SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 December 2021

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-27447	Mesa Labs AmegaView version 3.0 is vulnerable to a command injection, which may allow an attacker to remotely execute arbitrary code.	10.0	More Details
CVE-2021-42311	Microsoft Defender for IoT Remote Code Execution Vulnerability	10.0	More Details
CVE-2021-42313	Microsoft Defender for IoT Remote Code Execution Vulnerability	10.0	More Details
CVE-2021-40850	TCMAN GIM is vulnerable to a SQL injection vulnerability inside several available webservice methods in /PC/WebService.asmx.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27449	Mesa Labs AmegaView Versions 3.0 and prior has a command injection vulnerability that can be exploited to execute commands in the web server.	9.9	More Details
CVE-2021-44676	Zoho ManageEngine Access Manager Plus before 4203 allows anyone to view a few data elements (e.g., access control details) and modify a few aspects of the application state.	9.8	More Details
CVE-2020-18078	A vulnerability in /include/web_check.php of SEMCMS v3.8 allows attackers to reset the Administrator account's password.	9.8	More Details
CVE-2021-23803	This affects the package latte/latte before 2.10.6. There is a way to bypass allowFunctions that will affect the security of the application. When the template is set to allow/disallow the use of certain functions, adding control characters (x00-x08) after the function will bypass these restrictions.	9.8	More Details
CVE-2021-44159	4MOSAn GCB Doctor’s file upload function has improper user privilege control. A remote attacker can upload arbitrary files including webshell files without authentication and execute arbitrary code in order to perform arbitrary system operations or deny of service attack.	9.8	More Details
CVE-2021-44164	Chain Sea ai chatbot system’s file upload function has insufficient filtering for special characters in URLs, which allows a remote attacker to by-pass file type validation, upload malicious script and execute arbitrary code without authentication, in order to take control of the system or terminate service.	9.8	More Details
CVE-2021-44732	Mbed TLS before 3.0.1 has a double free in certain out-of-memory conditions, as demonstrated by an mbedtls_ssl_set_session() failure.	9.8	More Details
CVE-2021-44790	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.	9.8	More Details
CVE-2021-44675	Zoho ManageEngine ServiceDesk Plus MSP before 10.5 Build 10534 is vulnerable to unauthenticated remote code execution due to a filter bypass in which authentication is not required.	9.8	More Details
CVE-2021-43439	RCE in Add Review Function in iResturant 1.0 Allows remote attacker to execute commands remotely	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44525	Zoho ManageEngine PAM360 before build 5303 allows attackers to modify a few aspects of application state because of a filter bypass in which authentication is not required.	9.8	More Details
CVE-2021-41560	OpenCATS through 0.9.6 allows remote attackers to execute arbitrary code by uploading an executable file via lib/FileUtility.php.	9.8	More Details
CVE-2021-24849	The wcfm_ajax_controller AJAX action of the WCFM Marketplace WordPress plugin before 3.4.12, available to unauthenticated and authenticated user, does not properly sanitise multiple parameters before using them in SQL statements, leading to SQL injections	9.8	More Details
CVE-2021-45252	Multiple SQL injection vulnerabilities are found on Simple Forum-Discussion System 1.0 For example on three applications which are manage_topic.php, manage_user.php, and ajax.php. The attacker can be retrieving all information from the database of this system by using this vulnerability.	9.8	More Details
CVE-2021-45253	The id parameter in view_storage.php from Simple Cold Storage Management System 1.0 appears to be vulnerable to SQL injection attacks. A payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.	9.8	More Details
CVE-2021-45255	The email parameter from ajax.php of Video Sharing Website 1.0 appears to be vulnerable to SQL injection attacks. A payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.	9.8	More Details
CVE-2021-45090	Stormshield Endpoint Security before 2.1.2 allows remote code execution.	9.8	More Details
CVE-2021-36336	Wyse Management Suite 3.3.1 and below versions contain a deserialization vulnerability that could allow an unauthenticated attacker to execute code on the affected system.	9.8	More Details
CVE-2021-45092	Thinfinity VirtualUI before 3.0 has functionality in /lab.html reachable by default that could allow IFRAME injection via the vpath parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41844	Crocoblock JetEngine before 2.9.1 does not properly validate and sanitize form data.	9.8	More Details
CVE-2021-44350	SQL Injection vulnerability exists in ThinkPHP5 5.0.x <=5.1.22 via the parseOrder function in Builder.php.	9.8	More Details
CVE-2021-0889	In Android TV , there is a possible silent pairing due to lack of rate limiting in the pairing flow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-8.1 Android-9Android ID: A-180745296	9.8	More Details
CVE-2021-42945	A SQL Injection vulnerability exists in ZZCMS 2021 via the askbigclassid parameter in /admin/ask.php.	9.8	More Details
CVE-2021-43113	iTextPDF in iText 7 and up to (excluding 4.4.13.3) 7.1.17 allows command injection via a CompareTool filename that is mishandled on the gs (aka Ghostscript) command line in GhostscriptHelper.java.	9.8	More Details
CVE-2021-43215	iSNS Server Memory Corruption Vulnerability Can Lead to Remote Code Execution	9.8	More Details
CVE-2021-43899	Microsoft 4K Wireless Display Adapter Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-43907	Visual Studio Code WSL Extension Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-44653	Online Magazine Management System 1.0 contains a SQL injection authentication bypass vulnerability. The Admin panel authentication can be bypassed due to SQL injection vulnerability in the login form allowing attacker to gain access as admin to the application.	9.8	More Details
CVE-2021-44655	Online Pre-owned/Used Car Showroom Management System 1.0 contains a SQL injection authentication bypass vulnerability. Admin panel authentication can be bypassed due to SQL injection vulnerability in the login form allowing attacker to get admin access on the application.	9.8	More Details
CVE-2021-4119	bookstack is vulnerable to Improper Access Control	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42216	A Broken or Risky Cryptographic Algorithm exists in AnonAddy 0.8.5 via VerificationController.php.	9.8	More Details
CVE-2021-0956	In NfcTag::discoverTechnologies (activation) of NfcTag.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 additionalSystem execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-189942532	9.8	More Details
CVE-2021-36888	Unauthenticated Arbitrary Options Update vulnerability leading to full website compromise discovered in Image Hover Effects Ultimate (versions <= 9.6.1) WordPress plugin.	9.8	More Details
CVE-2021-39641	Product: AndroidVersions: Android kernelAndroid ID: A-126949257References: N/A	9.8	More Details
CVE-2021-39644	Product: AndroidVersions: Android kernelAndroid ID: A-199809304References: N/A	9.8	More Details
CVE-2021-39645	Product: AndroidVersions: Android kernelAndroid ID: A-199805112References: N/A	9.8	More Details
CVE-2021-39655	Product: AndroidVersions: Android kernelAndroid ID: A-192641593References: N/A	9.8	More Details
CVE-2021-27856	FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p91 and 10.2.2r42 includes an account named "cmuser" that has administrative privileges and no password. Older versions of FatPipe software may also be vulnerable. The FatPipe advisory identifier for this vulnerability is FPSA002.	9.8	More Details
CVE-2020-8105	OS Command Injection vulnerability in the wirelessConnect handler of Abode iota All-In-One Security Kit allows an attacker to inject commands and gain root access. This issue affects: Abode iota All-In-One Security Kit versions prior to 1.0.2.23_6.9V_dev_t2_homekit_RF_2.0.19_s2_kvsABODE oz.	9.6	More Details
CVE-2021-43905	Microsoft Office app Remote Code Execution Vulnerability	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36779	A Missing Authentication for Critical Function vulnerability in SUSE Longhorn allows any workload in the cluster to execute any binary present in the image on the host without authentication. This issue affects: SUSE Longhorn longhorn versions prior to 1.1.3; longhorn versions prior to 1.2.3.	9.6	More Details
CVE-2021-43834	eLabFTW is an electronic lab notebook manager for research teams. In versions prior to 4.2.0 there is a vulnerability which allows an attacker to authenticate as an existing user, if that user was created using a single sign-on authentication option such as LDAP or SAML. It impacts instances where LDAP or SAML is used for authentication instead of the (default) local password mechanism. Users should upgrade to at least version 4.2.0.	9.1	More Details
CVE-2021-43882	Microsoft Defender for IoT Remote Code Execution Vulnerability	9.0	More Details
CVE-2021-4139	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-27855	FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p91 and 10.2.2r42 allows a remote, authenticated attacker with read-only privileges to grant themselves administrative privileges. Older versions of FatPipe software may also be vulnerable. The FatPipe advisory identifier for this vulnerability is FPSA001.	8.8	More Details
CVE-2021-4130	snipe-it is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2021-42309	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24846	The get_query() function of the Ni WooCommerce Custom Order Status WordPress plugin before 1.9.7, used by the niwoocos_ajax AJAX action, available to all authenticated users, does not properly sanitise the sort parameter before using it in a SQL statement, leading to an SQL injection, exploitable by any authenticated users, such as subscriber	8.8	More Details
CVE-2021-42314	Microsoft Defender for IoT Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-42315	Microsoft Defender for IoT Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-43083	Apache PLC4X - PLC4C (Only the C language implementation was effected) was vulnerable to an unsigned integer underflow flaw inside the tcp transport. Users should update to 0.9.1, which addresses this issue. However, in order to exploit this vulnerability, a user would have to actively connect to a mallicious device which could send a response with invalid content. Currently we consider the probability of this being exploited as quite minimal, however this could change in the future, especially with the industrial networks growing more and more together.	8.8	More Details
CVE-2021-45041	SuiteCRM before 7.12.2 and 8.x before 8.0.1 allows authenticated SQL injection via the Tooltips action in the Project module, involving resource_id and start_date.	8.8	More Details
CVE-2021-44874	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to Insecure design on report build via SQL query. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. The bi report module exposes direct SQL commands via POST data in order to select data for report generation. A malicious actor can use the bi report endpoint as a direct SQL prompt under the authenticated user.	8.8	More Details
CVE-2021-27859	A missing authorization vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p91 and 10.2.2r42 allows an authenticated, remote attacker with read-only privileges to create an account with administrative privileges. Older versions of FatPipe software may also be vulnerable. This does not appear to be a CSRF vulnerability. The FatPipe advisory identifier for this vulnerability is FPSA005.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43806	Tuleap is a Libre and Open Source tool for end to end traceability of application and system developments. In affected versions Tuleap does not sanitize properly user settings when constructing the SQL query to browse and search commits in the CVS repositories. A authenticated malicious user with read access to a CVS repository could execute arbitrary SQL queries. Tuleap instances without an active CVS repositories are not impacted. The following versions contain the fix: Tuleap Community Edition 13.2.99.155, Tuleap Enterprise Edition 13.1-7, and Tuleap Enterprise Edition 13.2-6.	8.8	More Details
CVE-2021-45017	Cross Site Request Forgery (CSRF) vulnerability exits in Catfish <=6.1.* when you upload an html file containing CSRF on the website that uses a google editor; you can specify the menu url address as your malicious url address in the Add Menu column.	8.8	More Details
CVE-2021-0968	In osi_malloc and osi_calloc of allocator.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution 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-197868577	8.8	More Details
CVE-2021-0967	In vorbis_book_decodev_set of codebook.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-199065614	8.8	More Details
CVE-2021-0965	In AndroidManifest.xml of Settings, there is a possible pairing of a Bluetooth device without user's consent 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-12 Android-9Android ID: A-194300867	8.8	More Details
CVE-2021-22057	VMware Workspace ONE Access 21.08, 20.10.0.1, and 20.10 contain an authentication bypass vulnerability. A malicious actor, who has successfully provided first-factor authentication, may be able to obtain second-factor authentication provided by VMware Verify.	8.8	More Details
CVE-2021-45099	The addon.stdin service in addon-ssh (aka Home Assistant Community Add-on: SSH & Web Terminal) before 10.0.0 has an attack surface that requires social engineering. NOTE: the vendor does not agree that this is a vulnerability; however, addon.stdin was removed as a defense-in-depth measure against complex social engineering situations	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43877	ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-0930	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC 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-181660091	8.8	More Details
CVE-2020-19316	OS Command injection vulnerability in function link in Filesystem.php in Laravel Framework before 5.8.17.	8.8	More Details
CVE-2021-44657	In StackStorm versions prior to 3.6.0, the jinja interpreter was not run in sandbox mode and thus allows execution of unsafe system commands. Jinja does not enable sandboxed mode by default due to backwards compatibility. Stackstorm now sets sandboxed mode for jinja by default.	8.8	More Details
CVE-2021-41262	Galette is a membership management web application built for non profit organizations and released under GPLv3. Versions prior to 0.9.6 are subject to SQL injection attacks by users with "member" privilege. Users are advised to upgrade to version 0.9.6 as soon as possible. There are no known workarounds.	8.8	More Details
CVE-2021-43437	In sourcecodetester Engineers Online Portal as of 10-21-21, an attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways. Very often multiple websites are hosted on the same IP address. This is where the Host Header comes in. This header specifies which website should process the HTTP request. The web server uses the value of this header to dispatch the request to the specified website. Each website hosted on the same IP address is called a virtual host. And It's possible to send requests with arbitrary Host Headers to the first virtual host.	8.8	More Details
CVE-2021-0918	In gatt_process_notification of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-197536150	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42912	FiberHome ONU GPON AN5506-04-F RP2617 is affected by an OS command injection vulnerability. This vulnerability allows the attacker, once logged in, to send commands to the operating system as the root user via the ping diagnostic tool, bypassing the IP address field, and concatenating OS commands with a semicolon.	8.8	More Details
CVE-2021-4131	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2021-45102	An issue was discovered in HTCondor 9.0.x before 9.0.4 and 9.1.x before 9.1.2. When authenticating to an HTCondor daemon using a SciToken, a user may be granted authorizations beyond what the token should allow.	8.8	More Details
CVE-2021-24750	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 4.8 does not properly sanitise and escape the refUrl in the refDetails AJAX action, available to any authenticated user, which could allow users with a role as low as subscriber to perform SQL injection attacks	8.8	More Details
CVE-2021-41870	An issue was discovered in the firmware update form in Socomec REMOTE VIEW PRO 2.0.41.4. An authenticated attacker can bypass a client-side file-type check and upload arbitrary .php files.	8.8	More Details
CVE-2021-41365	Microsoft Defender for IoT Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43844	MSEdgeRedirect is a tool to redirect news, search, widgets, weather, and more to a user's default browser. MSEdgeRedirect versions before 0.5.0.1 are vulnerable to Remote Code Execution via specifically crafted URLs. This vulnerability requires user interaction and the acceptance of a prompt. With how MSEdgeRedirect is coded, parameters are impossible to pass to any launched file. However, there are two possible scenarios in which an attacker can do more than a minor annoyance. In Scenario 1 (confirmed), a user visits an attacker controlled webpage; the user is prompted with, and downloads, an executable payload; the user is prompted with, and accepts, the aforementioned crafted URL prompt; and RCE executes the payload the user previously downloaded, if the download path is successfully guessed. In Scenario 2 (not yet confirmed), a user visits an attacked controlled webpage; the user is prompted with, and accepts, the aforementioned crafted URL prompt; and a payload on a remote, attacker controlled, SMB server is executed. The issue was found in the _DecodeAndRun() function, in which I incorrectly assumed _WinAPI_UrlIs() would only accept web resources. Unfortunately, file:/// passes the default _WinAPI_UrlIs check(). File paths are now directly checked for and must fail. There is no currently known exploitation of this vulnerability in the wild. A patched version, 0.5.0.1, has been released that checks for and denies these crafted URLs. There are no workarounds for this issue. Users are advised not to accept any unexpected prompts from web pages.	8.8	More Details
