnerability in GitLab CE/EE affecting all versions starting from 12.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows low-privileged users to bypass file size limits in the NPM package repository to potentially cause denial of service.	4.3	More Details
CVE-2021-39892	In all versions of GitLab CE/EE since version 12.0, a lower privileged user can import users from projects that they don't have a maintainer role on and disclose email addresses of those users.	4.3	More Details
CVE-2021-42067	In SAP NetWeaver AS for ABAP and ABAP Platform - versions 701, 702, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 786, an attacker authenticated as a regular user can use the S/4 Hana dashboard to reveal systems and services which they would not normally be allowed to see. No information alteration or denial of service is possible.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37865	Mattermost 6.2 and earlier fails to sufficiently process a specifically crafted GIF file when it is uploaded while drafting a post, which allows authenticated users to cause resource exhaustion while processing the file, resulting in server-side Denial of Service.	4.3	More Details
CVE-2021-44739	Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page.	4.3	More Details
CVE-2022-23111	A cross-site request forgery (CSRF) vulnerability in Jenkins Publish Over SSH Plugin 1.22 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials.	4.3	More Details
CVE-2022-23113	Jenkins Publish Over SSH Plugin 1.22 and earlier performs a validation of the file name specifying whether it is present or not, resulting in a path traversal vulnerability allowing attackers with Item/Configure permission to discover the name of the Jenkins controller files.	4.3	More Details
CVE-2021-44836	An issue was discovered in Delta RM 1.2. The /risque/risque/workflow/reset endpoint is lacking access controls, and it is possible for an unprivileged user to reopen a risk with a POST request, using the risqueID parameter to identify the risk to be re-opened.	4.3	More Details
CVE-2022-21692	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions anyone with access to the chat environment can write messages disguised as another chat participant.	4.3	More Details
CVE-2021-25025	The EventCalendar WordPress plugin before 1.1.51 does not have proper authorisation and CSRF checks in the add_calendar_event AJAX actions, allowing users with a role as low as subscriber to create events	4.3	More Details
CVE-2022-21695	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions authenticated users (or unauthenticated in public mode) can send messages without being visible in the list of chat participants. This issue has been resolved in version 2.5.	4.3	More Details
CVE-2022-21691	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions chat participants can spoof their channel leave message, tricking others into assuming they left the chatroom.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0245	Cross-Site Request Forgery (CSRF) in GitHub repository livehelperchat/livehelperchat prior to 2.0.	4.3	More Details
CVE-2022-21673	Grafana is an open-source platform for monitoring and observability. In affected versions when a data source has the Forward OAuth Identity feature enabled, sending a query to that datasource with an API token (and no other user credentials) will forward the OAuth Identity of the most recently logged-in user. This can allow API token holders to retrieve data for which they may not have intended access. This attack relies on the Grafana instance having data sources that support the Forward OAuth Identity feature, the Grafana instance having a data source with the Forward OAuth Identity feature toggled on, the Grafana instance having OAuth enabled, and the Grafana instance having usable API keys. This issue has been patched in versions 7.5.13 and 8.3.4.	4.3	More Details
CVE-2022-21696	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions it is possible to change the username to that of another chat participant with an additional space character at the end of the name string. An adversary with access to the chat environment can use the rename feature to impersonate other participants by adding whitespace characters at the end of the username.	4.3	More Details
CVE-2021-44838	An issue was discovered in Delta RM 1.2. Using the /risque/risque/ajax-details endpoint, with a POST request indicating the risk to access with the id parameter, it is possible for users to access risks of other companies.	4.3	More Details
CVE-2022-0184	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode.	4.3	More Details
CVE-2022-20614	A missing permission check in Jenkins Mailer Plugin 391.ve4a_38c1b_cf4b_ and earlier allows attackers with Overall/Read access to use the DNS used by the Jenkins instance to resolve an attacker-specified hostname.	4.3	More Details
CVE-2022-20613	A cross-site request forgery (CSRF) vulnerability in Jenkins Mailer Plugin 391.ve4a_38c1b_cf4b_ and earlier allows attackers to use the DNS used by the Jenkins instance to resolve an attacker-specified hostname.	4.3	More Details
CVE-2022-20620	Missing permission checks in Jenkins SSH Agent Plugin 1.23 and earlier allows attackers with Overall/Read access to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20618	A missing permission check in Jenkins Bitbucket Branch Source Plugin 737.vdf9dc06105be and earlier allows attackers with Overall/Read access to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-20616	Jenkins Credentials Binding Plugin 1.27 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read access to validate if a credential ID refers to a secret file credential and whether it's a zip file.	4.3	More Details
CVE-2021-37867	Mattermost Boards plugin v0.10.0 and earlier fails to protect email addresses of all users via one of the Boards APIs, which allows authenticated and unauthorized users to access this information resulting in sensitive & private information disclosure.	4.3	More Details
