SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 June 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-2021-34679	Thycotic Password Reset Server before 5.3.0 allows credential disclosure.	10.0	More Details
CVE-2021-33841	SGE-PLC1000 device, in its 0.9.2b firmware version, does not handle some requests correctly, allowing a remote attacker to inject code into the operating system with maximum privileges.	10.0	More Details
CVE-2021-23230	A SQL Injection vulnerability in the OPCUA interface of Gallagher Command Centre allows a remote unprivileged Command Centre Operator to modify Command Centre databases undetected. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1359 (MR3); 8.20 versions prior to 8.20.1259 (MR5); 8.10 versions prior to 8.10.1284 (MR7); version 8.00 and prior versions.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23140	Improper Authorization vulnerability in Gallagher Command Centre Server allows command line macros to be modified by an unauthorised Command Centre Operator. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1359 (MR3); 8.20 versions prior to 8.20.1259 (MR5); version 8.10 and prior versions.	9.9	More Details
CVE-2021-24037	A use after free in hermes, while emitting certain error messages, prior to commit d86e185e485b6330216dee8e854455c694e3a36e allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2021-22765	A CWE-20: Improper Input Validation vulnerability exists in PowerLogic EGX100 (Versions 3.0.0 and newer) and PowerLogic EGX300 (All Versions) that could cause denial of service or remote code execution via a specially crafted HTTP packet	9.8	More Details
CVE-2021-0324	Product: AndroidVersions: Android SoCAndroid ID: A-175402462	9.8	More Details
CVE-2021-32682	elFinder is an open-source file manager for web, written in JavaScript using jQuery UI. Several vulnerabilities affect elFinder 2.1.58. These vulnerabilities can allow an attacker to execute arbitrary code and commands on the server hosting the elFinder PHP connector, even with minimal configuration. The issues were patched in version 2.1.59. As a workaround, ensure the connector is not exposed without authentication.	9.8	More Details
CVE-2020-11134	Possible stack out of bound write might happen due to time bitmap length and bit duration fields of the attributes like NAN ranging setup attribute inside a NAN management frame are not Properly validated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-27200	In WoWonder 3.0.4, remote attackers can take over any account due to the weak cryptographic algorithm in recover.php. The code parameter is easily predicted from the time of day.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22763	A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists in PowerLogic PM55xx, PowerLogic PM8ECC, PowerLogic EGX100 and PowerLogic EGX300 (see security notification for version infromation) that could allow an attacker administrator level access to a device.	9.8	More Details
CVE-2021-22768	A CWE-20: Improper Input Validation vulnerability exists in PowerLogic EGX100 (Versions 3.0.0 and newer) and PowerLogic EGX300 (All Versions) that could cause denial of service or remote code execution via a specially crafted HTTP packet.This CVE ID is unique from CVE-2021-22767	9.8	More Details
CVE-2021-22767	A CWE-20: Improper Input Validation vulnerability exists in PowerLogic EGX100 (Versions 3.0.0 and newer) and PowerLogic EGX300 (All Versions) that could cause denial of service or remote code execution via a specially crafted HTTP packet.This CVE ID is unique from CVE-2021-2276	9.8	More Details
CVE-2021-3013	ripgrep before 13 on Windows allows attackers to trigger execution of arbitrary programs from the current working directory via the -z/--search-zip or --pre flag.	9.8	More Details
CVE-2021-22915	Nextcloud server before 19.0.11, 20.0.10, 21.0.2 is vulnerable to brute force attacks due to lack of inclusion of IPv6 subnets in rate-limiting considerations. This could potentially result in an attacker bypassing rate-limit controls such as the Nextcloud brute-force protection.	9.8	More Details
CVE-2021-0474	In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-177611958	9.8	More Details
CVE-2021-21795	A heap-based buffer overflow vulnerability exists in the PSD read_icc_icCurve_data functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to an integer overflow that, in turn, leads to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-21824	An out-of-bounds write vulnerability exists in the JPG Handle_JPEG420 functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21833	An improper array index validation vulnerability exists in the TIF IP_planar_raster_unpack functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2020-29214	SQL injection vulnerability in SourceCodester Alumni Management System 1.0 allows the user to inject SQL payload to bypass the authentication via admin/login.php.	9.8	More Details
CVE-2021-27388	SINAMICS medium voltage routable products are affected by a vulnerability in the Sm@rtServer component for remote access that could allow an unauthenticated attacker to cause a denial-of-service condition, and/or execution of limited configuration modifications and/or execution of limited control commands on the SINAMICS Medium Voltage Products, Remote Access (SINAMICS SL150: All versions, SINAMICS SM150: All versions, SINAMICS SM150i: All versions).	9.8	More Details
CVE-2021-32930	The affected product's configuration is vulnerable due to missing authentication, which may allow an attacker to change configurations and execute arbitrary code on the iView (versions prior to v5.7.03.6182).	9.8	More Details
CVE-2021-33833	ConnMan (aka Connection Manager) 1.30 through 1.39 has a stack-based buffer overflow in uncompress in dnsproxy.c via NAME, RDATA, or RDLENGTH (for A or AAAA).	9.8	More Details
CVE-2021-34170	Bandai Namco FromSoftware Dark Souls III allows remote attackers to execute arbitrary code.	9.8	More Details
CVE-2020-11182	Possible heap overflow while parsing NAL header due to lack of check of length of data received from user in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	9.8	More Details
CVE-2020-11176	While processing server certificate from IPSec server, certificate validation for subject alternative name API can cause heap overflow which can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile	9.8	More Details
CVE-2020-11291	Possible buffer overflow while updating ikev2 parameters for delete payloads received during informational exchange due to lack of check of input validation for certain parameters received from the ePDG server in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23847	A Missing Authentication in Critical Function in Bosch IP cameras allows an unauthenticated remote attacker to extract sensitive information or change settings of the camera by sending crafted requests to the device. Only devices of the CPP6, CPP7 and CPP7.3 family with firmware 7.70, 7.72, and 7.80 prior to B128 are affected by this vulnerability. Versions 7.62 or lower and INTEOX cameras are not affected.	9.8	More Details
CVE-2020-15377	Webtools in Brocade SANnav before version 2.1.1 allows unauthenticated users to make requests to arbitrary hosts due to a misconfiguration; this is commonly referred to as Server-Side Request Forgery (SSRF).	9.8	More Details
CVE-2021-33357	A vulnerability exists in RaspAP 2.6 to 2.6.5 in the "iface" GET parameter in /ajax/networking/get_netcfg.php, when the "iface" parameter value contains special characters such as ";" which enables an unauthenticated attacker to execute arbitrary OS commands.	9.8	More Details
CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow	9.8	More Details
CVE-2020-23323	There is a heap-buffer-overflow at re-parser.c in re_parse_char_escape in JerryScript 2.2.0.	9.8	More Details
CVE-2021-33622	Sylabs Singularity 3.5.x and 3.6.x, and SingularityPRO before 3.5-8, has an Incorrect Check of a Function's Return Value.	9.8	More Details
CVE-2021-25948	Prototype pollution vulnerability in 'expand-hash' versions 0.1.0 through 1.0.1 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-25949	Prototype pollution vulnerability in 'set-getter' version 0.1.0 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-23302	There is a heap-use-after-free at ecma-helpers-string.c:772 in ecma_ref_ecma_string in JerryScript 2.2.0	9.8	More Details
CVE-2020-23303	There is a heap-buffer-overflow at jmem-poolman.c:165 in jmem_pools_collect_empty in JerryScript 2.2.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23306	There is a stack-overflow at ecma-regexp-object.c:535 in ecma_regexp_match in JerryScript 2.2.0.	9.8	More Details
CVE-2020-23321	There is a heap-buffer-overflow at lit-strings.c:431 in lit_read_code_unit_from_utf8 in JerryScript 2.2.0.	9.8	More Details
CVE-2021-27410	The affected product is vulnerable to an out-of-bounds write, which may result in corruption of data or code execution on the Welch Allyn medical device management tools (Welch Allyn Service Tool: versions prior to v1.10, Welch Allyn Connex Device Integration Suite – Network Connectivity Engine (NCE): versions prior to v5.3, Welch Allyn Software Development Kit (SDK): versions prior to v3.2, Welch Allyn Connex Central Station (CS): versions prior to v1.8.6, Welch Allyn Service Monitor: versions prior to v1.7.0.0, Welch Allyn Connex Vital Signs Monitor (CVSM): versions prior to v2.43.02, Welch Allyn Connex Integrated Wall System (CIWS): versions prior to v2.43.02, Welch Allyn Connex Spot Monitor (CSM): versions prior to v1.52, Welch Allyn Spot Vital Signs 4400 Device (Spot 4400) / Welch Allyn Spot 4400 Vital Signs Extended Care Device: versions prior to v1.11.00).	9.8	More Details
CVE-2020-11126	Possible out of bound read while WLAN frame parsing due to lack of check for body and header length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2020-5003	IBM Financial Transaction Manager 3.2.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 192956.	9.1	More Details
CVE-2021-24035	A lack of filename validation when unzipping archives prior to WhatsApp for Android v2.21.8.13 and WhatsApp Business for Android v2.21.8.13 could have allowed path traversal attacks that overwrite WhatsApp files.	9.1	More Details
CVE-2021-34363	The thefuck (aka The Fuck) package before 3.31 for Python allows Path Traversal that leads to arbitrary file deletion via the "undo archive operation" feature.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11159	Buffer over-read can happen while processing WPA,RSN IE of beacon and response frames if IE length is less than length of frame pointer being accessed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2021-25387	An improper input validation vulnerability in sflacfd_get_frm() in libsflacextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.	9.0	More Details
CVE-2021-25386	An improper input validation vulnerability in sdfffd_parse_chunk_FVER() in libsdffextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.	9.0	More Details
CVE-2021-25384	An improper input validation vulnerability in sdfffd_parse_chunk_PROP() with Sample Rate Chunk in libsdffextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.	9.0	More Details
CVE-2021-25383	An improper input validation vulnerability in scmn_mfal_read() in libsapeextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.	9.0	More Details
CVE-2021-25385	An improper input validation vulnerability in sdfffd_parse_chunk_PROP() in libsdffextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-30553	Use after free in Network service in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-24489	Incomplete cleanup in some Intel(R) VT-d products may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2021-30547	Out of bounds write in ANGLE in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31837	Memory corruption vulnerability in the driver file component in McAfee GetSusp prior to 4.0.0 could allow a program being investigated on the local machine to trigger a buffer overflow in GetSusp, leading to the execution of arbitrary code, potentially triggering a BSOD.	8.8	More Details
CVE-2021-30545	Use after free in Extensions in Google Chrome prior to 91.0.4472.101 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-33842	Improper Authentication vulnerability in the cookie parameter of Circutor SGE-PLC1000 firmware version 0.9.2b allows an attacker to perform operations as an authenticated user. In order to exploit this vulnerability, the attacker must be within the network where the device affected is located.	8.8	More Details
CVE-2021-30544	Use after free in BFCache in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-31928	Annex Cloud Loyalty Experience Platform <2021.1.0.1 allows any authenticated attacker to escalate privileges to superadministrator. It was fixed in v2021.1.0.2.	8.8	More Details
CVE-2021-34128	LaikeTui 3.5.0 allows remote authenticated users to execute arbitrary PHP code by using index.php?module=system&action=pay to upload a ZIP archive containing a .php file, as demonstrated by the ../../../../phpinfo.php pathname.	8.8	More Details
CVE-2021-31659	TP-Link TL-SG2005, TL-SG2008, etc. 1.0.0 Build 20180529 Rel.40524 is vulnerable to Cross Site Request Forgery (CSRF). All configuration information is placed in the URL, without any additional token authentication information. A malicious link opened by the switch administrator may cause the password of the switch to be modified and the configuration file to be tampered with.	8.8	More Details