CVE-2021-3860	JFrog Artifactory before 7.25.4 (Enterprise+ deployments only), is vulnerable to Blind SQL Injection by a low privileged authenticated user due to incomplete validation when performing an SQL query.	8.8	More Details
CVE-2021-32498	SICK SOPAS ET before version 4.8.0 allows attackers to manipulate the pathname of the emulator and use path traversal to run an arbitrary executable located on the host system. When the user starts the emulator from SOPAS ET the corresponding executable will be started instead of the emulator	8.6	More Details
CVE-2021-32497	SICK SOPAS ET before version 4.8.0 allows attackers to wrap any executable file into an SDD and provide this to a SOPAS ET user. When a user starts the emulator the executable is run without further checks.	8.6	More Details
CVE-2021-43836	Sulu is an open-source PHP content management system based on the Symfony framework. In affected versions an attacker can read arbitrary local files via a PHP file include. In a default configuration this also leads to remote code execution. The problem is patched with the Versions 1.6.44, 2.2.18, 2.3.8, 2.4.0. For users unable to upgrade overwrite the service `sulu_route.generator.expression_token_provider` and wrap the translator before passing it to the expression language.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43837	vault-cli is a configurable command-line interface tool (and python library) to interact with Hashicorp Vault. In versions before 3.0.0 vault-cli features the ability for rendering templated values. When a secret starts with the prefix `!template!`, vault-cli interprets the rest of the contents of the secret as a Jinja2 template. Jinja2 is a powerful templating engine and is not designed to safely render arbitrary templates. An attacker controlling a jinja2 template rendered on a machine can trigger arbitrary code, making this a Remote Code Execution (RCE) risk. If the content of the vault can be completely trusted, then this is not a problem. Otherwise, if your threat model includes cases where an attacker can manipulate a secret value read from the vault using vault-cli, then this vulnerability may impact you. In 3.0.0, the code related to interpreting vault templated secrets has been removed entirely. Users are advised to upgrade as soon as possible. For users unable to upgrade a workaround does exist. Using the environment variable `VAULT_CLI_RENDER=false` or the flag `--no-render` (placed between `vault-cli` and the subcommand, e.g. `vault-cli --no-render get-all`) or adding `render: false` to the vault-cli configuration yaml file disables rendering and removes the vulnerability. Using the python library, you can use: `vault_cli.get_client(render=False)` when creating your client to get a client that will not render templated secrets and thus operates securely.	8.4	More Details
CVE-2021-43587	Dell PowerPath Management Appliance, versions 3.2, 3.1, 3.0 P01, 3.0, and 2.6, use hard-coded cryptographic key. A local high-privileged malicious user may potentially exploit this vulnerability to gain access to secrets and elevate to gain higher privileges.	8.2	More Details
CVE-2021-41028	A combination of a use of hard-coded cryptographic key vulnerability [CWE-321] in FortiClientEMS 7.0.1 and below, 6.4.6 and below and an improper certificate validation vulnerability [CWE-297] in FortiClientWindows, FortiClientLinux and FortiClientMac 7.0.1 and below, 6.4.6 and below may allow an unauthenticated and network adjacent attacker to perform a man-in-the-middle attack between the EMS and the FCT via the telemetry protocol.	8.2	More Details
CVE-2021-44224	A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41260	Galette is a membership management web application built for non profit organizations and released under GPLv3. Versions prior to 0.9.6 do not check for Cross Site Request Forgery attacks. All users are advised to upgrade to 0.9.6 as soon as possible. There are no known workarounds for this issue.	8.2	More Details
CVE-2020-35214	An issue in Atomix v3.1.5 allows a malicious Atomix node to remove states of ONOS storage via abuse of primitive operations.	8.1	More Details
CVE-2021-45101	An issue was discovered in HTCondor before 8.8.15, 9.0.x before 9.0.4, and 9.1.x before 9.1.2. Using standard command-line tools, a user with only READ access to an HTCondor SchedD or Collector daemon can discover secrets that could allow them to control other users' jobs and/or read their data.	8.1	More Details
CVE-2021-43217	Windows Encrypting File System (EFS) Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-24739	The Logo Carousel WordPress plugin before 3.4.2 allows users with a role as low as Contributor to duplicate and view arbitrary private posts made by other users via the Carousel Duplication feature	8.1	More Details
CVE-2021-43833	eLabFTW is an electronic lab notebook manager for research teams. In versions prior to 4.2.0 there is a vulnerability which allows any authenticated user to gain access to arbitrary accounts by setting a specially crafted email address. This vulnerability impacts all instances that have not set an explicit email domain name allowlist. Note that whereas neither administrators nor targeted users are notified of a change, an attacker will need to control an account. The default settings require administrators to validate newly created accounts. The problem has been patched. Users should upgrade to at least version 4.2.0. For users unable to upgrade enabling an email domain allow list (from Sysconfig panel, Security tab) will completely resolve the issue.	8.1	More Details
CVE-2021-41261	Galette is a membership management web application built for non profit organizations and released under GPLv3. Versions prior to 0.9.6 are subject to stored cross site scripting attacks via the preferences footer. The preference footer can only be altered by a site admin. This issue has been resolved in the 0.9.6 release and all users are advised to upgrade. There are no known workarounds.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43935	The impacted products, when configured to use SSO, are affected by an improper authentication vulnerability. This vulnerability allows the application to accept manual entry of any active directory (AD) account provisioned in the application without supplying a password, resulting in access to the application as the supplied AD account, with all associated privileges.	8.1	More Details
CVE-2020-35213	An issue in Atomix v3.1.5 allows attackers to cause a denial of service (DoS) via false link event messages sent to a master ONOS node.	8.1	More Details
CVE-2021-44207	Acclaim USAHERDS through 7.4.0.1 uses hard-coded credentials.	8.1	More Details
CVE-2021-42310	Microsoft Defender for IoT Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-36780	A Missing Authentication for Critical Function vulnerability in longhorn of SUSE Longhorn allows attackers to connect to a longhorn-engine replica instance granting it the ability to read and write data to and from a replica that they should not have access to. This issue affects: SUSE Longhorn longhorn versions prior to 1.1.3; longhorn versions prior to 1.2.3v.	8.1	More Details
CVE-2021-42320	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details
CVE-2021-35234	Numerous exposed dangerous functions within Orion Core has allows for read-only SQL injection leading to privileged escalation. An attacker with low-user privileges may steal password hashes and password salt information.	8.0	More Details
CVE-2021-0933	In onCreate of CompanionDeviceActivity.java or DeviceChooserActivity.java, there is a possible way for HTML tags to interfere with a consent dialog due to improper input validation. This could lead to remote escalation of privilege, confusing the user into accepting pairing of a malicious Bluetooth device, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-172251622	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0932	In showNotification of NavigationModeController.java, there is a possible confused deputy due to an unsafe PendingIntent. This could lead to local escalation of privilege that allows actions performed as the System UI with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-173025705	7.8	More Details
CVE-2021-43747	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-43025	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-1017	In AdapterService and GattService definition of AndroidManifest.xml, there is a possible way to disable bluetooth connection due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-182583850	7.8	More Details
CVE-2021-0929	In ion_dma_buf_end_cpu_access and related functions of ion.c, 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 kernelAndroid ID: A-187527909References: Upstream kernel	7.8	More Details
CVE-2021-0928	In createFromParcel of OutputConfiguration.java, there is a possible parcel serialization/deserialization mismatch due to improper input validation. 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-9Android ID: A-188675581	7.8	More Details
CVE-2021-43024	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43026	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-0927	In requestChannelBrowsable of TvInputManagerService.java, there is a possible permission bypass 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-10 Android-11 Android-12 Android-8.1 Android-9Android ID: A-189824175	7.8	More Details
CVE-2021-0926	In onCreate of NfcImportVCardActivity.java, there is a possible way to add a contact without user's consent 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-12 Android-9Android ID: A-191053931	7.8	More Details
CVE-2021-0924	In xhci_vendor_get_ops of xhci.c, there is a possible out of bounds read due to a missing 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-194461020References: Upstream kernel	7.8	More Details
CVE-2021-1029	In setClientStateLocked of SurfaceFlinger.cpp, there is a possible out of bounds write 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-12Android ID: A-193034677	7.8	More Details
CVE-2021-0923	In createOrUpdate of Permission.java, there is a possible way to gain internal permissions 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-12Android ID: A-195338390	7.8	More Details
CVE-2021-1028	In setClientStateLocked of SurfaceFlinger.cpp, there is a possible out of bounds write 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-12Android ID: A-193034683	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1027	In setTransactionState of SurfaceFlinger, there is possible arbitrary code execution in a privileged process due to improper casting. 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-193033243	7.8	More Details
CVE-2021-0953	In setOnClickActivityIntent of SearchWidgetProvider.java, there is a possible way to access contacts and history bookmarks without permission 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-184046278	7.8	More Details
CVE-2021-0999	In the broadcast definition in AndroidManifest.xml, there is a possible way to set the A2DP bluetooth device connection state 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-12Android ID: A-196858999	7.8	More Details
CVE-2021-43022	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious PNG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-38401	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an untrusted pointer dereference, which may allow an attacker to execute arbitrary code and cause the application to crash.	7.8	More Details
CVE-2021-38421	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an out-of-bounds read, which may allow an attacker to read sensitive information from other memory locations or cause a crash.	7.8	More Details
CVE-2021-1003	In adjustStreamVolume of AudioService.java, there is a possible way for unprivileged app to change audio stream volume 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-12Android ID: A-189857506	7.8	More Details
CVE-2021-1004	In getConfiguredNetworks of WifiServiceImpl.java, there is a possible way to determine whether an app is installed, without query permissions, 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-12Android ID: A-197749180	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38419	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an out-of-bounds write, which can result in data corruption, a system crash, or code execution.	7.8	More Details
CVE-2021-1048	In ep_loop_check_proc of eventpoll.c, 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 kernelAndroid ID: A-204573007References: Upstream kernel	7.8	More Details
CVE-2021-1044	In eicOpsDecryptAes128Gcm of acropora/app/identity/identity_support.c, there is a possible out of bounds write due to a missing 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-195570681References: N/A	7.8	More Details
CVE-2021-38415	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable a heap-based buffer overflow when parsing a specially crafted project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-38413	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to a stack-based buffer overflow, which may allow an attacker to achieve code execution.	7.8	More Details
CVE-2021-39640	In __dwc3_gadget_ep0_queue of ep0.c, there is a possible out of bounds write due to improper locking. 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-157294279References: N/A	7.8	More Details
CVE-2021-38409	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an access of uninitialized pointer, which may allow an attacker read from or write to unexpected memory locations, leading to a denial-of-service.	7.8	More Details
CVE-2021-39651	In TBD of TBD, there is a possible way to access PIN protected settings bypassing PIN confirmation 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 kernelAndroid ID: A-193438173References: N/A	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43021	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious EXR file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-39653	In (TBD) of (TBD), there is a possible way to boot with a hidden debug policy due to a missing warning to the user. This could lead to local escalation of privilege after preparing the device, hiding the warning, and passing the phone to a new user, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-193443223References: N/A	7.8	More Details
CVE-2021-0922	In enforceCrossUserOrProfilePermission of PackageManagerService.java, there is a possible bypass of INTERACT_ACROSS_PROFILES permission 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-11Android ID: A-195630721	7.8	More Details
CVE-2021-0985	In onReceive of AlertReceiver.java, there is a possible way to dismiss system dialog 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-12Android ID: A-190403923	7.8	More Details
CVE-2021-0984	In onNullBinding of ManagedServices.java, there is a possible permission bypass due to an incorrectly unbound service. 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-192475653	7.8	More Details
CVE-2021-0981	In enqueueNotificationInternal of NotificationManagerService.java, there is a possible way to run a foreground service without showing a notification due to improper input validation. 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-11Android ID: A-191981182	7.8	More Details
CVE-2021-1040	In onCreate of BluetoothPairingSelectionFragment.java, 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-182810085	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45078	stab_xcoff_builtin_type in stabs.c in GNU Binutils through 2.37 allows attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact, as demonstrated by an out-of-bounds write. NOTE: this issue exists because of an incorrect fix for CVE-2018-12699.	7.8	More Details
CVE-2021-0970	In createFromParcel of GpsNavigationMessage.java, there is a possible Parcel serialization/deserialization mismatch. 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-196970023	7.8	More Details
CVE-2021-1039	In NotificationAccessActivity 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-182808318	7.8	More Details
CVE-2021-27445	Mesa Labs AmegaView Versions 3.0 and prior has insecure file permissions that could be exploited to escalate privileges on the device.	7.8	More Details
CVE-2021-0649	In stopVpnProfile of Vpn.java, there is a possible VPN profile reset due to a permissions bypass. This could lead to local escalation of privilege CONTROL_ALWAYS_ON_VPN with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-191382886	7.8	More Details
CVE-2021-43028	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-0921	In ParsingPackageImpl of ParsingPackageImpl.java, there is a possible parcel serialization/deserialization mismatch due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-195962697	7.8	More Details
CVE-2021-43237	Windows Setup Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43232	Windows Event Tracing Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43231	Windows NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-0799	In ActivityThread.java, there is a possible way to collide the content provider's authorities. 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-197647956	7.8	More Details