CVE-2022-20612	A cross-site request forgery (CSRF) vulnerability in Jenkins 2.329 and earlier, LTS 2.319.1 and earlier allows attackers to trigger build of job without parameters when no security realm is set.	4.3	More Details
CVE-2022-0226	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-23566	The package nanoid from 3.0.0 and before 3.1.31 are vulnerable to Information Exposure via the valueOf() function which allows to reproduce the last id generated.	4.0	More Details
CVE-2022-23134	After the initial setup process, some steps of setup.php file are reachable not only by super-administrators, but by unauthenticated users as well. Malicious actor can pass step checks and potentially change the configuration of Zabbix Frontend.	3.7	More Details
CVE-2022-21694	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. The website mode of the onionshare allows to use a hardened CSP, which will block any scripts and external resources. It is not possible to configure this CSP for individual pages and therefore the security enhancement cannot be used for websites using javascript or external resources like fonts or images.	3.7	More Details
CVE-2021-41809	SSRF vulnerability in M-Files Server products with versions before 22.1.11017.1, in a preview function allowed making queries from the server with certain document types referencing external entities.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0093	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab allows a user with an expired password to access sensitive information through RSS feeds.	3.5	More Details
CVE-2021-39927	Server side request forgery protections in GitLab CE/EE versions between 8.4 and 14.4.4, between 14.5.0 and 14.5.2, and between 14.6.0 and 14.6.1 would fail to protect against attacks sending requests to localhost on port 80 or 443 if GitLab was configured to run on a port other than 80 or 443	3.5	More Details
CVE-2022-21683	Wagtail is a Django based content management system focused on flexibility and user experience. When notifications for new replies in comment threads are sent, they are sent to all users who have replied or commented anywhere on the site, rather than only in the relevant threads. This means that a user could listen in to new comment replies on pages they have not have editing access to, as long as they have left a comment or reply somewhere on the site. A patched version has been released as Wagtail 2.15.2, which restores the intended behaviour - to send notifications for new replies to the participants in the active thread only (editing permissions are not considered). New comments can be disabled by setting `WAGTAILADMIN_COMMENTS_ENABLED = False` in the Django settings file.	3.5	More Details
CVE-2021-44740	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are 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.	3.3	More Details
CVE-2021-34910	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14883.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44715	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. 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.	3.3	More Details
CVE-2021-34884	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14837.	3.3	More Details
CVE-2021-44741	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are 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.	3.3	More Details
CVE-2021-44742	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-34916	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14894.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34943	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15051.	3.3	More Details
CVE-2021-45051	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an use-after-free vulnerability in the processing of Format event actions 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.	3.3	More Details
CVE-2021-45052	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are 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 TIF file.	3.3	More Details
CVE-2021-34944	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15052.	3.3	More Details
CVE-2021-34901	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14874.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34902	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14875.	3.3	More Details
CVE-2021-34882	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14835.	3.3	More Details
CVE-2021-34890	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14843.	3.3	More Details
CVE-2021-34883	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14836.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34889	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14842.	3.3	More Details
CVE-2022-23114	Jenkins Publish Over SSH Plugin 1.22 and earlier stores password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	3.3	More Details
CVE-2022-23132	During Zabbix installation from RPM, DAC_OVERRIDE SELinux capability is in use to access PID files in [/var/run/zabbix] folder. In this case, Zabbix Proxy or Server processes can bypass file read, write and execute permissions check on the file system level	3.3	More Details
CVE-2021-45054	Adobe InCopy version 16.4 (and earlier) is affected by a use-after-free vulnerability in the processing of a JPEG2000 file 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.	3.3	More Details
CVE-2021-45059	Adobe InDesign version 16.4 (and earlier) is affected by a use-after-free vulnerability in the processing of a JPEG2000 file 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.	3.3	More Details
CVE-2021-34881	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OBJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14834.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39628	In StatusBar.java, there is a possible disclosure of notification content on the lockscreen due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-189575031	3.3	More Details