CVE-2021-32683	wire-webapp is the web version of Wire, an open-source messenger. A cross-site scripting vulnerability exists in wire-webapp prior to version 2021-06-01-production.0. If a user is instructed to open an image in a new tab (right click -> open in new tab, or copy the URL and paste it in the URL bar), an the image payload is executed on the domain hosting the app (app.wire.com). In particular, if an image contains malicious code in addition to the actual picture, this code is executed on app.wire.com. This allows the attacker to fully control the user account. The vulnerability was patched in version 2021-06-01-production.0. As a workaround, users should not try to open image URLs.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21665	A cross-site request forgery (CSRF) vulnerability in Jenkins XebiaLabs XL Deploy Plugin 10.0.1 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing Username/password credentials stored in Jenkins.	8.8	More Details
CVE-2021-33393	lfs/backup in IPFire 2.25-core155 does not ensure that /var/ipfire/backup/bin/backup.pl is owned by the root account. It might be owned by an unprivileged account, which could potentially be used to install a Trojan horse backup.pl script that is later executed by root. Similar problems with the ownership/permissions of other files may be present as well.	8.8	More Details
CVE-2021-21808	A memory corruption vulnerability exists in the PNG png_palette_process functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to a heap buffer overflow. An attacker can provide malicious inputs to trigger this vulnerability.	8.8	More Details
CVE-2021-33894	In Progress MOVEit Transfer before 2019.0.6 (11.0.6), 2019.1.x before 2019.1.5 (11.1.5), 2019.2.x before 2019.2.2 (11.2.2), 2020.x before 2020.0.5 (12.0.5), 2020.1.x before 2020.1.4 (12.1.4), and 2021.x before 2021.0.1 (13.0.1), a SQL injection vulnerability exists in SILUtility.vb in MOVEit.DMZ.WebApp in the MOVEit Transfer web app. This could allow an authenticated attacker to gain unauthorized access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and/or execute SQL statements that alter or delete database elements.	8.8	More Details
CVE-2021-0475	In on_l2cap_data_ind of btif_sock_l2cap.cc, there is possible memory corruption due to a use after free. 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-11 Android-10Android ID: A-175686168	8.8	More Details
CVE-2021-0101	Buffer overflow in the BMC firmware for Intel(R) Server BoardM10JNP2SB before version EFI BIOS 7215, BMC 8100.01.08 may allow an unauthenticated user to potentially enable an escalation of privilege via adjacent access.	8.8	More Details
CVE-2021-0070	Improper input validation in the BMC firmware for Intel(R) Server Board M10JNP2SB before version EFI BIOS 7215, BMC 8100.01.08 may allow an unauthenticated user to potentially enable an escalation of privilege via adjacent access.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24341	When deleting a date in the Xllentech English Islamic Calendar WordPress plugin before 2.6.8, the year_number and month_number POST parameters are not sanitised, escaped or validated before being used in a SQL statement, leading to SQL injection.	8.8	More Details
CVE-2021-24347	The SP Project & Document Manager WordPress plugin before 4.22 allows users to upload files, however, the plugin attempts to prevent php and other similar files that could be executed on the server from being uploaded by checking the file extension. It was discovered that php files could still be uploaded by changing the file extension's case, for example, from "php" to "pHP".	8.8	More Details
CVE-2021-24352	The export_data function of the Simple 301 Redirects by BetterLinks WordPress plugin before 2.0.4 had no capability or nonce checks making it possible for unauthenticated users to export a site's redirects.	8.8	More Details
CVE-2021-24353	The import_data function of the Simple 301 Redirects by BetterLinks WordPress plugin before 2.0.4 had no capability or nonce checks making it possible for unauthenticated users to import a set of site redirects.	8.8	More Details
CVE-2021-24354	A lack of capability checks and insufficient nonce check on the AJAX action in the Simple 301 Redirects by BetterLinks WordPress plugin before 2.0.4, made it possible for authenticated users to install arbitrary plugins on vulnerable sites.	8.8	More Details
CVE-2021-33358	Multiple vulnerabilities exist in RaspAP 2.3 to 2.6.5 in the "interface", "ssid" and "wpa_passphrase" POST parameters in /hostapd, when the parameter values contain special characters such as ";" or "$()" which enables an authenticated attacker to execute arbitrary OS commands.	8.8	More Details
CVE-2021-33356	Multiple privilege escalation vulnerabilities in RaspAP 1.5 to 2.6.5 could allow an authenticated remote attacker to inject arbitrary commands to /installers/common.sh component that can result in remote command execution with root privileges.	8.8	More Details
CVE-2021-24356	In the Simple 301 Redirects by BetterLinks WordPress plugin before 2.0.4, a lack of capability checks and insufficient nonce check on the AJAX action, simple301redirects/admin/activate_plugin, made it possible for authenticated users to activate arbitrary plugins installed on vulnerable sites.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3196	An issue was discovered in Hitachi ID Bravura Security Fabric 11.0.0 through 11.1.3, 12.0.0 through 12.0.2, and 12.1.0. When using federated identity management (authenticating via SAML through a third-party identity provider), an attacker can inject additional data into a signed SAML response being transmitted to the service provider (ID Bravura Security Fabric). The application successfully validates the signed values but uses the unsigned malicious values. An attacker with lower-privilege access to the application can inject the username of a high-privilege user to impersonate that user.	8.8	More Details
CVE-2021-29995	A Cross Site Request Forgery (CSRF) issue in Server Console in CloverDX through 5.9.0 allows remote attackers to execute any action as the logged-in user (including script execution). The issue is resolved in CloverDX 5.10, CloverDX 5.9.1, CloverDX 5.8.2, and CloverDX 5.7.1.	8.8	More Details
CVE-2021-30548	Use after free in Loader in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30546	Use after free in Autofill in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-25682	It was discovered that the get_pid_info() function in data/apport did not properly parse the /proc/pid/status file from the kernel.	8.8	More Details
CVE-2021-26828	OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows allows remote authenticated users to upload and execute arbitrary JSP files via view_edit.shtm.	8.8	More Details
CVE-2021-28814	An improper access control vulnerability has been reported to affect QNAP NAS. If exploited, this vulnerability allows remote attackers to compromise the security of the software. This issue affects: QNAP Systems Inc. Helpdesk versions prior to 3.0.4.	8.8	More Details
CVE-2021-25684	It was discovered that apport in data/apport did not properly open a report file to prevent hanging reads on a FIFO.	8.8	More Details
CVE-2021-25683	It was discovered that the get_starttime() function in data/apport did not properly parse the /proc/pid/stat file from the kernel.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0473	In rw_t3t_process_error of rw_t3t.cc, there is a possible double free due to uninitialized data. 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-9 Android-10 Android-11 Android-8.1Android ID: A-179687208	8.8	More Details
CVE-2021-26995	E-Series SANtricity OS Controller Software 11.x versions prior to 11.70.1 are susceptible to a vulnerability which when successfully exploited could allow privileged attackers to execute arbitrary code.	8.8	More Details
CVE-2020-11256	Memory corruption due to lack of check of validation of pointer to buffer passed to trustzone in Snapdragon Wired Infrastructure and Networking	8.8	More Details
CVE-2020-11257	Memory corruption due to lack of validation of pointer arguments passed to TrustZone BSP in Snapdragon Wired Infrastructure and Networking	8.8	More Details
CVE-2020-11258	Memory corruption due to lack of validation of pointer arguments passed to Trustzone BSP in Snapdragon Wired Infrastructure and Networking	8.8	More Details
CVE-2020-11259	Memory corruption due to lack of validation of pointer arguments passed to Trustzone BSP in Snapdragon Wired Infrastructure and Networking	8.8	More Details
CVE-2020-13663	Cross Site Request Forgery vulnerability in Drupal Core Form API does not properly handle certain form input from cross-site requests, which can lead to other vulnerabilities.	8.8	More Details
CVE-2021-29754	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a privilege escalation vulnerability when using the SAML Web Inbound Trust Association Interceptor (TAI). IBM X-Force ID: 202006.	8.8	More Details
CVE-2021-26195	An issue was discovered in JerryScript 2.4.0. There is a heap-buffer-overflow in lexer_parse_number in js-lexer.c file.	8.8	More Details
CVE-2021-25424	Improper authentication vulnerability in Tizen bluetooth-frwk prior to Firmware update JUN-2021 Release allows bluetooth attacker to take over the user's bluetooth device without user awareness.	8.8	More Details
CVE-2021-30551	Type confusion in V8 in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30550	Use after free in Accessibility in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30549	Use after free in Spell check in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30552	Use after free in Extensions in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-20731	WSR-1166DHP3 firmware Ver.1.16 and prior and WSR-1166DHP4 firmware Ver.1.02 and prior allow an attacker to execute arbitrary OS commands with root privileges via unspecified vectors.	8.8	More Details
CVE-2020-24671	Trace Financial CRESTBridge <6.3.0.02 contains an authenticated SQL injection vulnerability, which was fixed in 6.3.0.03.	8.8	More Details
CVE-2020-24667	Trace Financial CRESTBridge <6.3.0.02 contains an authenticated SQL injection vulnerability, which was fixed in 6.3.0.03.	8.8	More Details
CVE-2021-33205	Western Digital EdgeRover before 0.25 has an escalation of privileges vulnerability where a low privileged user could load malicious content into directories with higher privileges, because of how Node.js is used. An attacker can gain admin privileges and carry out malicious activities such as creating a fake library and stealing user credentials.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21382	Restund is an open source NAT traversal server. The restund TURN server can be instructed to open a relay to the loopback address range. This allows you to reach any other service running on localhost which you might consider private. In the configuration that we ship (https://github.com/wireapp/ansible-restund/blob/master/templates/restund.conf.j2#L40-L43) the `status` interface of restund is enabled and is listening on `127.0.0.1`.The `status` interface allows users to issue administrative commands to `restund` like listing open relays or draining connections. It would be possible for an attacker to contact the status interface and issue administrative commands by setting `XOR-PEER-ADDRESS` to `127.0.0.1:{{restund_udp_status_port}}` when opening a TURN channel. We now explicitly disallow relaying to loopback addresses, 'any' addresses, link local addresses, and the broadcast address. As a workaround disable the `status` module in your restund configuration. However there might still be other services running on `127.0.0.0/8` that you do not want to have exposed. The `turn` module can be disabled. Restund will still perform STUN and this might already be enough for initiating calls in your environments. TURN is only used as a last resort when other NAT traversal options do not work. One should also make sure that the TURN server is set up with firewall rules so that it cannot relay to other addresses that you don't want the TURN server to relay to. For example other services in the same VPC where the TURN server is running. Ideally TURN servers should be deployed in an isolated fashion where they can only reach what they need to reach to perform their task of assisting NAT-traversal.	8.6	More Details
CVE-2021-1900	Possible use after free in Display due to race condition while creating an external display in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2020-11260	An improper free of uninitialized memory can occur in DIAG services in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2020-11267	Stack out-of-bounds write occurs while setting up a cipher device if the provided IV length exceeds the max limit value in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23854	An error in the handling of a page parameter in Bosch IP cameras may lead to a reflected cross site scripting (XSS) in the web-based interface. This issue only affects versions 7.7x and 7.6x. All other versions are not affected.	8.3	More Details
CVE-2021-23853	In Bosch IP cameras, improper validation of the HTTP header allows an attacker to inject arbitrary HTTP headers through crafted URLs.	8.3	More Details
CVE-2021-23848	An error in the URL handler Bosch IP cameras may lead to a reflected cross site scripting (XSS) in the web-based interface. An attacker with knowledge of the camera address can send a crafted link to a user, which will execute javascript code in the context of the user.	8.3	More Details