CVE-2021-43229	Windows NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-43226	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-0673	In Audio Aurisys HAL, there is a possible permission bypass 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. Patch ID: ALPS05977326; Issue ID: ALPS05977326.	7.8	More Details
CVE-2021-43223	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-4136	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-43214	Web Media Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43207	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42312	Microsoft Defender for IoT Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-41360	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-41333	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40453	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-40452	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-40441	Windows Media Center Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-23545	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!ReadXPM_W+0x0000000000000531.	7.8	More Details
CVE-2021-43326	Automox Agent before 32 on Windows incorrectly sets permissions on a temporary directory.	7.8	More Details
CVE-2021-43325	Automox Agent 33 on Windows incorrectly sets permissions on a temporary directory. NOTE: this issue exists because of a CVE-2021-43326 regression.	7.8	More Details
CVE-2021-40827	Clementine Music Player through 1.3.1 (when a GLib 2.0.0 DLL is used) is vulnerable to a Read Access Violation on Block Data Move, affecting the MP3 file parsing functionality at memcpy+0x265. The vulnerability is triggered when the user opens a crafted MP3 file or loads a remote stream URL that is mishandled by Clementine. Attackers could exploit this issue to cause a crash (DoS) of the clementine.exe process or achieve arbitrary code execution in the context of the current logged-in Windows user.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40826	Clementine Music Player through 1.3.1 is vulnerable to a User Mode Write Access Violation, affecting the MP3 file parsing functionality at clementine+0x3aa207. The vulnerability is triggered when the user opens a crafted MP3 file or loads a remote stream URL that is mishandled by Clementine. Attackers could exploit this issue to cause a crash (DoS) of the clementine.exe process or achieve arbitrary code execution in the context of the current logged-in Windows user.	7.8	More Details
CVE-2021-4008	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcRenderCompositeGlyphs function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2021-4009	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcXFixesCreatePointerBarrier function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2021-4010	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcScreenSaverSuspend function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2021-4011	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SwapCreateRegister function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2021-43234	Windows Fax Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43230	Windows NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-43891	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43248	Windows Digital Media Receiver Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43883	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-43238	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-44423	An out-of-bounds read vulnerability exists when reading a BMP file using Open Design Alliance (ODA) Drawings Explorer before 2022.12. The specific issue exists after loading BMP files. Unchecked input data from a crafted BMP file leads to an out-of-bounds read. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-0675	In alac decoder, 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. Patch ID: ALPS06064258; Issue ID: ALPS06064258.	7.8	More Details
CVE-2021-43875	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43240	NTFS Set Short Name Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-43518	Teeworlds up to and including 0.7.5 is vulnerable to Buffer Overflow. A map parser does not validate m_Channels value coming from a map file, leading to a buffer overflow. A malicious server may offer a specially crafted map that will overwrite client's stack causing denial of service or code execution.	7.8	More Details
CVE-2021-44860	An out-of-bounds read vulnerability exists when reading a TIF file using Open Design Alliance Drawings SDK before 2022.12. The specific issue exists after loading TIF files. An unchecked input data from a crafted TIF file leads to an out-of-bounds read. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-43029	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43256	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43245	Windows Digital TV Tuner Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-43247	Windows TCP/IP Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-44859	An out-of-bounds read vulnerability exists when reading a TGA file using Open Design Alliance Drawings SDK before 2022.12. The specific issue exists after loading TGA files. An unchecked input data from a crafted TGA file leads to an out-of-bounds read. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-44422	An Improper Input Validation Vulnerability exists when reading a BMP file using Open Design Alliance Drawings SDK before 2022.12. Crafted data in a BMP file can trigger a write operation past the end of an allocated buffer, or lead to a heap-based buffer overflow. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-43831	Gradio is an open source framework for building interactive machine learning models and demos. In versions prior to 2.5.0 there is a vulnerability that affects anyone who creates and publicly shares Gradio interfaces. File paths are not restricted and users who receive a Gradio link can access any files on the host computer if they know the file names or file paths. This is limited only by the host operating system. Paths are opened in read only mode. The problem has been patched in gradio 2.5.0.	7.7	More Details
CVE-2021-43242	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-32499	SICK SOPAS ET before version 4.8.0 allows attackers to manipulate the command line arguments to pass in any value to the Emulator executable.	7.5	More Details
CVE-2021-40851	TCMAN GIM is vulnerable to a lack of authorization in all available webservice methods listed in /PC/WebService.asmx. The exploitation of this vulnerability might allow a remote attacker to obtain information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41498	Buffer overflow in ajaxsoundstudio.com Pyo <lt and 1.03 in the Server_jack_init function. which allows attackers to conduct Denial of Service attacks by arbitrary constructing a overlong server name.	7.5	More Details
CVE-2021-41499	Buffer Overflow Vulnerability exists in ajaxsoundstudio.com n Pyo < 1.03 in the Server_debug function, which allows remote attackers to conduct DoS attacks by deliberately passing on an overlong audio file name.	7.5	More Details
CVE-2020-35209	An issue in Atomix v3.1.5 allows unauthorized Atomix nodes to join a target cluster via providing configuration information.	7.5	More Details
CVE-2021-38244	A regular expression denial of service (ReDoS) vulnerability exits in cbioportal 3.6.21 and older via a POST request to /ProteinArraySignificanceTest.json.	7.5	More Details
CVE-2021-37262	JFinal_cms 5.1.0 is vulnerable to regex injection that may lead to Denial of Service.	7.5	More Details
CVE-2021-41497	Null pointer reference in CMS_Conservative_increment_obj in RaRe-Technologies bounter version 1.01 and 1.10, allows attackers to conduct Denial of Service attacks by inputting a huge width of hash bucket.	7.5	More Details
CVE-2021-45100	The ksmbd server through 3.4.2, as used in the Linux kernel through 5.15.8, sometimes communicates in cleartext even though encryption has been enabled. This occurs because it sets the SMB2_GLOBAL_CAP_ENCRYPTION flag when using the SMB 3.1.1 protocol, which is a violation of the SMB protocol specification. When Windows 10 detects this protocol violation, it disables encryption.	7.5	More Details
CVE-2021-41500	Incomplete string comparison vulnerability exits in cvxopt.org cvxop <= 1.2.6 in APIs (cvxopt.cholmod.diag, cvxopt.cholmod.getfactor, cvxopt.cholmod.solve, cvxopt.cholmod.spsolve), which allows attackers to conduct Denial of Service attacks by construct fake Capsule objects.	7.5	More Details
CVE-2021-44315	In Bus Pass Management System v1.0, Directory Listing/Browsing is enabled on the web server which allows an attacker to view the sensitive files of the application, for example: Any file which contains sensitive information of the user or server.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45098	An issue was discovered in Suricata before 6.0.4. It is possible to bypass/evade any HTTP-based signature by faking an RST TCP packet with random TCP options of the md5header from the client side. After the three-way handshake, it's possible to inject an RST ACK with a random TCP md5header option. Then, the client can send an HTTP GET request with a forbidden URL. The server will ignore the RST ACK and send the response HTTP packet for the client's request. These packets will not trigger a Suricata reject action.	7.5	More Details
CVE-2021-22054	VMware Workspace ONE UEM console 20.0.8 prior to 20.0.8.37, 20.11.0 prior to 20.11.0.40, 21.2.0 prior to 21.2.0.27, and 21.5.0 prior to 21.5.0.37 contain an SSRF vulnerability. This issue may allow a malicious actor with network access to UEM to send their requests without authentication and to gain access to sensitive information.	7.5	More Details
CVE-2021-1045	Product: AndroidVersions: Android kernelAndroid ID: A-195580473References: N/A	7.5	More Details
CVE-2020-35211	An issue in Atomix v3.1.5 allows unauthorized Atomix nodes to become the lead node in a target cluster via manipulation of the variable terms in RaftContext.	7.5	More Details
CVE-2021-44858	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. It is possible to use action=edit&undo= followed by action=mcrundo and action=mcrrestore to view private pages on a private wiki that has at least one page set in $wgWhitelistRead.	7.5	More Details
CVE-2021-20608	Improper Handling of Length Parameter Inconsistency vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior allows a remote unauthenticated attacker to cause a DoS condition in GX Works2 by getting GX Works2 to read a tampered program file from a Mitsubishi Electric PLC by sending malicious crafted packets to tamper with the program file.	7.5	More Details
CVE-2021-22056	VMware Workspace ONE Access 21.08, 20.10.0.1, and 20.10 and Identity Manager 3.3.5, 3.3.4, and 3.3.3 contain an SSRF vulnerability. A malicious actor with network access may be able to make HTTP requests to arbitrary origins and read the full response.	7.5	More Details
CVE-2021-44162	Chain Sea ai chatbot system’s specific file download function has path traversal vulnerability. The function has improper filtering of special characters in URL parameters, which allows a remote attacker to download arbitrary system files without authentication.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39646	Product: AndroidVersions: Android kernelAndroid ID: A-201537251References: N/A	7.5	More Details
CVE-2020-18081	The checkuser function of SEMCMS 3.8 was discovered to contain a vulnerability which allows attackers to obtain the password in plaintext through a SQL query.	7.5	More Details
CVE-2020-18077	A buffer overflow vulnerability in the Virtual Path Mapping component of FTPShell v6.83 allows attackers to cause a denial of service (DoS).	7.5	More Details
CVE-2021-41561	Improper Input Validation vulnerability in Parquet-MR of Apache Parquet allows an attacker to DoS by malicious Parquet files. This issue affects Apache Parquet-MR version 1.9.0 and later versions.	7.5	More Details
CVE-2021-41451	A misconfiguration in HTTP/1.0 and HTTP/1.1 of the web interface in TP-Link AX10v1 before V1_211117 allows a remote unauthenticated attacker to send a specially crafted HTTP request and receive a misconfigured HTTP/0.9 response, potentially leading into a cache poisoning attack.	7.5	More Details
CVE-2021-27857	A missing authorization vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p91 and 10.2.2r42 allows a remote, unauthenticated attacker to download a configuration archive. The attacker needs to know or correctly guess the hostname of the target system since the hostname is used as part of the configuration archive file name. Older versions of FatPipe software may also be vulnerable. The FatPipe advisory identifier for this vulnerability is FPSA003.	7.5	More Details
CVE-2021-42913	The SyncThru Web Service on Samsung SCX-6x55X printers allows an attacker to gain access to a list of SMB users and cleartext passwords by reading the HTML source code. Authentication is not required.	7.5	More Details
CVE-2021-4110	mruby is vulnerable to NULL Pointer Dereference	7.5	More Details
CVE-2021-23797	All versions of package http-server-node are vulnerable to Directory Traversal via use of --path-as-is.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0925	In rw_t4t_sm_detect_ndef of rw_t4t.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure due to a limited change in behavior based on the out of bounds data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-191444150	7.5	More Details
CVE-2021-45451	In Mbed TLS before 3.1.0, psa_aead_generate_nonce allows policy bypass or oracle-based decryption when the output buffer is at memory locations accessible to an untrusted application.	7.5	More Details
CVE-2021-43233	Remote Desktop Client Remote Code Execution Vulnerability	7.5	More Details
CVE-2021-43228	SymCrypt Denial of Service Vulnerability	7.5	More Details
CVE-2021-43839	Cronos is a commercial implementation of a blockchain. In Cronos nodes running versions before v0.6.5, it is possible to take transaction fees from Cosmos SDK's FeeCollector for the current block by sending a custom crafted MsgEthereumTx. This problem has been patched in Cronos v0.6.5. There are no tested workarounds. All validator node operators are recommended to upgrade to Cronos v0.6.5 at their earliest possible convenience.	7.5	More Details
CVE-2021-43225	Bot Framework SDK Remote Code Execution Vulnerability	7.5	More Details
CVE-2021-43222	Microsoft Message Queuing Information Disclosure Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44877	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to Incorrect Access Control. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. A broken access control vulnerability has been found while using a temporary generated token in order to consume api resources. The vulnerability allows an unauthenticated attacker to use an api endpoint to generate a temporary JWT token that is designed to reference the correct tenant prior to authentication, to request system configuration parameters using direct api requests. The correct exploitation of this vulnerability causes sensitive information exposure. In case the tenant has an smtp credential set, the full credential information is disclosed.	7.5	More Details
CVE-2021-43888	Microsoft Defender for IoT Information Disclosure Vulnerability	7.5	More Details
CVE-2021-43893	Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability	7.5	More Details
CVE-2021-24981	The Directorist WordPress plugin before 7.0.6.2 was vulnerable to Cross-Site Request Forgery to Remote File Upload leading to arbitrary PHP shell uploads in the wp-content/plugins directory.	7.5	More Details
CVE-2021-45290	A Denial of Service vulnerability exits in Binaryen 103 due to an assertion abort in wasm::handle_unreachable.	7.5	More Details
CVE-2021-1002	In WT_Interpolate of eas_wtengine.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-194533433	7.5	More Details
CVE-2021-43236	Microsoft Message Queuing Information Disclosure Vulnerability	7.5	More Details
CVE-2021-45043	HD-Network Real-time Monitoring System 2.0 allows ../ directory traversal to read /etc/shadow via the /language/lang s_Language parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1022	In btif_in_hf_client_generic_evt of btif_hf_client.cc, there is a possible Bluetooth service crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-180420059	7.5	More Details
CVE-2019-19138	Ivanti Workspace Control before 10.4.50.0 allows attackers to degrade integrity.	7.5	More Details
CVE-2021-45450	In Mbed TLS before 2.28.0 and 3.x before 3.1.0, psa_cipher_generate_iv and psa_cipher_encrypt allow policy bypass or oracle-based decryption when the output buffer is at memory locations accessible to an untrusted application.	7.5	More Details
CVE-2021-23450	All versions of package dojo are vulnerable to Prototype Pollution via the setObject function.	7.5	More Details
CVE-2021-43892	Microsoft BizTalk ESB Toolkit Spoofing Vulnerability	7.4	More Details
CVE-2021-43219	DirectX Graphics Kernel File Denial of Service Vulnerability	7.4	More Details
CVE-2021-1021	In snoozeNotificationInt of NotificationManagerService.java, there is a possible way to disable notification for an arbitrary user due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-195031703	7.3	More Details
CVE-2021-1020	In snoozeNotification of NotificationListenerService.java, there is a possible way to disable notification for an arbitrary user due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-195111725	7.3	More Details
CVE-2021-1019	In snoozeNotification of NotificationListenerService.java, there is a possible permission confusion due to a misleading user consent dialog. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-195031401	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1016	In onCreate of UsbPermissionActivity.java, there is a possible way to grant an app access to USB without informed user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-183610267	7.3	More Details