CVE-2021-34888	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14841.	3.3	More Details
CVE-2021-34887	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14840.	3.3	More Details
CVE-2021-43752	Adobe Illustrator versions 25.4.2 (and earlier) and 26.0.1 (and earlier) are 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.	3.3	More Details
CVE-2022-0131	Jimoty App for Android versions prior to 3.7.42 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	3.3	More Details
CVE-2021-34886	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of FBX files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14839.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44840	An issue was discovered in Delta RM 1.2. Using an privileged account, it is possible to edit, create, and delete risk labels, such as Criticality and Priority Indication labels. By using the /core/table/query endpoint, and by using a POST request and indicating the affected label with tableUid parameter and the operation with datas[query], it is possible to edit, create, and delete the following labels: Priority Indication, Quality Evaluation, Progress Margin and Priority. Furthermore, it is also possible to export Criticality labels with an unprivileged user.	2.7	More Details
CVE-2021-28376	ChronoForms 7.0.7 allows fname Directory Traversal to read arbitrary files.	2.7	More Details
CVE-2021-37864	Mattermost 6.1 and earlier fails to sufficiently validate permissions while viewing archived channels, which allows authenticated users to view contents of archived channels even when this is denied by system administrators by directly accessing the APIs.	2.6	More Details
CVE-2021-44714	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a Violation of Secure Design Principles that could lead to a Security feature bypass. Acrobat Reader DC displays a warning message when a user clicks on a PDF file, which could be used by an attacker to mislead the user. In affected versions, this warning message does not include custom protocols when used by the sender. User interaction is required to abuse this vulnerability as they would need to click 'allow' on the warning message of a malicious file.	2.5	More Details
CVE-2021-41808	In M-Files Server product with versions before 21.11.10775.0, enabling logging of Federated authentication to event log wrote sensitive information to log. Mitigating factors are logging is disabled by default.	2.0	More Details
CVE-2020-13023	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 2020. Notes: none	N/A	More Details
CVE-2020-12958	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 2020. Notes: none	N/A	More Details
CVE-2020-13010	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13011	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 2020. Notes: none	N/A	More Details
CVE-2020-13012	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 2020. Notes: none	N/A	More Details
CVE-2020-13013	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 2020. Notes: none	N/A	More Details
CVE-2020-13014	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 2020. Notes: none	N/A	More Details
CVE-2020-13020	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 2020. Notes: none	N/A	More Details
CVE-2020-13015	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 2020. Notes: none	N/A	More Details
CVE-2020-13016	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 2020. Notes: none	N/A	More Details
CVE-2020-13017	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 2020. Notes: none	N/A	More Details
CVE-2020-13018	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 2020. Notes: none	N/A	More Details
CVE-2020-13019	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 2020. Notes: none	N/A	More Details
CVE-2020-13022	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 2020. Notes: none	N/A	More Details
CVE-2020-13021	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12956	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 2020. Notes: none	N/A	More Details
CVE-2020-13740	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 2020. Notes: none	N/A	More Details
CVE-2020-12955	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 2020. Notes: none	N/A	More Details
CVE-2020-12953	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 2020. Notes: none	N/A	More Details
CVE-2021-38892	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-45388	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-45608. Reason: This candidate is a reservation duplicate of CVE-2021-45608. Notes: All CVE users should reference CVE-2021-45608 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-46012	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA	N/A	More Details
CVE-2022-22122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: None. Reason: This candidate is a reservation duplicate of [CVE-2021-37866]. Notes: All CVE users should reference [CVE-2021-37866] instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-12907	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 2020. Notes: none	N/A	More Details
CVE-2020-12908	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12918	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 2020. Notes: none	N/A	More Details
CVE-2020-12934	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 2020. Notes: none	N/A	More Details
CVE-2020-12937	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 2020. Notes: none	N/A	More Details
CVE-2020-12938	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 2020. Notes: none	N/A	More Details
CVE-2020-12939	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 2020. Notes: none	N/A	More Details
CVE-2020-12942	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 2020. Notes: none	N/A	More Details
CVE-2020-12943	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 2020. Notes: none	N/A	More Details