CVE-2021-32677	FastAPI is a web framework for building APIs with Python 3.6+ based on standard Python type hints. FastAPI versions lower than 0.65.2 that used cookies for authentication in path operations that received JSON payloads sent by browsers were vulnerable to a Cross-Site Request Forgery (CSRF) attack. In versions lower than 0.65.2, FastAPI would try to read the request payload as JSON even if the content-type header sent was not set to application/json or a compatible JSON media type (e.g. application/geo+json). A request with a content type of text/plain containing JSON data would be accepted and the JSON data would be extracted. Requests with content type text/plain are exempt from CORS preflights, for being considered Simple requests. The browser will execute them right away including cookies, and the text content could be a JSON string that would be parsed and accepted by the FastAPI application. This is fixed in FastAPI 0.65.2. The request data is now parsed as JSON only if the content-type header is application/json or another JSON compatible media type like application/geo+json. It's best to upgrade to the latest FastAPI, but if updating is not possible then a middleware or a dependency that checks the content-type header and aborts the request if it is not application/json or another JSON compatible content type can act as a mitigating workaround.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22901	curl 7.75.0 through 7.76.1 suffers from a use-after-free vulnerability resulting in already freed memory being used when a TLS 1.3 session ticket arrives over a connection. A malicious server can use this in rare unfortunate circumstances to potentially reach remote code execution in the client. When libcurl at run-time sets up support for TLS 1.3 session tickets on a connection using OpenSSL, it stores pointers to the transfer in-memory object for later retrieval when a session ticket arrives. If the connection is used by multiple transfers (like with a reused HTTP/1.1 connection or multiplexed HTTP/2 connection) that first transfer object might be freed before the new session is established on that connection and then the function will access a memory buffer that might be freed. When using that memory, libcurl might even call a function pointer in the object, making it possible for a remote code execution if the server could somehow manage to get crafted memory content into the correct place in memory.	8.1	More Details
CVE-2021-23394	The package studio-42/elfinder before 2.1.58 are vulnerable to Remote Code Execution (RCE) via execution of PHP code in a .phar file. NOTE: This only applies if the server parses .phar files as PHP.	8.1	More Details
CVE-2021-0133	Key exchange without entity authentication in the Intel(R) Security Library before version 3.3 may allow an authenticated user to potentially enable escalation of privilege via network access.	8.1	More Details
CVE-2021-31658	TP-Link TL-SG2005, TL-SG2008, etc. 1.0.0 Build 20180529 Rel.40524 is affected by an Array index error. The interface that provides the "device description" function only judges the length of the received data, and does not filter special characters. This vulnerability will cause the application to crash, and all device configuration information will be erased.	8.1	More Details
CVE-2021-34129	LaikeTui 3.5.0 allows remote authenticated users to delete arbitrary files, as demonstrated by deleting install.lock in order to reinstall the product in an attacker-controlled manner. This deletion is possible via directory traversal in the uploadImg, oldpic, or imgurl parameter.	8.1	More Details
CVE-2021-23204	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Gallagher Command Centre Server allows OSDP key material to be exposed to Command Centre Operators. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1359 (MR3).	8.1	More Details
CVE-2021-21557	Dell PowerEdge Server BIOS and select Dell Precision Rack BIOS contain an out-of-bounds array access vulnerability. A local malicious user with high privileges may potentially exploit this vulnerability, leading to a denial of service, arbitrary code execution, or information disclosure in System Management Mode.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23205	Improper Encoding or Escaping in Gallagher Command Centre Server allows a Command Centre Operator to alter the configuration of Controllers and other hardware items beyond their privilege. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1359 (MR3); 8.20 versions prior to 8.20.1259 (MR5); version 8.10 and prior versions.	8.1	More Details
CVE-2020-24474	Buffer overflow in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.48.ce3e3bd2 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	8.0	More Details
CVE-2021-31485	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12711.	7.8	More Details
CVE-2020-24473	Out of bounds write in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.48.ce3e3bd2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-7860	UnEGG v0.5 and eariler versions have a Integer overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by UnEGG. Attackers could exploit this and arbitrary code execution. This issue affects: Estsoft UnEGG 0.5 versions prior to 1.0 on linux.	7.8	More Details
CVE-2021-0498	In memory management driver, there is a possible memory corruption due to a double 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 SoCAndroid ID: A-183461321	7.8	More Details
CVE-2021-0497	In memory management driver, there is a possible memory corruption 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 SoCAndroid ID: A-183461320	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0496	In memory management driver, there is a possible memory corruption 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 SoCAndroid ID: A-183467912	7.8	More Details
CVE-2021-31484	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12710.	7.8	More Details
CVE-2021-0495	In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-183459083	7.8	More Details
CVE-2021-0494	In memory management driver, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-183461318	7.8	More Details
CVE-2021-0493	In memory management driver, 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 SoCAndroid ID: A-183461317	7.8	More Details
CVE-2021-0492	In memory management driver, 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 SoCAndroid ID: A-183459078	7.8	More Details
CVE-2021-0491	In memory management driver, there is a possible escalation of privilege 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 SoCAndroid ID: A-183461315	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3041	A local privilege escalation vulnerability exists in the Palo Alto Networks Cortex XDR agent on Windows platforms that enables an authenticated local Windows user to execute programs with SYSTEM privileges. This requires the user to have the privilege to create files in the Windows root directory or to manipulate key registry values. This issue impacts: Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.11; Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.8; Cortex XDR agent 7.2 versions earlier than Cortex XDR agent 7.2.3; All versions of Cortex XDR agent 7.2 without content update release 171 or a later version.	7.8	More Details
CVE-2021-0490	In memory management driver, 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 SoCAndroid ID: A-183464868	7.8	More Details
CVE-2021-0489	In memory management driver, 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 SoCAndroid ID: A-183464866	7.8	More Details
CVE-2021-0487	In onCreate of CalendarDebugActivity.java, there is a possible way to export calendar data to the sdcard without user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174046397	7.8	More Details
CVE-2021-0485	In getMinimalSize of PipBoundsAlgorithm.java, there is a possible bypass of restrictions on background processes due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174302616	7.8	More Details
CVE-2021-0106	Incorrect default permissions in the Intel(R) Optane(TM) DC Persistent Memory for Windows software versions before 2.00.00.3842 or 1.00.00.3515 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0104	Uncontrolled search path element in the installer for the Intel(R) Rapid Storage Technology software, before versions 17.9.0.34, 18.0.0.640 and 18.1.0.24, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0102	Insecure inherited permissions in the Intel Unite(R) Client for Windows before version 4.2.25031 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2021-0057	Uncontrolled search path in the Intel(R) NUC M15 Laptop Kit Driver Pack software before updated version 1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-31502	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13673.	7.8	More Details
CVE-2020-12981	An insufficient input validation in the AMD Graphics Driver for Windows 10 may allow unprivileged users to unload the driver, potentially causing memory corruptions in high privileged processes, which can lead to escalation of privileges or denial of service.	7.8	More Details
CVE-2020-12980	An out of bounds write and read vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.	7.8	More Details
CVE-2021-0052	Incorrect default privileges in the Intel(R) Computing Improvement Program before version 2.4.6522 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2021-0055	Insecure inherited permissions for some Intel(R) NUC 9 Extreme Laptop Kit LAN Drivers before version 10.42 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0056	Insecure inherited permissions for the Intel(R) NUC M15 Laptop Kit Driver Pack software before updated version 1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0058	Incorrect default permissions in the Intel(R) NUC M15 Laptop Kit Driver Pack software before updated version 1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0100	Incorrect default permissions in the installer for the Intel(R) SSD Data Center Tool, versions downloaded before 12/31/2020, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0073	Insufficient control flow management in Intel(R) DSA before version 20.11.50.9 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0074	Improper permissions in the installer for the Intel(R) Computing Improvement Program software before version 2.4.5982 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0077	Insecure inherited permissions in the installer for the Intel(R) VTune(TM) Profiler before version 2021.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-7864	Parameter manipulation can bypass authentication to cause file upload and execution. This will execute the remote code. This issue affects: Raonwiz DEXT5Editor versions prior to 3.5.1405747.1100.03.	7.8	More Details
CVE-2021-0094	Improper link resolution before file access in Intel(R) DSA before version 20.11.50.9 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2021-0098	Improper access control in the Intel Unite(R) Client for Windows before version 4.2.25031 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2021-0481	In onActivityResult of EditUserPhotoController.java, there is a possible access of unauthorized files due to an unexpected URI handler. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-172939189	7.8	More Details
CVE-2021-0477	In notifyScreenshotError of ScreenshotNotificationsController.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-178189250	7.8	More Details
CVE-2021-23023	On version 7.2.1.x before 7.2.1.3 and 7.1.x before 7.1.9.9 Update 1, a DLL hijacking issue exists in cachecleaner.dll included in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25401	Intent redirection vulnerability in Samsung Health prior to version 6.16 allows attacker to execute privileged action.	7.8	More Details
CVE-2021-22756	A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of user-supplied data validation, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2021-22755	A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2021-22754	A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to lack of proper validation of user-supplied data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2021-22753	A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing length checks, when a malicious WSP file is being parsed by IGSS Definition.	7.8	More Details
CVE-2021-22752	A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing size checks, when a malicious WSP (Workspace) file is being parsed by IGSS Definition.	7.8	More Details
CVE-2021-25400	Intent redirection vulnerability in Samsung Internet prior to version 14.0.1.20 allows attacker to execute privileged action.	7.8	More Details
CVE-2021-22751	A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or execution of arbitrary code due to lack of input validation, when a malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2021-22758	A CWE-824: Access of uninitialized pointer vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to lack validation of user-supplied input data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22750	A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21041 and prior that could result in loss of data or remote code execution due to missing length checks, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2021-25407	A possible out of bounds write vulnerability in NPU driver prior to SMR JUN-2021 Release 1 allows arbitrary memory write.	7.8	More Details
CVE-2021-25408	A possible buffer overflow vulnerability in NPU driver prior to SMR JUN-2021 Release 1 allows arbitrary memory write and code execution.	7.8	More Details