CVE-2021-27453	Mesa Labs AmegaView Versions 3.0 uses default cookies that could be set to bypass authentication to the web application, which may allow an attacker to gain access.	7.3	More Details
CVE-2021-27451	Mesa Labs AmegaView Versions 3.0 and prior's passcode is generated by an easily reversible algorithm, which may allow an attacker to gain access to the device.	7.3	More Details
CVE-2021-0434	In onReceive of BluetoothPermissionRequest.java, there is a possible phishing attack allowing a malicious Bluetooth device to acquire permissions based on insufficient information presented to the user in the consent dialog. 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-9Android ID: A-167403112	7.3	More Details
CVE-2021-0769	In onCreate of AllowBindAppWidgetActivity.java, there is a possible bypass of user interaction requirements due to unclear UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-184676316	7.3	More Details
CVE-2021-0954	In ResolverActivity, there is a possible user interaction bypass due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-143559931	7.3	More Details
CVE-2021-43889	Microsoft Defender for IoT Remote Code Execution Vulnerability	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43835	Sulu is an open-source PHP content management system based on the Symfony framework. In affected versions Sulu users who have access to any subset of the admin UI are able to elevate their privilege. Over the API it was possible for them to give themselves permissions to areas which they did not already had. This issue was introduced in 2.0.0-RC1 with the new ProfileController putAction. The versions have been patched in 2.2.18, 2.3.8 and 2.4.0. For users unable to upgrade the only known workaround is to apply a patch to the ProfileController manually.	7.2	More Details
CVE-2021-40853	TCMAN GIM does not perform an authorization check when trying to access determined resources. A remote attacker could exploit this vulnerability to access URL that require privileges without having them. The exploitation of this vulnerability might allow a remote attacker to obtain sensible information.	7.2	More Details
CVE-2021-42294	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2021-42138	A user of a machine protected by SafeNet Agent for Windows Logon may leverage weak entropy to access the encrypted credentials of any or all the users on that machine.	7.2	More Details
CVE-2021-43890	We have investigated reports of a spoofing vulnerability in AppX installer that affects Microsoft Windows. Microsoft is aware of attacks that attempt to exploit this vulnerability by using specially crafted packages that include the malware family known as Emotet/Trickbot/Bazaloader. An attacker could craft a malicious attachment to be used in phishing campaigns. The attacker would then have to convince the user to open the specially crafted attachment. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Please see the Security Updates table for the link to the updated app. Alternatively you can download and install the Installer using the links provided in the FAQ section. Please see the Mitigations and Workaround sections for important information about steps you can take to protect your system from this vulnerability. December 27 2023 Update: In recent months, Microsoft Threat Intelligence has seen an increase in activity from threat actors leveraging social engineering and phishing techniques to target Windows OS users and utilizing the ms-appinstaller URI scheme. To address this increase in activity, we have updated the App Installer to disable the ms-appinstaller protocol by default and recommend other potential mitigations.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44023	A link following denial-of-service (DoS) vulnerability in the Trend Micro Security (Consumer) 2021 familiy of products could allow an attacker to abuse the PC Health Checkup feature of the product to create symlinks that would allow modification of files which could lead to a denial-of-service.	7.1	More Details
CVE-2021-43239	Windows Recovery Environment Agent Elevation of Privilege Vulnerability	7.1	More Details
CVE-2021-3960	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the UpdateServer component of Bitdefender GravityZone allows an attacker to execute arbitrary code on vulnerable instances. This issue affects Bitdefender GravityZone versions prior to 3.3.8.272	7.1	More Details
CVE-2020-8968	Parallels Remote Application Server (RAS) allows a local attacker to retrieve certain profile password in clear text format by uploading a previously stored cyphered file by Parallels RAS. The confidentiality, availability and integrity of the information of the user could be compromised if an attacker is able to recover the profile password.	7.1	More Details
CVE-2021-0963	In onCreate of KeyChainActivity.java, there is a possible way to use an app certificate stored in keychain 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-199754277	7.1	More Details
CVE-2021-0955	In pf_write_buf of FuseDaemon.cpp, there is possible memory corruption 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-11Android ID: A-192085766	7.0	More Details
CVE-2021-35248	It has been reported that any Orion user, e.g. guest accounts can query the Orion.UserSettings entity and enumerate users and their basic settings.	6.8	More Details
CVE-2021-40170	An RF replay attack vulnerability in the SecuritasHome home alarm system, version HPGW-G 0.0.2.23F BG_U-ITR-F1-BD_BL.A30.20181117, allows an attacker to trigger arbitrary system functionality by replaying previously recorded signals. This lets an adversary, among other things, disarm an armed system.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3959	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService component of Bitdefender Endpoint Security Tools allows an attacker to proxy requests to the relay server. This issue affects: Bitdefender Bitdefender GravityZone versions prior to 3.3.8.272	6.8	More Details
CVE-2021-39639	In TBD of fvp.c, there is a possible way to glitch CPU behavior due to a missing permission check. This could lead to local escalation of privilege with physical access to device internals with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-198291476References: N/A	6.8	More Details
CVE-2021-35244	The "Log alert to a file" action within action management enables any Orion Platform user with Orion alert management rights to write to any file. An attacker with Orion alert management rights could use this vulnerability to perform an unrestricted file upload causing a remote code execution.	6.8	More Details
CVE-2021-0895	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672003.	6.7	More Details
CVE-2021-0896	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05671206.	6.7	More Details
CVE-2021-0897	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05670549.	6.7	More Details
CVE-2021-0894	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672038.	6.7	More Details
CVE-2021-0898	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672071.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0904	In SRAMROM, there is a possible permission bypass due to an insecure permission setting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06076938; Issue ID: ALPS06076938.	6.7	More Details
CVE-2021-0899	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672059.	6.7	More Details
CVE-2021-0893	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05687474.	6.7	More Details
CVE-2021-0901	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05664618.	6.7	More Details
CVE-2021-0903	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05656488.	6.7	More Details
CVE-2021-0679	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05687781.	6.7	More Details
CVE-2021-23814	This affects the package unisharp/laravel-filemanager from 0.0.0. The upload() function does not sufficiently validate the file type when uploading. An attacker may be able to reproduce the following steps: - Install a package with a web Laravel application. - Navigate to the Upload window - Upload an image file, then capture the request - Edit the request contents with a malicious file (webshell) - Enter the path of file uploaded on URL - Remote Code Execution **Note: Prevention for bad extensions can be done by using a whitelist in the config file(lfm.php). Corresponding document can be found in the [here](https://unisharp.github.io/laravel-filemanager/configfolder-categories).	6.7	More Details
CVE-2021-0678	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05722511.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1024	In onEventReceived of EventResultPersister.java, there is a possible intent redirection due to a confused deputy. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-191283525	6.7	More Details
CVE-2021-39652	In sec_ts_parsing_cmds of (TBD), there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-194499021References: N/A	6.7	More Details
CVE-2021-36316	Dell EMC Avamar Server versions 18.2, 19.1, 19.2, 19.3, and 19.4 contain an improper privilege management vulnerability in AUI. A malicious user with high privileges could potentially exploit this vulnerability, leading to the disclosure of the AUI info and performing some unauthorized operation on the AUI.	6.7	More Details
CVE-2021-39656	In __configfs_open_file of file.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174049066References: Upstream kernel	6.7	More Details
CVE-2021-0977	In phNxpNHal_DtaUpdate of phNxpNciHal_dta.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-183487770	6.7	More Details
CVE-2021-36318	Dell EMC Avamar versions 18.2,19.1,19.2,19.3,19.4 contain a plain-text password storage vulnerability. A high privileged user could potentially exploit this vulnerability, leading to a complete outage.	6.7	More Details
CVE-2021-39650	In (TBD) of (TBD), 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-169763055References: N/A	6.7	More Details
CVE-2021-39649	In regmap_exit of regmap.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174049006References: N/A	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36317	Dell EMC Avamar Server version 19.4 contains a plain-text password storage vulnerability in AvInstaller. A local attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.7	More Details
CVE-2021-39643	In ic_startRetrieveEntryValue of acropora/app/identity/ic.c, there is a possible bypass of defense-in-depth due to missing validation of the return value. 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-195573629References: N/A	6.7	More Details
CVE-2021-39638	In periodic_io_work_func of lwis_periodic_io.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-195607566References: N/A	6.7	More Details
CVE-2021-41276	Tuleap is a Libre and Open Source tool for end to end traceability of application and system developments. In affected versions Tuleap does not sanitize properly the search filter built from the ldap_id attribute of a user during the daily synchronization. A malicious user could force accounts to be suspended or take over another account by forcing the update of the ldap_uid attribute. Note that the malicious user either need to have site administrator capability on the Tuleap instance or be an LDAP operator with the capability to create/modify account. The Tuleap instance needs to have the LDAP plugin activated and enabled for this issue to be exploitable. This issue has been patched in Tuleap Community Edition 13.2.99.31, Tuleap Enterprise Edition 13.1-5, and Tuleap Enterprise Edition 13.2-3.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43782	Tuleap is a Libre and Open Source tool for end to end traceability of application and system developments. This is a follow up to GHSA-887w-pv2r-x8pm/CVE-2021-41276, the initial fix was incomplete. Tuleap does not sanitize properly the search filter built from the ldap_id attribute of a user during the daily synchronization. A malicious user could force accounts to be suspended or take over another account by forcing the update of the ldap_uid attribute. Note that the malicious user either need to have site administrator capability on the Tuleap instance or be an LDAP operator with the capability to create/modify account. The Tuleap instance needs to have the LDAP plugin activated and enabled for this issue to be exploitable. The following versions contain the fix: Tuleap Community Edition 13.2.99.83, Tuleap Enterprise Edition 13.1-6, and Tuleap Enterprise Edition 13.2-4.	6.7	More Details
CVE-2021-42550	In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.	6.6	More Details
CVE-2021-43244	Windows Kernel Information Disclosure Vulnerability	6.5	More Details
CVE-2020-35215	An issue in Atomix v3.1.5 allows attackers to access sensitive information when a malicious Atomix node queries distributed variable primitives which contain the entire primitive lists that ONOS nodes use to share important states.	6.5	More Details
CVE-2021-26800	Cross Site Request Forgery (CSRF) vulnerability in Change-password.php in phpgurukul user management system in php using stored procedure V1.0, allows attackers to change the password to an arbitrary account.	6.5	More Details
CVE-2021-42809	Improper Access Control of Dynamically-Managed Code Resources (DLL) in Thales Sentinel Protection Installer could allow the execution of arbitrary code.	6.5	More Details
CVE-2021-44857	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. It is possible to use action=mcrundo followed by action=mcrrestore to replace the content of any arbitrary page (that the user doesn't have edit rights for). This applies to any public wiki, or a private wiki that has at least one page set in $wgWhitelistRead.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41843	An authenticated SQL injection issue in the calendar search function of OpenEMR 6.0.0 before patch 3 allows an attacker to read data from all tables of the database via the parameter provider_id, as demonstrated by the /interface/main/calendar/index.php?module=PostCalendar&func=search URI.	6.5	More Details
CVE-2021-44145	In the TransformXML processor of Apache NiFi before 1.15.1 an authenticated user could configure an XSLT file which, if it included malicious external entity calls, may reveal sensitive information.	6.5	More Details
CVE-2021-43847	HumHub is an open-source social network kit written in PHP. Prior to HumHub version 1.10.3 or 1.9.3, it could be possible for registered users to become unauthorized members of private Spaces. Versions 1.10.3 and 1.9.3 contain a patch for this issue.	6.5	More Details
CVE-2021-36337	Dell Wyse Management Suite version 3.3.1 and prior support insecure Transport Security Protocols TLS 1.0 and TLS 1.1 which are susceptible to Man-In-The-Middle attacks thereby compromising Confidentiality and Integrity of data.	6.5	More Details
CVE-2021-0993	In getOffsetBeforeAfter of TextLine.java, there is a possible denial of service due to resource exhaustion. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-193849901	6.5	More Details
CVE-2021-43216	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	6.5	More Details
CVE-2021-42293	Microsoft Jet Red Database Engine and Access Connectivity Engine Elevation of Privilege Vulnerability	6.5	More Details
CVE-2021-20330	An attacker with basic CRUD permissions on a replicated collection can run the applyOps command with specially malformed oplog entries, resulting in a potential denial of service on secondaries. This issue affects MongoDB Server v4.0 versions prior to 4.0.27; MongoDB Server v4.2 versions prior to 4.2.16; MongoDB Server v4.4 versions prior to 4.4.9.	6.5	More Details
CVE-2020-35210	A vulnerability in Atomix v3.1.5 allows attackers to cause a denial of service (DoS) via a Raft session flooding attack using Raft OpenSessionRequest messages.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42808	Improper Access Control in Thales Sentinel Protection Installer could allow a local user to escalate privileges.	6.5	More Details
CVE-2021-0976	In toBARK of floor0.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-199680600	6.5	More Details
CVE-2021-0969	In getTitle of AccessPoint.java, there is a possible unhandled exception due to a missing null check. This could lead to remote denial of service if a proximal Wi-Fi AP provides invalid information with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-199922685	6.5	More Details
CVE-2021-4123	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	6.5	More Details
CVE-2021-0964	In C2SoftMP3::process() of C2SoftMp3Dec.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-193363621	6.5	More Details
CVE-2021-0650	In WT_InterpolateNoLoop of eas_wtengine.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-190286685	6.5	More Details
CVE-2021-38900	IBM Business Process Manager 8.5 and 8.6 and IBM Business Automation Workflow 18.0, 19.0, 20.0 and 21.0 could allow a privileged user to obtain highly sensitive information due to improper access controls. IBM X-Force ID: 209607.	6.5	More Details
CVE-2021-0971	In MPEG4Source::read of MPEG4Extractor.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-188893559	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43812	The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. Versions before 1.6.2 do not filter out certain returnTo parameter values from the login url, which expose the application to an open redirect vulnerability. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue.	6.4	More Details
CVE-2021-0920	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug due to a race condition. 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-196926917References: Upstream kernel	6.4	More Details
CVE-2021-39642	In synchronous_process_io_entries of lwis_ioctl.c, there is a possible out of bounds write due to a race condition. 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-195731663References: N/A	6.4	More Details