CVE-2020-12945	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 2020. Notes: none	N/A	More Details
CVE-2020-12947	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 2020. Notes: none	N/A	More Details
CVE-2020-12948	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 2020. Notes: none	N/A	More Details
CVE-2020-12949	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 2020. Notes: none	N/A	More Details
CVE-2020-12950	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12952	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 2020. Notes: none	N/A	More Details
CVE-2020-13024	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 2020. Notes: none	N/A	More Details
CVE-2020-13033	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 2020. Notes: none	N/A	More Details
CVE-2020-13025	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 2020. Notes: none	N/A	More Details
CVE-2020-13076	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 2020. Notes: none	N/A	More Details
CVE-2020-13725	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 2020. Notes: none	N/A	More Details
CVE-2020-13724	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 2020. Notes: none	N/A	More Details
CVE-2020-13723	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 2020. Notes: none	N/A	More Details
CVE-2020-13722	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 2020. Notes: none	N/A	More Details
CVE-2020-13721	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 2020. Notes: none	N/A	More Details
CVE-2020-13720	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 2020. Notes: none	N/A	More Details
CVE-2020-13719	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13718	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 2020. Notes: none	N/A	More Details
CVE-2020-13717	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 2020. Notes: none	N/A	More Details
CVE-2020-13716	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 2020. Notes: none	N/A	More Details
CVE-2020-13715	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 2020. Notes: none	N/A	More Details
CVE-2020-13714	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 2020. Notes: none	N/A	More Details
CVE-2020-13713	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 2020. Notes: none	N/A	More Details
CVE-2020-13089	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 2020. Notes: none	N/A	More Details
CVE-2020-13088	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 2020. Notes: none	N/A	More Details
CVE-2020-13087	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 2020. Notes: none	N/A	More Details
CVE-2020-13086	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 2020. Notes: none	N/A	More Details
CVE-2020-13085	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 2020. Notes: none	N/A	More Details
CVE-2020-13084	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13083	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 2020. Notes: none	N/A	More Details
CVE-2020-13082	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 2020. Notes: none	N/A	More Details
CVE-2020-13081	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 2020. Notes: none	N/A	More Details
CVE-2020-13080	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 2020. Notes: none	N/A	More Details
CVE-2020-13079	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 2020. Notes: none	N/A	More Details
CVE-2020-13078	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 2020. Notes: none	N/A	More Details
CVE-2020-13726	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 2020. Notes: none	N/A	More Details
CVE-2020-13727	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 2020. Notes: none	N/A	More Details
CVE-2020-13728	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 2020. Notes: none	N/A	More Details
CVE-2020-13739	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13742	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 2020. Notes: none	N/A	More Details
CVE-2020-13743	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 2020. Notes: none	N/A	More Details
CVE-2020-13744	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 2020. Notes: none	N/A	More Details
CVE-2020-13745	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 2020. Notes: none	N/A	More Details
CVE-2020-13746	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 2020. Notes: none	N/A	More Details
CVE-2020-13747	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 2020. Notes: none	N/A	More Details
CVE-2020-13748	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 2020. Notes: none	N/A	More Details
CVE-2020-13749	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 2020. Notes: none	N/A	More Details
CVE-2020-13750	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 2020. Notes: none	N/A	More Details
CVE-2020-13751	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 2020. Notes: none	N/A	More Details
CVE-2020-13752	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36734	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 2021. Notes: none	N/A	More Details
CVE-2020-13729	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 2020. Notes: none	N/A	More Details
CVE-2021-36735	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 2021. Notes: none	N/A	More Details
CVE-2021-36736	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 2021. Notes: none	N/A	More Details
CVE-2020-13738	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 2020. Notes: none	N/A	More Details
CVE-2020-13737	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 2020. Notes: none	N/A	More Details
CVE-2020-13736	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 2020. Notes: none	N/A	More Details
CVE-2020-13735	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 2020. Notes: none	N/A	More Details
CVE-2020-13734	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 2020. Notes: none	N/A	More Details