CVE-2020-11165	Memory corruption due to buffer overflow while copying the message provided by HLOS into buffer without validating the length of buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-25412	An improper access control vulnerability in genericssoservice prior to SMR JUN-2021 Release 1 allows local attackers to execute protected activity with system privilege via untrusted applications.	7.8	More Details
CVE-2021-25414	Improper sanitization of incoming intent in Samsung Contacts prior to SMR JUN-2021 Release 1 allows local attackers to copy or overwrite arbitrary files with Samsung Contacts privilege.	7.8	More Details
CVE-2021-22757	A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied input data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2021-22759	A CWE-416: Use after free vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to use of unchecked input data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2020-11306	Possible integer overflow in RPMB counter due to lack of length check on user provided data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11261	Memory corruption due to improper check to return error when user application requests memory allocation of a huge size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2020-11304	Possible out of bound read in DRM due to improper buffer length check. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-0472	In shouldLockKeyguard of LockTaskController.java, there is a possible way to exit App Pinning without a PIN due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-176801033	7.8	More Details
CVE-2020-11298	While waiting for a response to a callback or listener request, non-secure clients can change permissions to shared memory buffers used by HLOS Invoke Call to secure kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-23022	On version 7.2.1.x before 7.2.1.3 and 7.1.x before 7.1.9.9 Update 1, the BIG-IP Edge Client Windows Installer Service's temporary folder has weak file and folder permissions. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.8	More Details
CVE-2021-28210	An unlimited recursion in DxeCore in EDK II.	7.8	More Details
CVE-2020-11292	Possible buffer overflow in voice service due to lack of input validation of parameters in QMI Voice API in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2020-11240	Memory corruption due to ioctl command size was incorrectly set to the size of a pointer and not enough storage is allocated for the copy of the user argument in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22760	A CWE-763: Release of invalid pointer or reference vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing checks of user-supplied input data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2021-28805	Inclusion of sensitive information in the source code has been reported to affect certain QNAP switches running QSS. If exploited, this vulnerability allows attackers to read application data. This issue affects: QNAP Systems Inc. QSS versions prior to 1.0.3 build 20210505 on QSW-M2108-2C; versions prior to 1.0.3 build 20210505 on QSW-M2108-2S; versions prior to 1.0.3 build 20210505 on QSW-M2108R-2C; versions prior to 1.0.12 build 20210506 on QSW-M408.	7.8	More Details
CVE-2020-11239	Use after free issue when importing a DMA buffer by using the CPU address of the buffer due to attachment is not cleaned up properly in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2020-11235	Buffer overflow might occur while parsing unified command due to lack of check of input data received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-22762	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in remote code execution, when a malicious CGF or WSP file is being parsed by IGSS Definition.	7.8	More Details
CVE-2021-22761	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code e+F15xecution due to missing length check on user supplied data, when a malicious CGF file is imported to IGSS Definition.	7.8	More Details
CVE-2020-11178	Trusted APPS to overwrite the CPZ memory of another use-case as TZ only checks the physical address not overlapping with its memory and its RoT memory in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12982	An invalid object pointer free vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.	7.8	More Details
CVE-2021-25418	Improper component protection vulnerability in Samsung Internet prior to version 14.0.1.62 allows untrusted applications to execute arbitrary activity in specific condition.	7.8	More Details
CVE-2021-31495	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13307.	7.8	More Details
CVE-2021-31478	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12633.	7.8	More Details
CVE-2021-31492	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12720.	7.8	More Details
CVE-2021-31489	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12717.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31488	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12716.	7.8	More Details
CVE-2021-31500	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12746.	7.8	More Details
CVE-2021-31487	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12715.	7.8	More Details
CVE-2020-27384	The Gw2-64.exe in Guild Wars 2 launcher version 106916 suffers from an elevation of privileges vulnerability which can be used by an "Authenticated User" to modify the existing executable file with a binary of his choice. The vulnerability exist due to the improper permissions, with the 'F' flag (Full Control) for 'Everyone' group, making the entire directory 'Guild Wars 2' and its files and sub-dirs world-writable.	7.8	More Details
CVE-2021-31496	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13308.	7.8	More Details
CVE-2020-12360	Out of bounds read in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33669	Under certain conditions, SAP Mobile SDK Certificate Provider allows a local unprivileged attacker to exploit an insecure temporary file storage. For a successful exploitation user interaction from another user is required and could lead to complete impact of confidentiality integrity and availability.	7.8	More Details
CVE-2020-27383	Battle.net.exe in Battle.Net 1.27.1.12428 suffers from an elevation of privileges vulnerability which can be used by an "Authenticated User" to modify the existing executable file with a binary of his choice. The vulnerability exist due to weak set of permissions being granted to the "Authenticated Users Group" which grants the (F) Flag aka "Full Control"	7.8	More Details
CVE-2021-31491	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12719.	7.8	More Details
CVE-2021-31494	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13305.	7.8	More Details
CVE-2021-31479	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12634.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31493	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13304.	7.8	More Details
CVE-2021-31480	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12654.	7.8	More Details
CVE-2021-31481	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 SLDPRT files. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12659.	7.8	More Details
CVE-2021-31497	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of DWG files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13311.	7.8	More Details
CVE-2021-31482	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12708.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12986	An insufficient pointer validation vulnerability in the AMD Graphics Driver for Windows 10 may cause arbitrary code execution in the kernel, leading to escalation of privilege or denial of service.	7.8	More Details
CVE-2021-31483	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12709.	7.8	More Details
CVE-2021-31499	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12745.	7.8	More Details
CVE-2021-31486	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12712.	7.8	More Details
CVE-2020-12985	An insufficient pointer validation vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.	7.8	More Details
CVE-2020-12983	An out of bounds write vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privileges or denial of service.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31490	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12718.	7.8	More Details
CVE-2021-22181	A denial of service vulnerability in GitLab CE/EE affecting all versions since 11.8 allows an attacker to create a recursive pipeline relationship and exhaust resources.	7.7	More Details
CVE-2020-23309	There is an Assertion 'context_p->stack_depth == context_p->context_stack_depth' failed at js-parser-statm.c:2756 in parser_parse_statements in JerryScript 2.2.0.	7.5	More Details
CVE-2021-25417	Improper authorization in SDP SDK prior to SMR JUN-2021 Release 1 allows access to internal storage.	7.5	More Details
CVE-2020-23308	There is an Assertion 'context_p->stack_top_uint8 == LEXER_EXPRESSION_START' at js-parser-expr.c:3565 in parser_parse_expression in JerryScript 2.2.0.	7.5	More Details
CVE-2020-23311	There is an Assertion 'context_p->token.type == LEXER_RIGHT_BRACE || context_p->token.type == LEXER_ASSIGN || context_p->token.type == LEXER_COMMA' failed at js-parser-expr.c:3230 in parser_parse_object_initializer in JerryScript 2.2.0.	7.5	More Details
CVE-2020-23312	There is an Assertion 'context.status_flags & PARSER_SCANNING_SUCCESSFUL' failed at js-parser.c:2185 in parser_parse_source in JerryScript 2.2.0.	7.5	More Details
CVE-2020-23310	There is an Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at js-parser-statm.c:733 in parser_parse_function_statement in JerryScript 2.2.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27632	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EnqConvUniToSrvReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2021-28213	Example EDK2 encrypted private key in the IpSecDxe.efi present potential security risks.	7.5	More Details
CVE-2021-0466	In startIpClient of ClientModeImpl.java, there is a possible identifier which could be used to track a device. This could lead to remote information disclosure to a proximal attacker, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154114734	7.5	More Details
CVE-2020-23314	There is an Assertion 'block_found' failed at js-parser-statm.c:2003 parser_parse_try_statement_end in JerryScript 2.2.0.	7.5	More Details
CVE-2021-27631	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EnqConvUniToSrvReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2021-33359	A vulnerability exists in gowitness < 2.3.6 that allows an unauthenticated attacker to perform an arbitrary file read using the file:// scheme in the url parameter to get an image of any file.	7.5	More Details
CVE-2021-34555	OpenDMARC 1.4.1 and 1.4.1.1 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a multi-value From header field.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1937	Reachable assertion is possible while processing peer association WLAN message from host and nonstandard incoming packet in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-23313	There is an Assertion 'scope_stack_p > context_p->scope_stack_p' failed at js-scanner-util.c:2510 in scanner_literal_is_created in JerryScript 2.2.0	7.5	More Details
CVE-2021-22766	A CWE-20: Improper Input Validation vulnerability exists in PowerLogic EGX100 (Versions 3.0.0 and newer) and PowerLogic EGX300 (All Versions) that could cause denial of service via a specially crafted HTTP packet	7.5	More Details
CVE-2020-23319	There is an Assertion in '(flags >> CBC_STACK_ADJUST_SHIFT) >= CBC_STACK_ADJUST_BASE ll (CBC_STACK_ADJUST_BASE - (flags >> CBC_STACK_ADJUST_SHIFT)) <= context_p->stack_depth' in parser_emit_cbc_backward_branch in JerryScript 2.2.0.	7.5	More Details
CVE-2021-26845	Information Exposure vulnerability in Hitachi ABB Power Grids eSOMS allows unauthorized user to gain access to report data if the URL used to access the report is discovered. This issue affects: Hitachi ABB Power Grids eSOMS 6.0 versions prior to 6.0.4.2.2; 6.1 versions prior to 6.1.4; 6.3 versions prior to 6.3.	7.5	More Details
CVE-2021-20591	Uncontrolled Resource Consumption vulnerability in Mitsubishi Electric MELSEC iQ-R series CPU modules (R00/01/02CPU all versions, R04/08/16/32/120(EN)CPU all versions, R08/16/32/120SFCPU all versions, R08/16/32/120PCPU all versions, R08/16/32/120PSFCPU all versions) allows a remote unauthenticated attacker to prevent legitimate clients from connecting to the MELSOFT transmission port (TCP/IP) by not closing a connection properly, which may lead to a denial of service (DoS) condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31618	Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process. Since such a triggering HTTP/2 request is easy to craft and submit, this can be exploited to DoS the server. This issue affected mod_http2 1.15.17 and Apache HTTP Server version 2.4.47 only. Apache HTTP Server 2.4.47 was never released.	7.5	More Details
CVE-2021-20027	A buffer overflow vulnerability in SonicOS allows a remote attacker to cause a Denial of Service (DoS) by sending a specially crafted request. This vulnerability affects SonicOS Gen5, Gen6, Gen7 platforms, and SonicOSv virtual firewalls.	7.5	More Details
CVE-2020-15381	Brocade SANnav before version 2.1.1 contains an Improper Authentication vulnerability that allows cleartext transmission of authentication credentials of the jmx server.	7.5	More Details