CVE-2021-4124	janus-gateway is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-43440	Multiple Stored XSS Vulnerabilities in the Source Code of iOrder 1.0 allow remote attackers to execute arbitrary code via signup form in the Name and Phone number field.	6.1	More Details
CVE-2021-4121	yetiforcecrm is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2012-20001	PrestaShop before 1.5.2 allows XSS via the "<object data='data:text/html" substring in the message field.	6.1	More Details
CVE-2021-45018	Cross Site Scripting (XSS) vulnerability exists in Catfish <=6.3.0 via a Google search in url:/catfishcms/index.php/admin/Index/addmenu.htmland then the .html file on the website that uses this editor (the file suffix is allowed).	6.1	More Details
CVE-2021-24956	The Blog2Social: Social Media Auto Post & Scheduler WordPress plugin before 6.8.7 does not sanitise and escape the b2sShowByDate parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24941	The Popups, Welcome Bar, Optins and Lead Generation Plugin WordPress plugin before 2.0.5 does not sanitise and escape the message_id parameter of the get_message_action_row AJAX action before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-24907	The Contact Form, Drag and Drop Form Builder for WordPress plugin before 1.8.0 does not escape the status parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-24578	The SportsPress WordPress plugin before 2.7.9 does not sanitise and escape its match_day parameter before outputting back in the Events backend page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-45085	XSS can occur in GNOME Web (aka Epiphany) before 40.4 and 41.x before 41.1 via an about: page, as demonstrated by ephy-about:overview when a user visits an XSS payload page often enough to place that page on the Most Visited list.	6.1	More Details
CVE-2021-45086	XSS can occur in GNOME Web (aka Epiphany) before 40.4 and 41.x before 41.1 because a server's suggested_filename is used as the pdf_name value in PDF.js.	6.1	More Details
CVE-2021-40852	TCMAN GIM is affected by an open redirect vulnerability. This vulnerability allows the redirection of user navigation to pages controlled by the attacker. The exploitation of this vulnerability might allow a remote attacker to obtain information.	6.1	More Details
CVE-2020-18985	An issue in /domain/service/.ewell-known/caldav of Zimbra Collaboration 8.8.12 allows attackers to redirect users to any arbitrary website of their choosing.	6.1	More Details
CVE-2021-26787	A cross site scripting (XSS) vulnerability in Genesys Workforce Management 8.5.214.20 can occur (during record deletion) via the Time-off parameter.	6.1	More Details
CVE-2021-43678	Wechat-php-sdk v1.10.2 is affected by a Cross Site Scripting (XSS) vulnerability in Wechat.php.	6.1	More Details
CVE-2021-43675	Lychee-v3 3.2.16 is affected by a Cross Site Scripting (XSS) vulnerability in php/Access/Guest.php. The function exit will terminate the script and print the message to the user. The message will contain albumID which is controlled by the user.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36450	Verint Workforce Optimization (WFO) 15.2.8.10048 allows XSS via the control/my_notifications NEWUINAV parameter.	6.1	More Details
CVE-2021-44916	Opmantek Open-AudIT Community 4.2.0 (Fixed in 4.3.0) is affected by a Cross Site Scripting (XSS) vulnerability. If a bad value is passed to the routine via a URL, malicious JavaScript code can be executed in the victim's browser.	6.1	More Details
CVE-2020-18984	A reflected cross-site scripting (XSS) vulnerability in the zimbraAdmin/public/secureRequest.jsp component of Zimbra Collaboration 8.8.12 allows unauthenticated attackers to execute arbitrary web scripts or HTML via a host header injection.	6.1	More Details
CVE-2021-45088	XSS can occur in GNOME Web (aka Epiphany) before 40.4 and 41.x before 41.1 via an error page.	6.1	More Details
CVE-2021-44163	Chain Sea ai chatbot backend has improper filtering of special characters in URL parameters, which allows a remote attacker to perform JavaScript injection for XSS (reflected Cross-site scripting) attack without authentication.	6.1	More Details
CVE-2021-44116	Cross Site Scripting (XSS) vulnerability exits in Anchor CMS <=0.12.7 in posts.php. Attackers can use the posts column to upload the title and content containing malicious code to achieve the purpose of obtaining the administrator cookie, thereby achieving other malicious operations.	6.1	More Details
CVE-2021-45087	XSS can occur in GNOME Web (aka Epiphany) before 40.4 and 41.x before 41.1 when View Source mode or Reader mode is used, as demonstrated by a a page title.	6.1	More Details
CVE-2021-36887	Cross-Site Request Forgery (CSRF) vulnerability leading to Cross-Site Scripting (XSS) discovered in tarteaucitron.js – Cookies legislation & GDPR WordPress plugin (versions <= 1.5.4), vulnerable parameters "tarteaucitronEmail" and "tarteaucitronPass".	6.1	More Details
CVE-2021-36350	Dell PowerScale OneFS, versions 8.2.2-9.3.0.x, contain an authentication bypass by primary weakness in one of the authentication factors. A remote unauthenticated attacker may potentially exploit this vulnerability and bypass one of the factors of authentication.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29847	BMC firmware (IBM Power System S821LC Server (8001-12C) OP825.50) configuration changed to allow an authenticated user to open an insecure communication channel which could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 205267.	5.9	More Details
CVE-2020-35216	An issue in Atomix v3.1.5 allows attackers to cause a denial of service (DoS) via false member down event messages.	5.9	More Details
CVE-2021-45105	Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.	5.9	More Details
CVE-2021-43246	Windows Hyper-V Denial of Service Vulnerability	5.6	More Details
CVE-2021-43750	Adobe Premiere Rush versions 1.5.16 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-44924	An infinite loop vulnerability exists in gpac 1.1.0 in the gf_log function, which causes a Denial of Service.	5.5	More Details
CVE-2021-43748	Adobe Premiere Rush versions 1.5.16 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-44926	A null pointer dereference vulnerability exists in gpac 1.1.0-DEV in the gf_node_get_tag function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-44923	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_dump_vrml_dyn_field.isra function, which causes a segmentation fault and application crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44925	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_svg_get_attribute_name function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-44922	A null pointer dereference vulnerability exists in gpac 1.1.0 in the BD_CheckSFTimeOffset function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-41496	Buffer overflow in the array_from_pyobj function of fortranobject.c in NumPy < 1.19, which allows attackers to conduct a Denial of Service attacks by carefully constructing an array with negative values. NOTE: The vendor does not agree this is a vulnerability; the negative dimensions can only be created by an already privileged user (or internally)	5.5	More Details
CVE-2021-36341	Dell Wyse Device Agent version 14.5.4.1 and below contain a sensitive data exposure vulnerability. A local authenticated user with low privileges could potentially exploit this vulnerability in order to access sensitive information.	5.5	More Details
CVE-2021-44921	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_isom_parse_movie_boxes_internal function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-44920	An invalid memory address dereference vulnerability exists in gpac 1.1.0 in the dump_od_to_saf.isra function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-44919	A Null Pointer Dereference vulnerability exists in the gf_sg_vrml_mf_alloc function in gpac 1.1.0-DEV, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-44918	A Null Pointer Dereference vulnerability exists in gpac 1.1.0 in the gf_node_get_field function, which can cause a segmentation fault and application crash.	5.5	More Details
CVE-2021-44917	A Divide by Zero vulnerability exists in gnuplot 5.4 in the boundary3d function in graph3d.c, which could cause a Arithmetic exception and application crash.	5.5	More Details
CVE-2021-45297	An infinite loop vulnerability exists in Gpac 1.0.1 in gf_get_bit_size.	5.5	More Details
CVE-2021-45293	A Denial of Service vulnerability exists in Binaryen 103 due to an Invalid memory address dereference in wasm::WasmBinaryBuilder::visitLet.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45288	A Double Free vulnerability exists in filedump.c in GPAC 1.0.1, which could cause a Denail of Service via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-45292	The gf_isom_hint_rtp_read function in GPAC 1.0.1 allows attackers to cause a denial of service (Invalid memory address dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-45291	The gf_dump_setup function in GPAC 1.0.1 allows malicoius users to cause a denial of service (Invalid memory address dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-43746	Adobe Premiere Rush versions 1.5.16 (and earlier) allows access to an uninitialized pointer vulnerability that allows remote attackers to disclose sensitive information on affected installations. 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 MP4 files. The issue results from the lack of proper initialization of memory prior to accessing it.	5.5	More Details
CVE-2021-45289	A vulnerability exists in GPAC 1.0.1 due to an omission of security-relevant Information, which could cause a Denial of Service. The program terminates with signal SIGKILL.	5.5	More Details
CVE-2021-43749	Adobe Premiere Rush versions 1.5.16 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-44927	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_sg_vrml_mf_append function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-1026	In startRanging of RttServiceImpl.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-194798757	5.5	More Details
CVE-2021-45095	pep_sock_accept in net/phonet/pep.c in the Linux kernel through 5.15.8 has a refcount leak.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0931	In getAlias of BluetoothDevice.java, there is a possible way to create misleading permission dialogs due to missing data filtering. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-180747689	5.5	More Details
CVE-2021-43235	Storage Spaces Controller Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0704	In createNoCredentialsPermissionNotification and related functions of AccountManagerService.java, there is a possible way to retrieve accounts from the device without permissions due to a permissions bypass. 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-11 Android-9Android ID: A-179338675	5.5	More Details
CVE-2021-0653	In enqueueNotification of NetworkPolicyManagerService.java, there is a possible way to retrieve a trackable identifier due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-177931370	5.5	More Details
CVE-2021-1043	In TBD of TBD, there is a possible downgrade attack due to under utilized anti-rollback protections. 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-194697257References: N/A	5.5	More Details
CVE-2021-1041	In (TBD) of (TBD), there is a possible out of bounds read due to memory corruption. 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-182950799References: N/A	5.5	More Details
CVE-2021-1038	In UserDetailsActivity of AndroidManifest.xml, there is a possible DoS due to a tapjacking/overlay attack. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-183411279	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1009	In setApplicationCategoryHint of PackageManagerService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-189858128	5.5	More Details
CVE-2021-1030	In setNotificationsShownFromListener of NotificationManagerService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-194697001	5.5	More Details
CVE-2021-43896	Microsoft PowerShell Spoofing Vulnerability	5.5	More Details
CVE-2021-1025	In hasNamedWallpaper of WallpaperManagerService.java, there is a possible way to determine whether an app is installed, without query permissions, due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-193800652	5.5	More Details
CVE-2021-43880	Windows Mobile Device Management Elevation of Privilege Vulnerability	5.5	More Details
CVE-2021-43255	Microsoft Office Trust Center Spoofing Vulnerability	5.5	More Details
CVE-2021-1014	In getNetworkTypeForSubscriber of PhoneInterfaceManager.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-186776740	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1013	In checkExistsAndEnforceCannotModifyImmutablyRestrictedPermission of PermissionManagerService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-186404356	5.5	More Details
CVE-2021-43243	VP9 Video Extensions Information Disclosure Vulnerability	5.5	More Details
CVE-2021-1005	In getDeviceIdWithFeature of PhoneInterfaceManager.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-186530889	5.5	More Details
CVE-2021-1001	In PVInitVideoEncoder of mp4enc_api.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-190435883	5.5	More Details
CVE-2021-0998	In 'ih264e_find_bskip_params()' of ih264e_me.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-193442575	5.5	More Details
CVE-2021-0997	In handleUpdateNetworkState of GnssNetworkConnectivityHandler.java , there is a possible APN disclosure due to log information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-191086488	5.5	More Details
CVE-2021-1012	In onResume of NotificationAccessDetails.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-195412179	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1011	In setPackageStoppedState of PackageManagerService.java, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-188219307	5.5	More Details
CVE-2021-1010	In getSigningKeySet of PackageManagerService.java, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-189857801	5.5	More Details
CVE-2021-42295	Visual Basic for Applications Information Disclosure Vulnerability	5.5	More Details
CVE-2021-43224	Windows Common Log File System Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0966	In code generated by BuildParcelFields of generate_cpp.cpp, there is a possible way for a crafted parcelable to reveal uninitialized memory of a target process due to uninitialized data. This could lead to local information disclosure across Binder transactions with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-198346478	5.5	More Details
CVE-2021-43227	Storage Spaces Controller Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0674	In alac decoder, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06064258; Issue ID: ALPS06064237.	5.5	More Details
CVE-2021-20607	Integer Underflow vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior, Mitsubishi Electric MELSOFT Navigator versions 2.84N and prior and Mitsubishi Electric EZSocket versions 5.4 and prior allows an attacker to cause a DoS condition in the software by getting a user to open malicious project file specially crafted by an attacker.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20606	Out-of-bounds Read vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior, Mitsubishi Electric MELSOFT Navigator versions 2.84N and prior and Mitsubishi Electric EZSocket versions 5.4 and prior allows an attacker to cause a DoS condition in the software by getting a user to open malicious project file specially crafted by an attacker.	5.5	More Details
CVE-2021-0979	In isRequestPinItemSupported of ShortcutService.java, there is a possible cross-user leak of packages in which the default launcher supports requests to create pinned shortcuts due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-191772737	5.5	More Details
CVE-2021-0986	In hasGrantedPolicy of DevicePolicyManagerService.java, there is a possible information disclosure about the device owner, profile owner, or device admin 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-12Android ID: A-192247339	5.5	More Details
CVE-2021-3179	GGLocker iOS application, contains an insecure data storage of the password hash value which results in an authentication bypass.	5.5	More Details
CVE-2021-43842	Wiki.js is a wiki app built on Node.js. Wiki.js versions 2.5.257 and earlier are vulnerable to stored cross-site scripting through a SVG file upload. By creating a crafted SVG file, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the SVG is viewed directly by other users. Scripts do not execute when loaded inside a page via normal `<img>` tags. Commit 5d3e81496fba1f0fbd64eeb855f30f69a9040718 fixes this vulnerability by adding an optional (enabled by default) SVG sanitization step to all file uploads that match the SVG mime type. As a workaround, disable file upload for all non-trusted users. Wiki.js version 2.5.260 is the first production version to contain a patch. Version 2.5.258 is the first development build to contain a patch and is available only as a Docker image as requarks/wiki:canary-2.5.258.	5.4	More Details
CVE-2021-38883	IBM Business Automation Workflow 18.0, 19.0, 20,0 and 21.0 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209165.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38966	IBM Cloud Pak for Automation 21.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 212357.	5.4	More Details
CVE-2021-24738	The Logo Carousel WordPress plugin before 3.4.2 does not validate and escape the "Logo Margin" carousel option, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2021-42584	A Stored Cross Site Scripting (XSS) issue exists in Convos-Chat before 6.32.	5.4	More Details