CVE-2020-13733	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 2020. Notes: none	N/A	More Details
CVE-2020-13732	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13731	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 2020. Notes: none	N/A	More Details
CVE-2020-13730	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 2020. Notes: none	N/A	More Details
CVE-2020-13077	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 2020. Notes: none	N/A	More Details
CVE-2020-13075	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 2020. Notes: none	N/A	More Details
CVE-2020-13026	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 2020. Notes: none	N/A	More Details
CVE-2020-13074	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 2020. Notes: none	N/A	More Details
CVE-2020-13051	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 2020. Notes: none	N/A	More Details
CVE-2020-13050	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 2020. Notes: none	N/A	More Details
CVE-2020-13049	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 2020. Notes: none	N/A	More Details
CVE-2020-13048	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 2020. Notes: none	N/A	More Details
CVE-2020-13047	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 2020. Notes: none	N/A	More Details
CVE-2020-13046	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13045	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 2020. Notes: none	N/A	More Details
CVE-2020-13044	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 2020. Notes: none	N/A	More Details
CVE-2020-13043	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 2020. Notes: none	N/A	More Details
CVE-2020-13042	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 2020. Notes: none	N/A	More Details
CVE-2020-13041	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 2020. Notes: none	N/A	More Details
CVE-2020-13040	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 2020. Notes: none	N/A	More Details
CVE-2020-13039	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 2020. Notes: none	N/A	More Details
CVE-2020-13038	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 2020. Notes: none	N/A	More Details
CVE-2020-13037	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 2020. Notes: none	N/A	More Details
CVE-2020-13036	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 2020. Notes: none	N/A	More Details
CVE-2020-13035	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 2020. Notes: none	N/A	More Details
CVE-2020-13034	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13741	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 2020. Notes: none	N/A	More Details
CVE-2020-13032	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 2020. Notes: none	N/A	More Details
CVE-2020-13031	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 2020. Notes: none	N/A	More Details
CVE-2020-13030	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 2020. Notes: none	N/A	More Details
CVE-2020-13029	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 2020. Notes: none	N/A	More Details
CVE-2020-13028	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 2020. Notes: none	N/A	More Details
CVE-2020-13027	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 2020. Notes: none	N/A	More Details
CVE-2021-45782	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-45781	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-45780	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-13062	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 2020. Notes: none	N/A	More Details
CVE-2020-13073	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13072	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 2020. Notes: none	N/A	More Details
CVE-2020-13071	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 2020. Notes: none	N/A	More Details
CVE-2020-13070	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 2020. Notes: none	N/A	More Details
CVE-2020-13069	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 2020. Notes: none	N/A	More Details
CVE-2020-13068	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 2020. Notes: none	N/A	More Details
CVE-2020-13067	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 2020. Notes: none	N/A	More Details
CVE-2020-13066	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 2020. Notes: none	N/A	More Details
CVE-2020-13065	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 2020. Notes: none	N/A	More Details
CVE-2020-13064	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 2020. Notes: none	N/A	More Details
CVE-2020-13063	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 2020. Notes: none	N/A	More Details
CVE-2020-13061	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 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45779	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-13060	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 2020. Notes: none	N/A	More Details
CVE-2020-13059	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 2020. Notes: none	N/A	More Details
CVE-2020-13058	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 2020. Notes: none	N/A	More Details
CVE-2020-13057	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 2020. Notes: none	N/A	More Details
CVE-2020-13056	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 2020. Notes: none	N/A	More Details
CVE-2020-13054	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 2020. Notes: none	N/A	More Details
CVE-2020-13053	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 2020. Notes: none	N/A	More Details
CVE-2020-13052	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 2020. Notes: none	N/A	More Details
CVE-2021-45774	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-45775	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45778	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-13055	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 2020. Notes: none	N/A	More Details