CVE-2020-15383	Running security scans against the SAN switch can cause config and secnotify processes within the firmware before Brocade Fabric OS v9.0.0, v8.2.2d and v8.2.1e to consume all memory leading to denial of service impacts possibly including a switch panic.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27196	Improper Input Validation vulnerability in Hitachi ABB Power Grids Relion 670 Series, Relion 670/650 Series, Relion 670/650/SAM600-IO, Relion 650, REB500, RTU500 Series, FOX615 (TEGO1), MSM, GMS600, PWC600 allows an attacker with access to the IEC 61850 network with knowledge of how to reproduce the attack, as well as the IP addresses of the different IEC 61850 access points (of IEDs/products), to force the device to reboot, which renders the device inoperable for approximately 60 seconds. This vulnerability affects only products with IEC 61850 interfaces. This issue affects: Hitachi ABB Power Grids Relion 670 Series 1.1; 1.2.3 versions prior to 1.2.3.20; 2.0 versions prior to 2.0.0.13; 2.1; 2.2.2 versions prior to 2.2.2.3; 2.2.3 versions prior to 2.2.3.2. Hitachi ABB Power Grids Relion 670/650 Series 2.2.0 versions prior to 2.2.0.13. Hitachi ABB Power Grids Relion 670/650/SAM600-IO 2.2.1 versions prior to 2.2.1.6. Hitachi ABB Power Grids Relion 650 1.1; 1.2; 1.3 versions prior to 1.3.0.7. Hitachi ABB Power Grids REB500 7.3; 7.4; 7.5; 7.6; 8.2; 8.3. Hitachi ABB Power Grids RTU500 Series 7.x version 7.x and prior versions; 8.x version 8.x and prior versions; 9.x version 9.x and prior versions; 10.x version 10.x and prior versions; 11.x version 11.x and prior versions; 12.x version 12.x and prior versions. Hitachi ABB Power Grids FOX615 (TEGO1) R1D02 version R1D02 and prior versions. Hitachi ABB Power Grids MSM 2.1.0 versions prior to 2.1.0. Hitachi ABB Power Grids GMS600 1.3.0 version 1.3.0 and prior versions. Hitachi ABB Power Grids PWC600 1.0 versions prior to 1.0.1.4; 1.1 versions prior to 1.1.0.1.	7.5	More Details
CVE-2021-26996	E-Series SANtricity OS Controller Software 11.x versions prior to 11.70.1 are susceptible to a vulnerability which when successfully exploited could allow a remote attacker to discover system configuration and application information which may aid in crafting more complex attacks.	7.5	More Details
CVE-2021-33668	Due to improper input sanitization, specially crafted LDAP queries can be injected by an unauthenticated user. This could partially impact the confidentiality of the application.	7.5	More Details
CVE-2020-23320	There is an Assertion in 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' in parser_parse_function_arguments in JerryScript 2.2.0.	7.5	More Details
CVE-2020-11238	Possible Buffer over-read in ARP/NS parsing due to lack of check of packet length received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15379	Brocade SANnav before v.2.1.0a could allow remote attackers cause a denial-of-service condition due to a lack of proper validation, of the length of user-supplied data as name for custom field name.	7.5	More Details
CVE-2020-15380	Brocade SANnav before version 2.1.1 logs account credentials at the ‘trace’ logging level.	7.5	More Details
CVE-2021-22902	The actionpack ruby gem (a framework for handling and responding to web requests in Rails) before 6.0.3.7, 6.1.3.2 suffers from a possible denial of service vulnerability in the Mime type parser of Action Dispatch. Carefully crafted Accept headers can cause the mime type parser in Action Dispatch to do catastrophic backtracking in the regular expression engine.	7.5	More Details
CVE-2020-11241	Out of bound read will happen if EAPOL Key length is less than expected while processing NAN shared key descriptor attribute in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-22904	The actionpack ruby gem before 6.1.3.2, 6.0.3.7, 5.2.4.6, 5.2.6 suffers from a possible denial of service vulnerability in the Token Authentication logic in Action Controller due to a too permissive regular expression. Impacted code uses `authenticate_or_request_with_http_token` or `authenticate_with_http_token` for request authentication.	7.5	More Details
CVE-2020-23322	There is an Assertion in 'context_p->token.type == LEXER_RIGHT_BRACE ll context_p->token.type == LEXER_ASSIGN ll context_p->token.type == LEXER_COMMA' in parser_parse_object_initializer in JerryScript 2.2.0.	7.5	More Details
CVE-2021-28857	TP-Link's TL-WPA4220 4.0.2 Build 20180308 Rel.37064 username and password are sent via the cookie.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27633	SAP NetWeaver AS for ABAP (RFC Gateway), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method ThCPIC() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2020-13950	Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service	7.5	More Details
CVE-2021-27628	SAP NetWeaver ABAP Server and ABAP Platform (Dispatcher), versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method DpRTmPrepareReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2021-27408	The affected product is vulnerable to an out-of-bounds read, which can cause information leakage leading to arbitrary code execution if chained to the out-of-bounds write vulnerability on the Welch Allyn medical device management tools (Welch Allyn Service Tool: versions prior to v1.10, Welch Allyn Connex Device Integration Suite – Network Connectivity Engine (NCE): versions prior to v5.3, Welch Allyn Software Development Kit (SDK): versions prior to v3.2, Welch Allyn Connex Central Station (CS): versions prior to v1.8.6, Welch Allyn Service Monitor: versions prior to v1.7.0.0, Welch Allyn Connex Vital Signs Monitor (CVSM): versions prior to v2.43.02, Welch Allyn Connex Integrated Wall System (CIWS): versions prior to v2.43.02, Welch Allyn Connex Spot Monitor (CSM): versions prior to v1.52, Welch Allyn Spot Vital Signs 4400 Device (Spot 4400) / Welch Allyn Spot 4400 Vital Signs Extended Care Device: versions prior to v1.11.00).	7.5	More Details
CVE-2021-26690	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27607	SAP NetWeaver ABAP Server and ABAP Platform (Dispatcher), versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method ThSncIn() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2021-27606	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EncOAMParamStore() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2020-12988	A potential denial of service (DoS) vulnerability exists in the integrated chipset that may allow a malicious attacker to hang the system when it is rebooted.	7.5	More Details
CVE-2021-27597	SAP NetWeaver AS for ABAP (RFC Gateway), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method memmove() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2021-27629	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EncPSetUnsupported() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27630	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EnqConvUniToSrvReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	7.5	More Details
CVE-2021-31538	LANCOM R&S Unified Firewall (UF) devices running LCOS FX 10.5 allow Relative Path Traversal.	7.5	More Details
CVE-2021-32932	The affected product is vulnerable to a SQL injection, which may allow an unauthorized attacker to disclose information on the iView (versions prior to v5.7.03.6182).	7.5	More Details
CVE-2020-15387	The host SSH servers of Brocade Fabric OS before Brocade Fabric OS v7.4.2h, v8.2.1c, v8.2.2, v9.0.0, and Brocade SANnav before v2.1.1 utilize keys of less than 2048 bits, which may be vulnerable to man-in-the-middle attacks and/or insecure SSH communications.	7.4	More Details
CVE-2021-32551	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-15 package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-32553	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-17 package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-32554	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the xorg package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-23395	This affects all versions of package nedb. The library could be tricked into adding or modifying properties of Object.prototype using a __proto__ or constructor.prototype payload.	7.3	More Details
CVE-2021-0090	Uncontrolled search path element in Intel(R) DSA before version 20.11.50.9 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0112	Unquoted service path in the Intel Unite(R) Client for Windows before version 4.2.25031 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.3	More Details
CVE-2021-0108	Uncontrolled search path in the Intel Unite(R) Client for Windows before version 4.2.25031 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.3	More Details
CVE-2021-32550	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-14 package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-32549	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-13 package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-32548	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-8 package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2020-8702	Uncontrolled search path element in the Intel(R) Processor Diagnostic Tool before version 4.1.5.37 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.3	More Details
CVE-2021-32547	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-lts package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-0105	Insecure inherited permissions in some Intel(R) ProSet/Wireless WiFi drivers may allow an authenticated user to potentially enable information disclosure and denial of service via adjacent access.	7.3	More Details
CVE-2020-35452	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow	7.3	More Details
CVE-2021-32552	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-16 package apport hooks, it could expose private data to other local users.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32555	It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the xorg-hwe-18.04 package apport hooks, it could expose private data to other local users.	7.3	More Details
CVE-2021-31840	A vulnerability in the preloading mechanism of specific dynamic link libraries in McAfee Agent for Windows prior to 5.7.3 could allow an authenticated, local attacker to perform a DLL preloading attack with unsigned DLLs. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. This would result in the user gaining elevated permissions and being able to execute arbitrary code.	7.3	More Details
CVE-2021-21736	A smart camera product of ZTE is impacted by a permission and access control vulnerability. Due to the defect of user permission management by the cloud-end app, users whose sharing permissions have been revoked can still control the camera, such as restarting the camera, restoring factory settings, etc.. This affects ZXHN HS562 V1.0.0.0B2.0000, V1.0.0.0B3.0000E	7.2	More Details
CVE-2021-23024	On version 8.0.x before 8.0.0.1, and all 6.x and 7.x versions, the BIG-IQ Configuration utility has an authenticated remote command execution vulnerability in undisclosed pages. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.2	More Details
CVE-2021-24348	The menu delete functionality of the Side Menu – add fixed side buttons WordPress plugin before 3.1.5, available to Administrator users takes the did GET parameter and uses it into an SQL statement without proper sanitisation, validation or escaping, therefore leading to a SQL Injection issue	7.2	More Details
CVE-2021-34539	An issue was discovered in CubeCoders AMP before 2.1.1.8. A lack of validation of the Java Version setting means that an unintended executable path can be set. The result is that high-privileged users can trigger code execution.	7.2	More Details
CVE-2020-15382	Brocade SANnav before version 2.1.1 uses a hard-coded administrator account with the weak password ‘passw0rd’ if a password is not provided for PostgreSQL at install-time.	7.2	More Details
CVE-2021-20081	Incomplete List of Disallowed Inputs in ManageEngine ServiceDesk Plus before version 11205 allows a remote, authenticated attacker to execute arbitrary commands with SYSTEM privileges.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11161	Out-of-bounds memory access can occur while calculating alignment requirements for a negative width from external components in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.1	More Details
CVE-2021-25399	Improper configuration in Smart Manager prior to version 11.0.05.0 allows attacker to access the file with system privilege.	7.1	More Details
CVE-2021-25410	Improper access control of a component in CallBGProvider prior to SMR JUN-2021 Release 1 allows local attackers to access arbitrary files with an escalated privilege.	7.1	More Details
CVE-2021-25388	Improper caller check vulnerability in Knox Core prior to SMR MAY-2021 Release 1 allows attackers to install arbitrary app.	7.1	More Details
CVE-2021-0482	In BinderDiedCallback of MediaCodec.cpp, there is a possible memory corruption 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-11Android ID: A-173791720	7.0	More Details
CVE-2020-11262	A race between command submission and destroying the context can cause an invalid context being added to the list leads to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.0	More Details
CVE-2021-0476	In FindOrCreatePeer of btif_av.cc, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-169252501	7.0	More Details
CVE-2020-11233	Time-of-check time-of-use race condition While processing partition entries due to newly created buffer was read again from mmc without validation in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11250	Use after free due to race condition when reopening the device driver repeatedly in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.0	More Details