CVE-2021-4132	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-38893	IBM Business Process Manager 8.5 and 8.6 and IBM Business Automation Workflow 18.0, 19.0, 20.0 and 21.0 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209512.	5.4	More Details
CVE-2021-41871	An issue was discovered in Socomec REMOTE VIEW PRO 2.0.41.4. Improper validation of input into the username field makes it possible to place a stored XSS payload. This is executed if an administrator views the System Event Log.	5.4	More Details
CVE-2020-19770	A cross-site scripting (XSS) vulnerability in the system bulletin component of WUZHI CMS v4.1.0 allows attackers to steal the admin's cookie.	5.4	More Details
CVE-2021-44317	In Bus Pass Management System v1.0, parameters 'pagedes' and `About Us` are affected with a Stored Cross-site scripting vulnerability.	5.4	More Details
CVE-2021-41557	Sofico Miles RIA 2020.2 Build 127964T is affected by Stored Cross Site Scripting (XSS). An attacker with access to a user account of the RIA IT or the Fleet role can create a crafted work order in the damage reports section (or change existing work orders). The XSS payload is in the work order number.	5.4	More Details
CVE-2021-43438	Stored XSS in Signup Form in iResturant 1.0 Allows Remote Attacker to Inject Arbitrary code via NAME and ADDRESS field	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42220	A Cross Site Scripting (XSS) vulnerability exists in Dolibarr before 14.0.3 via the ticket creation flow. Exploitation requires that an admin copies the payload into a box.	5.4	More Details
CVE-2021-4116	yetiforcecrm is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-35490	Thruk before 2.44 allows XSS for a quick command.	5.4	More Details
CVE-2021-44263	Gurock TestRail before 7.2.4 mishandles HTML escaping.	5.4	More Details
CVE-2021-44876	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to User enumeration. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. This issue occurs during the identification of the correct tenant for a given user, where a difference in messages could allow an attacker to determine if the given user is valid or not, enabling a brute force attack with valid users.	5.3	More Details
CVE-2021-44875	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to User enumeration. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. This issue occurs during the password recovery procedure for a given user, where a difference in messages could allow an attacker to determine if the given user is valid or not, enabling a brute force attack with valid users.	5.3	More Details
CVE-2021-43843	jsx-slack is a package for building JSON objects for Slack block kit surfaces from JSX. The maintainers found the patch for CVE-2021-43838 in jsx-slack v4.5.1 is insufficient tfor protection from a Regular Expression Denial of Service (ReDoS) attack. If an attacker can put a lot of JSX elements into `<blockquote>` tag _with including multibyte characters_, an internal regular expression for escaping characters may consume an excessive amount of computing resources. v4.5.1 passes the test against ASCII characters but misses the case of multibyte characters. jsx-slack v4.5.2 has updated regular expressions for escaping blockquote characters to prevent catastrophic backtracking. It is also including an updated test case to confirm rendering multiple tags in `<blockquote>` with multibyte characters.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43838	jsx-slack is a library for building JSON objects for Slack Block Kit surfaces from JSX. In versions prior to 4.5.1 users are vulnerable to a regular expression denial-of-service (ReDoS) attack. If attacker can put a lot of JSX elements into `<blockquote>` tag, an internal regular expression for escaping characters may consume an excessive amount of computing resources. jsx-slack v4.5.1 has patched to a regex for escaping blockquote characters. Users are advised to upgrade as soon as possible.	5.3	More Details
CVE-2021-44554	Thinfinity VirtualUI before 3.0 allows a malicious actor to enumerate users registered in the OS (Windows) through the /changePassword URI. By accessing the vector, an attacker can determine if a username exists thanks to the message returned; it can be presented in different languages according to the configuration of VirtualUI. Common users are administrator, admin, guest and krgtbt.	5.3	More Details
CVE-2021-40171	The absence of notifications regarding an ongoing RF jamming attack in the SecuritasHome home alarm system, version HPGW-G 0.0.2.23F BG_U-ITR-F1-BD_BL.A30.20181117, allows an attacker to block legitimate traffic while not alerting the owner of the system.	5.3	More Details
CVE-2021-45038	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. By using an action=rollback query, attackers can view private wiki contents.	5.3	More Details
CVE-2021-43846	`solidus_frontend` is the cart and storefront for the Solidus e-commerce project. Versions of `solidus_frontend` prior to 3.1.5, 3.0.5, and 2.11.14 contain a cross-site request forgery (CSRF) vulnerability that allows a malicious site to add an item to the user's cart without their knowledge. Versions 3.1.5, 3.0.5, and 2.11.14 contain a patch for this issue. The patch adds CSRF token verification to the "Add to cart" action. Adding forgery protection to a form that missed it can have some side effects. Other CSRF protection strategies as well as a workaround involving modifcation to config/application.rb` are available. More details on these mitigations are available in the GitHub Security Advisory.	5.3	More Details
CVE-2021-33430	A Buffer Overflow vulnerability exists in NumPy 1.9.x in the PyArray_NewFromDescr_int function of ctors.c when specifying arrays of large dimensions (over 32) from Python code, which could let a malicious user cause a Denial of Service. NOTE: The vendor does not agree this is a vulneraility; In (very limited) circumstances a user may be able provoke the buffer overflow, the user is most likely already privileged to at least provoke denial of service by exhausting memory. Triggering this further requires the use of uncommon API (complicated structured dtypes), which is very unlikely to be available to an unprivileged user	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34141	An incomplete string comparison in the numpy.core component in NumPy before 1.22.0 allows attackers to trigger slightly incorrect copying by constructing specific string objects. NOTE: the vendor states that this reported code behavior is "completely harmless."	5.3	More Details
CVE-2021-41495	Null Pointer Dereference vulnerability exists in numpy.sort in NumPy &lt and 1.19 in the PyArray_DescrNew function due to missing return-value validation, which allows attackers to conduct DoS attacks by repetitively creating sort arrays. NOTE: While correct that validation is missing, an error can only occur due to an exhaustion of memory. If the user can exhaust memory, they are already privileged. Further, it should be practically impossible to construct an attack which can target the memory exhaustion to occur at exactly this place	5.3	More Details
CVE-2021-43441	An HTML Injection Vulnerability in iOrder 1.0 allows the remote attacker to execute Malicious HTML codes via the signup form	5.3	More Details
CVE-2021-27858	A missing authorization vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p91 and 10.2.2r42 allows a remote attacker to access at least the URL "/fpui/jsp/index.jsp" leading to unknown impact, presumably some violation of confidentiality. Older versions of FatPipe software may also be vulnerable. The FatPipe advisory identifier for this vulnerability is FPSA004.	5.3	More Details
CVE-2021-45089	Stormshield Endpoint Security 2.x before 2.1.2 has Incorrect Access Control.	5.2	More Details
CVE-2021-1023	In onCreate of RequestIgnoreBatteryOptimizations.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-195963373	5.0	More Details
CVE-2021-0973	In isFileUri of UriUtil.java, there is a possible way to bypass ignoring file://URI attachment due to improper handling of case sensitivity. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-197328178	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0952	In doCropPhoto of PhotoSelectionHandler.java, there is a possible permission bypass due to a confused deputy. This could lead to local information disclosure of user's contacts with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-195748381	5.0	More Details
CVE-2021-0919	In getService of IServiceManager.cpp, there is a possible unhandled exception due to an integer overflow. This could lead to local denial of service making the lockscreen unusable with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-197336441	5.0	More Details
CVE-2021-45042	In HashiCorp Vault and Vault Enterprise before 1.7.7, 1.8.x before 1.8.6, and 1.9.x before 1.9.1, clusters using the Integrated Storage backend allowed an authenticated user (with write permissions to a kv secrets engine) to cause a panic and denial of service of the storage backend. The earliest affected version is 1.4.0.	4.9	More Details
CVE-2021-38701	Certain Motorola Solutions Avigilon devices allow XSS in the administrative UI. This affects T200/201 before 4.10.0.68; T290 before 4.4.0.80; T008 before 2.2.0.86; T205 before 4.12.0.62; T204 before 3.28.0.166; and T100, T101, T102, and T103 before 2.6.0.180.	4.8	More Details
CVE-2021-41962	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Vehicle Service Management System 1.0 via the Owner fullname parameter in a Send Service Request in vehicle_service.	4.8	More Details
CVE-2021-45096	KNIME Analytics Platform before 4.5.0 is vulnerable to XXE (external XML entity injection) via a crafted workflow file (.knwf), aka AP-17730.	4.7	More Details
CVE-2021-40835	An URL Address bar spoofing vulnerability was discovered in Safe Browser for iOS. When user clicks on a specially crafted a malicious URL, if user does not carefully pay attention to url, user may be tricked to think content may be coming from a valid domain, while it comes from another. This is performed by using a very long username part of the url so that user cannot see the domain name. A remote attacker can leverage this to perform url address bar spoofing attack. The fix is, browser no longer shows the user name part in address bar.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0996	In nfaHciCallback of HciEventManager.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure over NFC with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-181346545	4.5	More Details
CVE-2021-0958	In update of km_compat.cpp, there is a possible loss of potentially sensitive data due to a logic error in the code. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-200041882	4.4	More Details
CVE-2021-0961	In quota_proc_write of xt_quota2.c, there is a possible way to read kernel memory 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-196046570References: Upstream kernel	4.4	More Details
CVE-2021-43840	message_bus is a messaging bus for Ruby processes and web clients. In versions prior to 3.3.7 users who deployed message bus with diagnostics features enabled (default off) are vulnerable to a path traversal bug, which could lead to disclosure of secret information on a machine if an unintended user were to gain access to the diagnostic route. The impact is also greater if there is no proxy for your web application as the number of steps up the directories is not bounded. For deployments which uses a proxy, the impact varies. For example, If a request goes through a proxy like Nginx with `merge_slashes` enabled, the number of steps up the directories that can be read is limited to 3 levels. This issue has been patched in version 3.3.7. Users unable to upgrade should ensure that MessageBus::Diagnostics is disabled.	4.4	More Details
CVE-2021-1047	In valid_ipc_dram_addr of cm_access_control.c, there is a possible out of bounds read due to an integer overflow. 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-197966306References: N/A	4.4	More Details
CVE-2021-39636	In do_ipt_get_ctl and do_ipt_set_ctl of ip_tables.c, there is a possible way to leak kernel information 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-120612905References: Upstream kernel	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0676	In geniezone driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863009; Issue ID: ALPS05863009.	4.4	More Details
CVE-2021-44035	Wolters Kluwer TeamMate AM 12.4 Update 1 mishandles attachment uploads, such that an authenticated user may download and execute malicious files.	4.4	More Details
CVE-2021-39657	In ufshcd_eh_device_reset_handler of ufshcd.c, there is a possible out of bounds read due to a missing bounds check. 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-194696049References: Upstream kernel	4.4	More Details
CVE-2021-0902	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05656484.	4.4	More Details
CVE-2021-1006	In several functions of DatabaseManager.java, there is a possible leak of Bluetooth MAC addresses due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-183961974	4.4	More Details
CVE-2021-39647	In mon_smc_load_sp of gs101-sc/plat/samsung/exynos/soc/exynos9845/smc_booting.S, there is a possible reinitialization of TEE due to improper locking. 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-198713939References: N/A	4.4	More Details
CVE-2021-39637	In CreateDeviceInfo of trusty_remote_provisioning_context.cpp, there is a possible out of bounds read due to a missing bounds check. 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-193579873References: N/A	4.4	More Details
CVE-2021-0900	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672055.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0677	In ccu driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827154; Issue ID: ALPS05827154.	4.4	More Details
CVE-2021-1046	In lwis_dpm_update_clock of lwis_device_dpm.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-195609074References: N/A	4.4	More Details
CVE-2021-1042	In dsi_panel_debugfs_read_cmdset of dsi_panel.c, there is a possible disclosure of freed kernel heap memory due to a use after free. 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-187851056References: N/A	4.4	More Details
CVE-2021-1008	In addSubInfo of SubscriptionController.java, there is a possible way to force the user to make a factory reset due to a logic error in the code. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-197327688	4.4	More Details
CVE-2021-1007	In btu_hcif_process_event of btu_hcif.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-167759047	4.4	More Details
CVE-2021-4117	yetiforcecrm is vulnerable to Business Logic Errors	4.3	More Details
CVE-2021-43908	Visual Studio Code Spoofing Vulnerability	4.3	More Details
CVE-2021-45091	Stormshield Endpoint Security from 2.1.0 to 2.1.1 has Incorrect Access Control.	4.3	More Details
CVE-2021-4111	yetiforcecrm is vulnerable to Business Logic Errors	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39648	In gadget_dev_desc_UDC_show of configfs.c, there is a possible disclosure of kernel heap memory due to a race condition. 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-160822094References: Upstream kernel	4.1	More Details
CVE-2021-37862	Mattermost 6.0 and earlier fails to sufficiently validate the email address during registration, which allows attackers to trick users into signing up using attacker-controlled email addresses via crafted invitation token.	3.7	More Details
CVE-2021-37863	Mattermost 6.0 and earlier fails to sufficiently validate parameters during post creation, which allows authenticated attackers to cause a client-side crash of the web application via a maliciously crafted post.	3.5	More Details
CVE-2021-36889	Multiple Stored Authenticated Cross-Site Scripting (XSS) vulnerabilities were discovered in tarteaucitron.js – Cookies legislation & GDPR WordPress plugin (versions <= 1.6).	3.4	More Details
CVE-2021-0995	In registerSuggestionConnectionStatusListener of WifiServiceImpl.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-197536547	3.3	More Details
CVE-2021-0992	In onCreate of PaymentDefaultDialog.java, there is a possible way to change a default payment app without user consent due to tapjack overlay. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-180104327	3.3	More Details
CVE-2021-0989	In hasManageOngoingCallsPermission of TelecomServiceImpl.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-194105812	3.3	More Details
CVE-2021-0990	In getDeviceId of PhoneSubInfoController.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-185591180	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0994	In requestRouteToHostAddress of ConnectivityService.java, there is a possible way to determine whether an app is installed, without query permissions, due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-193801134	3.3	More Details
CVE-2021-0988	In getLaunchedFromUid and getLaunchedFromPackage of ActivityClientController.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-191954233	3.3	More Details
CVE-2021-44697	Adobe Audition versions 14.4 (and earlier), and 22.0 (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 MOV file.	3.3	More Details
CVE-2021-1034	In getLine1NumberForDisplay of PhoneInterfaceManager.java, there is apossible way to determine whether an app is installed, without querypermissions due to a missing permission check. This could lead to localinformation disclosure with no additional execution privileges needed. Userinteraction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-193441322	3.3	More Details
CVE-2021-1032	In getMimeGroup of PackageManagerService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-184745603	3.3	More Details
CVE-2021-1031	In cancelNotificationsFromListener of NotificationManagerService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-194697004	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1018	In adjustStreamVolume of AudioService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-194110891	3.3	More Details
CVE-2021-1015	In getMeidForSlot of PhoneInterfaceManager.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-186530496	3.3	More Details
CVE-2021-44182	Adobe Dimension versions 3.4.3 (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 SVG file.	3.3	More Details
CVE-2021-44183	Adobe Dimension versions 3.4.3 (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-2021-43030	Adobe Premiere Rush versions 1.5.16 (and earlier) allows access to an uninitialized pointer vulnerability that allows remote attackers to disclose arbitrary data on affected installations. 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 MP4 files. The issue results from the lack of proper initialization of memory prior to accessing it.	3.3	More Details
CVE-2021-44698	Adobe Audition versions 14.4 (and earlier), and 22.0 (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 MP4 file.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0978	In getSerialForPackage of DeviceIdentifiersPolicyService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-192587406	3.3	More Details
CVE-2021-0982	In getOrganizationNameForUser of DevicePolicyManagerService.java, there is a possible organization name disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-192368508	3.3	More Details
CVE-2021-0983	In createAdminSupportIntent of DevicePolicyManagerService.java, there is a possible disclosure of information about installed device/profile owner package name due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-192245204	3.3	More Details
CVE-2021-0987	In getNeighboringCellInfo of PhoneInterfaceManager.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-190619791	3.3	More Details
CVE-2021-44699	Adobe Audition versions 14.4 (and earlier), and 22.0 (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 MP4 file.	3.3	More Details
CVE-2021-45097	KNIME Server before 4.12.6 and 4.13.x before 4.13.4 (when installed in unattended mode) keeps the administrator's password in a file without appropriate file access controls, allowing all local users to read its content.	2.9	More Details
CVE-2021-0991	In OnMetadataChangedListener of AdvancedBluetoothDetailsHeaderController.java, there is a possible leak of Bluetooth MAC addresses due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-181588752	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16713	Rejected reason: 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-2020-16711	Rejected reason: 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-2020-16712	Rejected reason: 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-2020-16715	Rejected reason: 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-2020-16714	Rejected reason: 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-2020-16716	Rejected reason: 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-2020-16717	Rejected reason: 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-2020-16709	Rejected reason: 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-2020-16718	Rejected reason: 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-2020-16710	Rejected reason: 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-2020-16702	Rejected reason: 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-2020-16708	Rejected reason: 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-2020-16707	Rejected reason: 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-2020-16706	Rejected reason: 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-2020-16705	Rejected reason: 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-2020-16704	Rejected reason: 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-2020-16703	Rejected reason: 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-2020-16720	Rejected reason: 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-2020-16701	Rejected reason: 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-2020-16700	Rejected reason: 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-2020-16699	Rejected reason: 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-2020-16698	Rejected reason: 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-2020-16719	Rejected reason: 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-2020-16728	Rejected reason: 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-2020-16721	Rejected reason: 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-2020-16734	Rejected reason: 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-2020-16744	Rejected reason: 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-2020-16743	Rejected reason: 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-2020-16742	Rejected reason: 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-2020-16741	Rejected reason: 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-2020-16740	Rejected reason: 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-2020-16739	Rejected reason: 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-2020-16738	Rejected reason: 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-2020-16737	Rejected reason: 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-2020-16736	Rejected reason: 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-2020-16735	Rejected reason: 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-2020-16733	Rejected reason: 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-2020-16722	Rejected reason: 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-2020-16732	Rejected reason: 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-2020-16731	Rejected reason: 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-2020-16730	Rejected reason: 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-2020-16729	Rejected reason: 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-2020-16696	Rejected reason: 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-2020-16727	Rejected reason: 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-2020-16726	Rejected reason: 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-2020-16725	Rejected reason: 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-2020-16724	Rejected reason: 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-2020-16723	Rejected reason: 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-2020-16697	Rejected reason: 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-2020-16687	Rejected reason: 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-2020-16695	Rejected reason: 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-2020-16669	Rejected reason: 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-2020-16667	Rejected reason: 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-2020-16666	Rejected reason: 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-2020-16665	Rejected reason: 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-2020-16664	Rejected reason: 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-2020-16663	Rejected reason: 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-2020-16662	Rejected reason: 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-2020-16661	Rejected reason: 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-2020-16660	Rejected reason: 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-2020-16659	Rejected reason: 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-2020-16658	Rejected reason: 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-2020-16657	Rejected reason: 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-2020-16656	Rejected reason: 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-2020-16655	Rejected reason: 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-2020-16654	Rejected reason: 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-2020-16653	Rejected reason: 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-2020-16652	Rejected reason: 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-2020-16651	Rejected reason: 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-2020-16650	Rejected reason: 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-2020-16649	Rejected reason: 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-2020-16648	Rejected reason: 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-2020-16746	Rejected reason: 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-2020-16668	Rejected reason: 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-2020-16670	Rejected reason: 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-2020-16694	Rejected reason: 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-2020-16671	Rejected reason: 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-2020-16693	Rejected reason: 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-2020-16692	Rejected reason: 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-2020-16691	Rejected reason: 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-2020-16690	Rejected reason: 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-2020-16689	Rejected reason: 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-2020-16688	Rejected reason: 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-2020-16686	Rejected reason: 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-2020-16685	Rejected reason: 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-2020-16684	Rejected reason: 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-2020-16683	Rejected reason: 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-2020-16682	Rejected reason: 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-2020-16681	Rejected reason: 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-2020-16680	Rejected reason: 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-2020-16679	Rejected reason: 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-2020-16678	Rejected reason: 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-2020-16677	Rejected reason: 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-2020-16676	Rejected reason: 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-2020-16675	Rejected reason: 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-2020-16674	Rejected reason: 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-2020-16673	Rejected reason: 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-2020-16672	Rejected reason: 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-2020-16745	Rejected reason: 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-2020-16808	Rejected reason: 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-2020-16747	Rejected reason: 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-2020-16811	Rejected reason: 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-2020-16821	Rejected reason: 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-2020-16820	Rejected reason: 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-2020-16819	Rejected reason: 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-2020-16818	Rejected reason: 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-2020-16817	Rejected reason: 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-2020-16816	Rejected reason: 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-2020-16815	Rejected reason: 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-2020-16814	Rejected reason: 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-2020-16813	Rejected reason: 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-2020-16812	Rejected reason: 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-2020-16810	Rejected reason: 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-2020-16798	Rejected reason: 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-2020-16809	Rejected reason: 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-2020-16646	Rejected reason: 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-2020-16807	Rejected reason: 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-2020-16806	Rejected reason: 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-2020-16805	Rejected reason: 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-2020-16804	Rejected reason: 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-2020-16803	Rejected reason: 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-2020-16802	Rejected reason: 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-2020-16801	Rejected reason: 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-2020-16800	Rejected reason: 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-2020-16822	Rejected reason: 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-2020-16823	Rejected reason: 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-2020-16824	Rejected reason: 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-2020-16825	Rejected reason: 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-2020-3709	Rejected reason: 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-2020-3708	Rejected reason: 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-2020-3707	Rejected reason: 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-2020-3706	Rejected reason: 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-2020-3705	Rejected reason: 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-2020-3697	Rejected reason: 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-2020-3695	Rejected reason: 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-2020-3682	Rejected reason: 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-2020-3631	Rejected reason: 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-2020-3627	Rejected reason: 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-2020-16836	Rejected reason: 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-2020-16835	Rejected reason: 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-2020-16834	Rejected reason: 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-2020-16833	Rejected reason: 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-2020-16832	Rejected reason: 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-2020-16831	Rejected reason: 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-2020-16830	Rejected reason: 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-2020-16829	Rejected reason: 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-2020-16828	Rejected reason: 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-2020-16827	Rejected reason: 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-2020-16826	Rejected reason: 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-2020-16799	Rejected reason: 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-2020-16797	Rejected reason: 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-2020-16748	Rejected reason: 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-2020-16760	Rejected reason: 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-2020-16770	Rejected reason: 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-2020-16769	Rejected reason: 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-2020-16768	Rejected reason: 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-2020-16767	Rejected reason: 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-2020-16766	Rejected reason: 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-2020-16765	Rejected reason: 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-2020-16764	Rejected reason: 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-2020-16763	Rejected reason: 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-2020-16762	Rejected reason: 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-2020-16761	Rejected reason: 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-2020-16759	Rejected reason: 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-2020-16796	Rejected reason: 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-2020-16758	Rejected reason: 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-2020-16757	Rejected reason: 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-2020-16756	Rejected reason: 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-2020-16755	Rejected reason: 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-2020-16754	Rejected reason: 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-2020-16753	Rejected reason: 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-2020-16752	Rejected reason: 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-2020-16751	Rejected reason: 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-2020-16750	Rejected reason: 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-2020-16749	Rejected reason: 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-2020-16771	Rejected reason: 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-2020-16772	Rejected reason: 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-2020-16773	Rejected reason: 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-2020-16774	Rejected reason: 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-2020-16795	Rejected reason: 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-2020-16794	Rejected reason: 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-2020-16793	Rejected reason: 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-2020-16792	Rejected reason: 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-2020-16791	Rejected reason: 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-2020-16790	Rejected reason: 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-2020-16789	Rejected reason: 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-2020-16788	Rejected reason: 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-2020-16787	Rejected reason: 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-2020-16786	Rejected reason: 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-2020-16785	Rejected reason: 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-2020-16784	Rejected reason: 