CVE-2021-31997	A UNIX Symbolic Link (Symlink) Following vulnerability in python-postorius of openSUSE Leap 15.2, Factory allows local attackers to escalate from users postorius or postorius-admin to root. This issue affects: openSUSE Leap 15.2 python-postorius version 1.3.2-lp152.1.2 and prior versions. openSUSE Factory python-postorius version 1.3.4-2.1 and prior versions.	6.8	More Details
CVE-2020-24514	Improper authentication in some Intel(R) RealSense(TM) IDs may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2021-22175	When requests to the internal network for webhooks are enabled, a server-side request forgery vulnerability in GitLab affecting all versions starting from 10.5 was possible to exploit for an unauthenticated attacker even on a GitLab instance where registration is disabled	6.8	More Details
CVE-2021-34546	An unauthenticated attacker with physical access to a computer with NetSetMan Pro before 5.0 installed, that has the pre-logon profile switch button within the Windows logon screen enabled, is able to drop to an administrative shell and execute arbitrary commands as SYSTEM via the "save log to file" feature. To accomplish this, the attacker can navigate to cmd.exe.	6.8	More Details
CVE-2020-24516	Modification of assumed-immutable data in subsystem in Intel(R) CSME versions before 13.0.47, 13.30.17, 14.1.53, 14.5.32, 15.0.22 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2021-25397	An improper access control vulnerability in TelephonyUI prior to SMR MAY-2021 Release 1 allows local attackers to write arbitrary files of telephony process via untrusted applications.	6.8	More Details
CVE-2021-31998	A Incorrect Default Permissions vulnerability in the packaging of inn of SUSE Linux Enterprise Server 11-SP3; openSUSE Backports SLE-15-SP2, openSUSE Leap 15.2 allows local attackers to escalate their privileges from the news user to root. This issue affects: SUSE Linux Enterprise Server 11-SP3 inn version inn-2.4.2-170.21.3.1 and prior versions. openSUSE Backports SLE-15-SP2 inn versions prior to 2.6.2. openSUSE Leap 15.2 inn versions prior to 2.6.2.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25322	A UNIX Symbolic Link (Symlink) Following vulnerability in python-HyperKitty of openSUSE Leap 15.2, Factory allows local attackers to escalate privileges from the user hyperkitty or hyperkitty-admin to root. This issue affects: openSUSE Leap 15.2 python-HyperKitty version 1.3.2-lp152.2.3.1 and prior versions. openSUSE Factory python-HyperKitty versions prior to 1.3.4-5.1.	6.8	More Details
CVE-2020-12359	Insufficient control flow management in the firmware for some Intel(R) Processors may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2020-24515	Protection mechanism failure in some Intel(R) RealSense(TM) IDs may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2021-20329	Specific cstrings input may not be properly validated in the MongoDB Go Driver when marshalling Go objects into BSON. A malicious user could use a Go object with specific string to potentially inject additional fields into marshalled documents. This issue affects all MongoDB GO Drivers prior to and including 1.5.0.	6.8	More Details
CVE-2021-33887	Insufficient verification of data authenticity in Peloton TTR01 up to and including PTV55G allows an attacker with physical access to boot into a modified kernel/ramdisk without unlocking the bootloader.	6.8	More Details
CVE-2021-0467	In Chromecast bootROM, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the bootloader, with physical USB access, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-174490700	6.8	More Details
CVE-2020-12357	Improper initialization in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-25396	An improper input validation vulnerability in NPU firmware prior to SMR MAY-2021 Release 1 allows arbitrary memory write and code execution.	6.7	More Details
CVE-2020-24509	Insufficient control flow management in subsystem in Intel(R) SPS versions before SPS_E3_05.01.04.300.0, SPS_SoC-A_05.00.03.091.0, SPS_E5_04.04.04.023.0, or SPS_E5_04.04.03.263.0 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0054	Improper buffer restrictions in system firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0067	Improper access control in system firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-28211	A heap overflow in LzmaUefiDecompressGetInfo function in EDK II.	6.7	More Details
CVE-2020-8700	Improper input validation in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-11160	Resource leakage issue during dci client registration due to reference count is not decremented if dci client registration fails in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2021-3040	An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than Checkov 2.0.139. Checkov 1.0 versions are not impacted.	6.7	More Details
CVE-2020-8703	Improper buffer restrictions in a subsystem in the Intel(R) CSME versions before 11.8.86, 11.12.86, 11.22.86, 12.0.81, 13.0.47, 13.30.17, 14.1.53, 14.5.32 and 15.0.22 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-32942	The vulnerability could expose cleartext credentials from AVEVA InTouch Runtime 2020 R2 and all prior versions (WindowViewer) if an authorized, privileged user creates a diagnostic memory dump of the process and saves it to a non-protected location.	6.6	More Details
CVE-2021-24345	The page lists-management feature of the Sendit WP Newsletter WordPress plugin through 2.5.1, available to Administrator users does not sanitise, validate or escape the id_lista POST parameter before using it in SQL statement, therefore leading to Blind SQL Injection.	6.6	More Details
CVE-2021-25393	Improper sanitization of incoming intent in SecSettings prior to SMR MAY-2021 Release 1 allows local attackers to get permissions to access system uid data.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3256	KuaiFanCMS V5.x contains an arbitrary file read vulnerability in the html_url parameter of the chakanhtml.module.php file.	6.5	More Details
CVE-2021-24360	The Yes/No Chart WordPress plugin before 1.0.12 did not sanitise its sid shortcode parameter before using it in a SQL statement, allowing medium privilege users (contributor+) to perform Blind SQL Injection attacks	6.5	More Details
CVE-2021-21439	DoS attack can be performed when an email contains specially designed URL in the body. It can lead to the high CPU usage and cause low quality of service, or in extreme case bring the system to a halt. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.26 and prior versions; 8.0.x version 8.0.13 and prior versions.	6.5	More Details
CVE-2021-22905	Nextcloud Android App (com.nextcloud.client) before v3.16.0 is vulnerable to information disclosure due to searches for sharees being performed by default on the lookup server instead of only using the local Nextcloud server unless a global search has been explicitly chosen by the user.	6.5	More Details
CVE-2021-22906	Nextcloud End-to-End Encryption before 1.5.3, 1.6.3 and 1.7.1 suffers from a denial of service vulnerability due to permitting any authenticated users to lock files of other users.	6.5	More Details
CVE-2021-22912	Nextcloud iOS before 3.4.2 suffers from an information disclosure vulnerability when searches for sharees utilize the lookup server by default instead of only on the local Nextcloud server unless a global search has been explicitly chosen by the user.	6.5	More Details
CVE-2021-25419	Non-compliance of recommended secure coding scheme in Samsung Internet prior to version 14.0.1.62 allows attackers to display fake URL in address bar via phising URL link.	6.5	More Details
CVE-2021-22913	Nextcloud Deck before 1.2.7, 1.4.1 suffers from an information disclosure vulnerability when searches for sharees utilize the lookup server by default instead of only the local Nextcloud server unless a global search has been explicitly chosen by the user.	6.5	More Details
CVE-2021-23136	Improper Authorization vulnerability in Gallagher Command Centre Server allows macro overrides to be performed by an unprivileged Command Centre Operator. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1359 (MR3); 8.20 versions prior to 8.20.1259 (MR5); version 8.10 and prior versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25416	Assuming EL1 is compromised, an improper address validation in RKP prior to SMR JUN-2021 Release 1 allows local attackers to create executable kernel page outside code area.	6.5	More Details
CVE-2021-34369	portlets/contact/ref/refContactDetail.do in Accela Civic Platform through 20.1 allows remote attackers to obtain sensitive information via a modified contactSeqNumber value. NOTE: the vendor states "the information that is being queried is authorized for an authenticated user of that application, so we consider this not applicable.	6.5	More Details
CVE-2021-0113	Out of bounds write in the BMC firmware for Intel(R) Server Board M10JNP2SB before version EFI BIOS 7215, BMC 8100.01.08 may allow an unauthenticated user to potentially enable a denial of service via adjacent access.	6.5	More Details
CVE-2021-0097	Path traversal in the BMC firmware for Intel(R) Server Board M10JNP2SB before version EFI BIOS 7215, BMC 8100.01.08 may allow an unauthenticated user to potentially enable a denial of service via adjacent access.	6.5	More Details
CVE-2020-24513	Domain-bypass transient execution vulnerability in some Intel Atom(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2020-24511	Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2021-0131	Use of cryptographically weak pseudo-random number generator (PRNG) in an API for the Intel(R) Security Library before version 3.3 may allow an authenticated user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2021-21735	A ZTE product has an information leak vulnerability. Due to improper permission settings, an attacker with ordinary user permissions could exploit this vulnerability to obtain some sensitive user information through the wizard page without authentication. This affects ZXHN H168N all versions up to V3.5.0_EG1T4_TE.	6.5	More Details
CVE-2021-21664	An incorrect permission check in Jenkins XebiaLabs XL Deploy Plugin 10.0.1 and earlier allows attackers with Generic Create permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing Username/password credentials stored in Jenkins.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0089	Observable response discrepancy in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2021-27635	SAP NetWeaver AS for JAVA, versions - 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker authenticated as an administrator to connect over a network and submit a specially crafted XML file in the application because of missing XML Validation, this vulnerability enables attacker to fully compromise confidentiality by allowing them to read any file on the filesystem or fully compromise availability by causing the system to crash. The attack cannot be used to change any data so that there is no compromise as to integrity.	6.5	More Details
CVE-2021-26194	An issue was discovered in JerryScript 2.4.0. There is a heap-use-after-free in ecma_is_lexical_environment in the ecma-helpers.c file.	6.5	More Details
CVE-2021-26197	An issue was discovered in JerryScript 2.4.0. There is a SEGV in main_print_unhandled_exception in main-utils.c file.	6.5	More Details
CVE-2021-26198	An issue was discovered in JerryScript 2.4.0. There is a SEVG in ecma_deref_bigint in ecma-helpers.c file.	6.5	More Details
CVE-2021-26199	An issue was discovered in JerryScript 2.4.0. There is a heap-use-after-free in ecma_bytecode_ref in ecma-helpers.c file.	6.5	More Details
CVE-2021-26997	E-Series SANtricity OS Controller Software 11.x versions prior to 11.70.1 are susceptible to a vulnerability which when successfully exploited could allow a remote attacker to discover information via error messaging which may aid in crafting more complex attacks.	6.5	More Details
CVE-2021-0086	Observable response discrepancy in floating-point operations for some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2021-25406	Information exposure vulnerability in Gear S Plugin prior to version 2.2.05.20122441 allows unstrusted applications to access connected BT device information.	6.5	More Details
CVE-2020-11266	Image address is dereferenced before validating its range which can cause potential QSEE information leakage in Snapdragon Wired Infrastructure and Networking	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8670	Race condition in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.4	More Details
CVE-2021-25395	A race condition in MFC charger driver prior to SMR MAY-2021 Release 1 allows local attackers to bypass signature check given a radio privilege is compromised.	6.4	More Details
CVE-2021-25394	A use after free vulnerability via race condition in MFC charger driver prior to SMR MAY-2021 Release 1 allows arbitrary write given a radio privilege is compromised.	6.4	More Details
CVE-2020-8704	Race condition in a subsystem in the Intel(R) LMS versions before 2039.1.0.0 may allow a privileged user to potentially enable escalation of privilege via local access.	6.4	More Details
CVE-2021-21473	SAP NetWeaver AS ABAP and ABAP Platform, versions - 700, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, contains function module SRM_RFC_SUBMIT_REPORT which fails to validate authorization of an authenticated user thus allowing an unauthorized user to execute reports in SAP NetWeaver ABAP Platform.	6.3	More Details