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-2020-16783	Rejected reason: 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-2020-16782	Rejected reason: 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-2020-16781	Rejected reason: 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-2020-16780	Rejected reason: 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-2020-16779	Rejected reason: 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-2020-16778	Rejected reason: 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-2020-16777	Rejected reason: 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-2020-16776	Rejected reason: 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-2020-16775	Rejected reason: 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-2020-16647	Rejected reason: 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-2020-11389	Rejected reason: 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-2020-16645	Rejected reason: 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-2019-2368	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14185	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14184	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14183	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14182	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14181	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14180	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14179	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14178	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14177	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14176	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14175	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14174	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14173	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14172	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14171	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14170	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14169	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14168	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14167	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14166	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14165	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14164	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14163	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14162	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14161	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14160	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14158	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14157	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14186	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14187	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14188	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2353	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2366	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2365	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2364	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2363	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2362	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2361	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2360	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2359	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-2358	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2357	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2356	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2355	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2354	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2352	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14189	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2351	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2350	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2349	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2348	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-2347	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2344	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2342	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2340	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2286	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2282	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2280	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14191	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14190	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14154	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14153	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13973	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2019-13993	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-10619	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-10613	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-10599	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-10573	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-10568	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-10560	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2018-13979	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13978	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13977	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13976	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-13975	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13974	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13972	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2019-13997	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2018-13971	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-13970	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11954	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-11837	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2017-11071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-11020	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2021-44181	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious GIF file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44180	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious GIF file.	N/A	More Details
CVE-2021-44179	Adobe Dimension versions 3.4.3 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious GIF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-43763	Adobe Dimension versions 3.4.3 (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.	N/A	More Details
CVE-2021-43023	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious EPS/TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-40784	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-40783	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2019-13996	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14152	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14150	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14147	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14146	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14143	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14140	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14139	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14136	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14133	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14126	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14109	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14107	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14106	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14102	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14096	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2367	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2369	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2020-16644	Rejected reason: 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-2019-2370	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2020-11387	Rejected reason: 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-2020-11386	Rejected reason: 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-2020-11385	Rejected reason: 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-2020-11384	Rejected reason: 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-2020-11383	Rejected reason: 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-2020-11382	Rejected reason: 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-2020-11381	Rejected reason: 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-2020-11380	Rejected reason: 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-2020-11379	Rejected reason: 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-2020-11378	Rejected reason: 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-2020-11377	Rejected reason: 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-2020-11376	Rejected reason: 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-2020-11375	Rejected reason: 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-2020-11374	Rejected reason: 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-2020-11373	Rejected reason: 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-2020-11372	Rejected reason: 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-2020-11371	Rejected reason: 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-2020-11370	Rejected reason: 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-2020-11369	Rejected reason: 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-2020-11368	Rejected reason: 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-2020-11367	Rejected reason: 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-2020-11366	Rejected reason: 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-2020-11365	Rejected reason: 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-2020-11364	Rejected reason: 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-2020-11363	Rejected reason: 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-2020-11362	Rejected reason: 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-2020-11361	Rejected reason: 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-2020-11360	Rejected reason: 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-2020-11359	Rejected reason: 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-2020-11388	Rejected reason: 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-2020-11390	Rejected reason: 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-2020-11391	Rejected reason: 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-2020-11407	Rejected reason: 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-2020-16643	Rejected reason: 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-2020-16642	Rejected reason: 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-2020-16641	Rejected reason: 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-2020-16640	Rejected reason: 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-2020-16639	Rejected reason: 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-2020-16638	Rejected reason: 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-2020-16637	Rejected reason: 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-2020-11413	Rejected reason: 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-2020-11412	Rejected reason: 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-2020-11411	Rejected reason: 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-2020-11410	Rejected reason: 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-2020-11409	Rejected reason: 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-2020-11408	Rejected reason: 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-2020-11406	Rejected reason: 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-2020-11392	Rejected reason: 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-2020-11405	Rejected reason: 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-2020-11404	Rejected reason: 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-2020-11403	Rejected reason: 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-2020-11402	Rejected reason: 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-2020-11401	Rejected reason: 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-2020-11400	Rejected reason: 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-2020-11399	Rejected reason: 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-2020-11398	Rejected reason: 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-2020-11397	Rejected reason: 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-2020-11396	Rejected reason: 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-2020-11395	Rejected reason: 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-2020-11394	Rejected reason: 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-2020-11393	Rejected reason: 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-2020-11358	Rejected reason: 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-2020-11357	Rejected reason: 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-2020-11356	Rejected reason: 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-2020-11300	Rejected reason: 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-2020-11322	Rejected reason: 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-2020-11321	Rejected reason: 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-2020-11320	Rejected reason: 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-2020-11319	Rejected reason: 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-2020-11318	Rejected reason: 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-2020-11317	Rejected reason: 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-2020-11316	Rejected reason: 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-2020-11315	Rejected reason: 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-2020-11314	Rejected reason: 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-2020-11313	Rejected reason: 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-2020-11312	Rejected reason: 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-2020-11310	Rejected reason: 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-2020-11302	Rejected reason: 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-2019-2384	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2020-11324	Rejected reason: 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-2019-2383	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2382	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2381	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2380	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-2379	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2378	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2377	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2376	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2375	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2374	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2373	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2372	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-2371	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2020-11323	Rejected reason: 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-2020-11325	Rejected reason: 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-2020-11355	Rejected reason: 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-2020-11341	Rejected reason: 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-2020-11354	Rejected reason: 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-2020-11353	Rejected reason: 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-2020-11352	Rejected reason: 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-2020-11351	Rejected reason: 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-2020-11350	Rejected reason: 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-2020-11349	Rejected reason: 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-2020-11348	Rejected reason: 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-2020-11347	Rejected reason: 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-2020-11346	Rejected reason: 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-2020-11345	Rejected reason: 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-2020-11344	Rejected reason: 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-2020-11343	Rejected reason: 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-2020-11342	Rejected reason: 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-2020-11340	Rejected reason: 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-2020-11326	Rejected reason: 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-2020-11339	Rejected reason: 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-2020-11338	Rejected reason: 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-2020-11337	Rejected reason: 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-2020-11336	Rejected reason: 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-2020-11335	Rejected reason: 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-2020-11334	Rejected reason: 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-2020-11333	Rejected reason: 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-2020-11332	Rejected reason: 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-2020-11331	Rejected reason: 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-2020-11330	Rejected reason: 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-2020-11329	Rejected reason: 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-2020-11328	Rejected reason: 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-2020-11327	Rejected reason: 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-2019-14155	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details