CVE-2021-27887	Cross-site Scripting (XSS) vulnerability in the main dashboard of Ellipse APM versions allows an authenticated user or integrated application to inject malicious data into the application that can then be executed in a victim’s browser. This issue affects: Hitachi ABB Power Grids Ellipse APM 5.3 version 5.3.0.1 and prior versions; 5.2 version 5.2.0.3 and prior versions; 5.1 version 5.1.0.6 and prior versions.	6.3	More Details
CVE-2021-32684	magento-scripts contains scripts and configuration used by Create Magento App, a zero-configuration tool-chain which allows one to deploy Magento 2. In versions 1.5.1 and 1.5.2, after changing the function from synchronous to asynchronous there wasn't implemented handler in the start, stop, exec, and logs commands, effectively making them unusable. Version 1.5.3 contains patches for the problems.	6.2	More Details
CVE-2021-21490	SAP NetWeaver AS for ABAP (Web Survey), versions - 700, 702, 710, 711, 730, 731, 750, 750, 752, 75A, 75F, does not sufficiently encode input and output parameters which results in reflected cross site scripting vulnerability, through which a malicious user can access data relating to the current session and use it to impersonate a user and access all information with the same rights as the target user.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30133	A cross-site scripting (XSS) vulnerability in CloverDX Server 5.9.0, CloverDX 5.8.1, CloverDX 5.7.0, and earlier allows remote attackers to inject arbitrary web script or HTML via the sessionToken parameter of multiple methods in Simple HTTP API. This is resolved in 5.9.1 and 5.10.	6.1	More Details
CVE-2021-21555	Dell PowerEdge R640, R740, R740XD, R840, R940, R940xa, MX740c, MX840c, and T640 Server BIOS contain a heap-based buffer overflow vulnerability in systems with NVDIMM-N installed. A local malicious user with high privileges may potentially exploit this vulnerability, leading to a denial of Service, arbitrary code execution, or information disclosure in UEFI or BIOS Preboot Environment.	6.1	More Details
CVE-2020-13688	Cross-site scripting vulnerability in l Drupal Core allows an attacker could leverage the way that HTML is rendered for affected forms in order to exploit the vulnerability. This issue affects: Drupal Core 8.8.X versions prior to 8.8.10; 8.9.X versions prior to 8.9.6; 9.0.X versions prior to 9.0.6.	6.1	More Details
CVE-2021-21556	Dell PowerEdge R640, R740, R740XD, R840, R940, R940xa, MX740c, MX840c, and T640 Server BIOS contain a stack-based buffer overflow vulnerability in systems with NVDIMM-N installed. A local malicious user with high privileges may potentially exploit this vulnerability, leading to a denial of Service, arbitrary code execution, or information disclosure in UEFI or BIOS Preboot Environment.	6.1	More Details
CVE-2021-24351	The theplus_more_post AJAX action of The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.12 did not properly sanitise some of its fields, leading to a reflected Cross-Site Scripting (exploitable on both unauthenticated and authenticated users)	6.1	More Details
CVE-2021-24350	The Visitors WordPress plugin through 0.3 is affected by an Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability. The plugin would display the user's user agent string without validation or encoding within the WordPress admin panel.	6.1	More Details
CVE-2021-21666	Jenkins Kiuwan Plugin 1.6.0 and earlier does not escape query parameters in an error message for a form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-34370	Accela Civic Platform through 20.1 allows ssoAdapter/logoutAction.do successURL XSS. NOTE: the vendor states "there are configurable security flags and we are unable to reproduce them with the available information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22903	The actionpack ruby gem before 6.1.3.2 suffers from a possible open redirect vulnerability. Specially crafted Host headers in combination with certain "allowed host" formats can cause the Host Authorization middleware in Action Pack to redirect users to a malicious website. This is similar to CVE-2021-22881. Strings in config.hosts that do not have a leading dot are converted to regular expressions without proper escaping. This causes, for example, `config.hosts << "sub.example.com"` to permit a request with a Host header value of `sub-example.com`.	6.1	More Details
CVE-2021-33829	A cross-site scripting (XSS) vulnerability in the HTML Data Processor in CKEditor 4 4.14.0 through 4.16.x before 4.16.1 allows remote attackers to inject executable JavaScript code through a crafted comment because --!> is mishandled.	6.1	More Details
CVE-2021-24349	This Gallery from files WordPress plugin through 1.6.0 gives the functionality of uploading images to the server. But filenames are not properly sanitized before being output in an error message when they have an invalid extension, leading to a reflected Cross-Site Scripting issue. Due to the lack of CSRF check, the attack could also be performed via such vector.	6.1	More Details
CVE-2020-21316	A Cross-site scripting (XSS) vulnerability exists in the comment section in ZrLog 2.1.3, which allows remote attackers to inject arbitrary web script and stolen administrator cookies via the nickname parameter and gain access to the admin panel.	6.1	More Details
CVE-2021-33666	When SAP Commerce Cloud version 100, hosts a JavaScript storefront, it is vulnerable to MIME sniffing, which, in certain circumstances, could be used to facilitate an XSS attack or malware proliferation.	6.1	More Details
CVE-2019-25046	The Web Client in Cerberus FTP Server Enterprise before 10.0.19 and 11.x before 11.0.4 allows XSS via an SVG document.	6.1	More Details
CVE-2021-24358	The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.10 did not validate a redirect parameter on a specifically crafted URL before redirecting the user to it, leading to an Open Redirect issue.	6.1	More Details
CVE-2021-34540	Advantech WebAccess 8.4.2 and 8.4.4 allows XSS via the username column of the bwRoot.asp page of WADashboard.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20293	A reflected Cross-Site Scripting (XSS) flaw was found in RESTEasy in all versions of RESTEasy up to 4.6.0.Final, where it did not properly handle URL encoding when calling @javax.ws.rs.PathParam without any @Produces MediaType. This flaw allows an attacker to launch a reflected XSS attack. The highest threat from this vulnerability is to data confidentiality and integrity.	6.1	More Details
CVE-2021-34364	The Refined GitHub browser extension before 21.6.8 might allow XSS via a link in a document. NOTE: github.com sends Content-Security-Policy headers to, in general, address XSS and other concerns.	6.1	More Details
CVE-2021-29049	Cross-site scripting (XSS) vulnerability in the Portal Workflow module's edit process page in Liferay DXP 7.0 before fix pack 99, 7.1 before fix pack 23, 7.2 before fix pack 12 and 7.3 before fix pack 1, allows remote attackers to inject arbitrary web script or HTML via the currentURL parameter.	6.1	More Details
CVE-2021-21554	Dell PowerEdge R640, R740, R740XD, R840, R940, R940xa, MX740c, MX840c, and, Dell Precision 7920 Rack Workstation BIOS contain a stack-based buffer overflow vulnerability in systems with Intel Optane DC Persistent Memory installed. A local malicious user with high privileges may potentially exploit this vulnerability, leading to a denial of Service, arbitrary code execution, or information disclosure in UEFI or BIOS Preboot Environment.	6.1	More Details
CVE-2021-23211	Cleartext Storage of Sensitive Information in Memory vulnerability in Gallagher Command Centre Server allows Cloud end-to-end encryption key to be discoverable in server memory dumps. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3).	6.0	More Details
CVE-2021-23182	Cleartext Storage of Sensitive Information in Memory vulnerability in Gallagher Command Centre Server allows OSDP reader master keys to be discoverable in server memory dumps. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); All versions of 8.30.	6.0	More Details
CVE-2021-27627	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method ChartInterpreter::DoIt() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27626	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CMiniXMLParser::Parse() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details
CVE-2021-27625	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method IgsData::freeMemory() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details
CVE-2021-27634	SAP NetWeaver AS for ABAP (RFC Gateway), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method ThCpicDtCreate () causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details
CVE-2021-27624	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CiXMLIStreamRawBuffer::readRaw () which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details
CVE-2021-27623	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CXmlUtility::CheckLength() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27622	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CDrawRaster::LoadImageFromMemory() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details
CVE-2021-22895	Nextcloud Desktop Client before 3.3.1 is vulnerable to improper certificate validation due to lack of SSL certificate verification when using the "Register with a Provider" flow.	5.9	More Details
CVE-2021-27620	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method Ups::AddPart() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	5.9	More Details
CVE-2021-20732	The ATOM (ATOM - Smart life App for Android versions prior to 1.8.1 and ATOM - Smart life App for iOS versions prior to 1.8.2) does not verify server certificate properly, which allows man-in-the-middle attackers to eavesdrop on encrypted communication via a crafted certificate.	5.9	More Details
CVE-2021-0129	Improper access control in BlueZ may allow an authenticated user to potentially enable information disclosure via adjacent access.	5.7	More Details
CVE-2021-0484	In readVector of IMediaPlayer.cpp, there is a possible read of uninitialized heap data due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-173720767	5.5	More Details
CVE-2020-12290	Improper access control in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28687	HVM soft-reset crashes toolstack libxl requires all data structures passed across its public interface to be initialized before use and disposed of afterwards by calling a specific set of functions. Many internal data structures also require this initialize / dispose discipline, but not all of them. When the "soft reset" feature was implemented, the libxl__domain_suspend_state structure didn't require any initialization or disposal. At some point later, an initialization function was introduced for the structure; but the "soft reset" path wasn't refactored to call the initialization function. When a guest nwo initiates a "soft reboot", uninitialized data structure leads to an assert() when later code finds the structure in an unexpected state. The effect of this is to crash the process monitoring the guest. How this affects the system depends on the structure of the toolstack. For xl, this will have no security-relevant effect: every VM has its own independent monitoring process, which contains no state. The domain in question will hang in a crashed state, but can be destroyed by `xl destroy` just like any other non-cooperating domain. For daemon-based toolstacks linked against libxl, such as libvirt, this will crash the toolstack, losing the state of any in-progress operations (localized DoS), and preventing further administrator operations unless the daemon is configured to restart automatically (system-wide DoS). If crashes "leak" resources, then repeated crashes could use up resources, also causing a system-wide DoS.	5.5	More Details
CVE-2020-12291	Uncontrolled resource consumption in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-0480	In createPendingIntent of SnoozeHelper.java, there is a possible broadcast intent containing a sensitive identifier. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-174493336	5.5	More Details
CVE-2021-25423	Improper log management vulnerability in Watch Active2 PlugIn prior to 2.2.08.21033151 version allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone via log.	5.5	More Details
CVE-2020-12292	Improper conditions check in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-13938	Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25415	Assuming EL1 is compromised, an improper address validation in RKP prior to SMR JUN-2021 Release 1 allows local attackers to remap EL2 memory as writable.	5.5	More Details
CVE-2020-24475	Improper initialization in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.48.ce3e3bd2 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-25420	Improper log management vulnerability in Galaxy Watch PlugIn prior to version 2.2.05.21033151 allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log.	5.5	More Details
CVE-2021-25421	Improper log management vulnerability in Galaxy Watch3 PlugIn prior to version 2.2.09.21033151 allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log.	5.5	More Details
CVE-2020-12987	A heap information leak/kernel pool address disclosure vulnerability in the AMD Graphics Driver for Windows 10 may lead to KASLR bypass.	5.5	More Details
CVE-2021-25422	Improper log management vulnerability in Watch Active PlugIn prior to version 2.2.07.21033151 allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log.	5.5	More Details
CVE-2020-25467	A null pointer dereference was discovered lzo_decompress_buf in stream.c in lrzip 0.621 which allows an attacker to cause a denial of service (DOS) via a crafted compressed file.	5.5	More Details
CVE-2020-24486	Improper input validation in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-31811	In Apache PDFBox, a carefully crafted PDF file can trigger an OutOfMemory-Exception while loading the file. This issue affects Apache PDFBox version 2.0.23 and prior 2.0.x versions.	5.5	More Details
CVE-2021-31812	In Apache PDFBox, a carefully crafted PDF file can trigger an infinite loop while loading the file. This issue affects Apache PDFBox version 2.0.23 and prior 2.0.x versions.	5.5	More Details
CVE-2021-25413	Improper sanitization of incoming intent in Samsung Contacts prior to SMR JUN-2021 Release 1 allows local attackers to get permissions to access arbitrary data with Samsung Contacts privilege.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12296	Uncontrolled resource consumption in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-12295	Improper input validation in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-12294	Insufficient control flow management in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-12293	Improper control of a resource through its lifetime in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-12289	Out-of-bounds write in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-26314	Potential floating point value injection in all supported CPU products, in conjunction with software vulnerabilities relating to speculative execution with incorrect floating point results, may cause the use of incorrect data from FPVI and may result in data leakage.	5.5	More Details
CVE-2021-33659	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28689	x86: Speculative vulnerabilities with bare (non-shim) 32-bit PV guests 32-bit x86 PV guest kernels run in ring 1. At the time when Xen was developed, this area of the i386 architecture was rarely used, which is why Xen was able to use it to implement paravirtualisation, Xen's novel approach to virtualization. In AMD64, Xen had to use a different implementation approach, so Xen does not use ring 1 to support 64-bit guests. With the focus now being on 64-bit systems, and the availability of explicit hardware support for virtualization, fixing speculation issues in ring 1 is not a priority for processor companies. Indirect Branch Restricted Speculation (IBRS) is an architectural x86 extension put together to combat speculative execution sidechannel attacks, including Spectre v2. It was retrofitted in microcode to existing CPUs. For more details on Spectre v2, see: http://xenbits.xen.org/xsa/advisory-254.html However, IBRS does not architecturally protect ring 0 from predictions learnt in ring 1. For more details, see: https://software.intel.com/security-software-guidance/deep-dives/deep-dive-indirect-branch-restricted-speculation Similar situations may exist with other mitigations for other kinds of speculative execution attacks. The situation is quite likely to be similar for speculative execution attacks which have yet to be discovered, disclosed, or mitigated.	5.5	More Details
CVE-2021-26313	Potential speculative code store bypass in all supported CPU products, in conjunction with software vulnerabilities relating to speculative execution of overwritten instructions, may cause an incorrect speculation and could result in data leakage.	5.5	More Details
CVE-2021-28858	TP-Link's TL-WPA4220 4.0.2 Build 20180308 Rel.37064 does not use SSL by default. Attacker on the local network can monitor traffic and capture the cookie and other sensitive information.	5.5	More Details
CVE-2021-25405	An improper access control vulnerability in ScreenOffActivity in Samsung Notes prior to version 4.2.04.27 allows untrusted applications to access local files.	5.5	More Details
CVE-2020-11265	Information disclosure issue due to lack of validation of pointer arguments passed to TZ BSP in Snapdragon Wired Infrastructure and Networking	5.5	More Details
CVE-2021-27347	Use after free in lzma_decompress_buf function in stream.c in lrzip 0.631 allows attackers to cause Denial of Service (DoS) via a crafted compressed file.	5.5	More Details
CVE-2021-27345	A null pointer dereference was discovered in ucompthread in stream.c in lrzip 0.631 which allows attackers to cause a denial of service (DOS) via a crafted compressed file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27638	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated JT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2021-27639	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated JT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2021-27640	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PSD file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2021-27641	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2021-27642	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2021-27643	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2021-33660	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FLI file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33661	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2020-12288	Protection mechanism failure in some Intel(R) Thunderbolt(TM) controllers may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-34693	net/can/bcm.c in the Linux kernel through 5.12.10 allows local users to obtain sensitive information from kernel stack memory because parts of a data structure are uninitialized.	5.5	More Details
CVE-2019-9475	In /proc/net of the kernel filesystem, there is a possible information leak 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-10Android ID: A-9496886	5.5	More Details
CVE-2021-24382	The Smart Slider 3 Free and pro WordPress plugins before 3.5.0.9 did not sanitise the Project Name before outputting it back in the page, leading to a Stored Cross-Site Scripting issue. By default, only administrator users could access the affected functionality, limiting the exploitability of the vulnerability. However, some WordPress admins may allow lesser privileged users to access the plugin's functionality, in which case, privilege escalation could be performed.	5.4	More Details
CVE-2020-15385	Brocade SANnav before version 2.1.1 allows an authenticated attacker to list directories, and list files without permission. As a result, users without permission can see folders, and hidden files, and can create directories without permission.	5.4	More Details
CVE-2021-27615	SAP Manufacturing Execution versions - 15.1, 1.5.2, 15.3, 15.4, does not contain some HTTP security headers in their HTTP response. The lack of these headers in response can be exploited by the attacker to execute Cross-Site Scripting (XSS) attacks.	5.4	More Details
CVE-2020-5000	IBM Financial Transaction Manager 3.2.0 through 3.2.8 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: 192952.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29215	A Cross Site Scripting in SourceCodester Employee Management System 1.0 allows the user to execute alert messages via /Employee Management System/addemp.php on admin account.	5.4	More Details
CVE-2021-26829	OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows allows stored XSS via system_settings.shtm.	5.4	More Details
CVE-2021-23393	This affects the package Flask-Unchained before 0.9.0. When using the the _validate_redirect_url function, it is possible to bypass URL validation and redirect a user to an arbitrary URL by providing multiple back slashes such as \\\evil.com/path. This vulnerability is only exploitable if an alternative WSGI server other than Werkzeug is used, or the default behaviour of Werkzeug is modified using 'autocorrect_location_header=False.	5.4	More Details
CVE-2021-24357	In the Best Image Gallery & Responsive Photo Gallery – FooGallery WordPress plugin before 2.0.35, the Custom CSS field of each gallery is not properly sanitised or validated before being being output in the page where the gallery is embed, leading to a stored Cross-Site Scripting issue.	5.4	More Details
CVE-2020-24668	Trace Financial Crest Bridge <6.3.0.02 contains a stored XSS vulnerability, which was fixed in 6.3.0.03.	5.4	More Details
CVE-2021-24346	The Stock in & out WordPress plugin through 1.0.4 has a search functionality, the lowest accessible level to it being contributor. The srch POST parameter is not validated, sanitised or escaped before using it in the echo statement, leading to a reflected XSS issue	5.4	More Details
CVE-2020-24662	SmartStream Transaction Lifecycle Management (TLM) Reconciliation Premium (RP) <3.1.0 allows XSS. This was fixed in TLM RP 3.1.0.	5.4	More Details
CVE-2021-33665	SAP NetWeaver Application Server ABAP (Applications based on SAP GUI for HTML), versions - KRNL64NUC - 7.49, KRNL64UC - 7.49,7.53, KERNEL - 7.49,7.53,7.77,7.81,7.84, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-24663	Trace Financial CRESTBridge <6.3.0.02 contains a stored XSS vulnerability, which was fixed in 6.3.0.03.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33664	SAP NetWeaver Application Server ABAP (Applications based on Web Dynpro ABAP), versions - SAP_UI - 750,752,753,754,755, SAP_BASIS - 702, 731 does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2021-24359	The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.11 did not properly check that a user requesting a password reset was the legitimate user, allowing an attacker to send an arbitrary reset password email to a registered user on behalf of the WordPress site. Such issue could be chained with an open redirect (CVE-2021-24358) in version below 4.1.10, to include a crafted password reset link in the email, which would lead to an account takeover.	5.3	More Details
CVE-2021-28169	For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, it is possible for requests to the ConcatServlet with a doubly encoded path to access protected resources within the WEB-INF directory. For example a request to `/concat?/%2557EB-INF/web.xml` can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.	5.3	More Details
CVE-2020-15384	Brocade SANNav before version 2.1.1 contains an information disclosure vulnerability. Successful exploitation of internal server information in the initial login response header.	5.3	More Details
CVE-2020-15378	The OVA version of Brocade SANnav before version 2.1.1 installation with IPv6 networking exposes the docker container ports to the network, increasing the potential attack surface.	5.3	More Details
CVE-2020-15386	Brocade Fabric OS prior to v9.0.1a and 8.2.3a and after v9.0.0 and 8.2.2d may observe high CPU load during security scanning, which could lead to a slower response to CLI commands and other operations.	5.3	More Details
CVE-2021-33663	SAP NetWeaver AS ABAP, versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83,7.84, allows an unauthorized attacker to insert cleartext commands due to improper restriction of I/O buffering into encrypted SMTP sessions over the network which can partially impact the integrity of the application.	5.3	More Details
CVE-2021-20728	Improper access control vulnerability in goo blog App for Android ver.1.2.25 and earlier and for iOS ver.1.3.3 and earlier allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30641	Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'	5.3	More Details
CVE-2021-22749	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Modicon X80 BMXNOR0200H RTU SV1.70 IR22 and prior that could cause information leak concerning the current RTU configuration including communication parameters dedicated to telemetry, when a specially crafted HTTP request is sent to the web server of the module.	5.3	More Details
CVE-2021-22897	curl 7.61.0 through 7.76.1 suffers from exposure of data element to wrong session due to a mistake in the code for CURLOPT_SSL_CIPHER_LIST when libcurl is built to use the Schannel TLS library. The selected cipher set was stored in a single "static" variable in the library, which has the surprising side-effect that if an application sets up multiple concurrent transfers, the last one that sets the ciphers will accidentally control the set used by all transfers. In a worst-case scenario, this weakens transport security significantly.	5.3	More Details
CVE-2021-26993	E-Series SANtricity OS Controller Software 11.x versions prior to 11.70.1 are susceptible to a vulnerability which when successfully exploited could allow a remote attacker to cause a partial Denial of Service (DoS) to the web server.	5.3	More Details
CVE-2019-17567	Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.	5.3	More Details
CVE-2021-22764	A CWE-287: Improper Authentication vulnerability exists in PowerLogic PM55xx, PowerLogic PM8ECC, PowerLogic EGX100 and PowerLogic EGX300 (see security notification for version infromation) that could cause loss of connectivity to the device via Modbus TCP protocol when an attacker sends a specially crafted HTTP request.	5.3	More Details
CVE-2021-25425	Improper check vulnerability in Samsung Health prior to version 6.17 allows attacker to read internal cache data via exported component.	5.3	More Details
CVE-2021-32557	It was discovered that the process_report() function in data/whoopsie-upload-all allowed arbitrary file writes via symlinks.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31832	Improper Neutralization of Input in the ePO administrator extension for McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.200 allows a remote ePO DLP administrator to inject JavaScript code into the alert configuration text field. This JavaScript will be executed when an end user triggers a DLP policy on their machine.	5.2	More Details
CVE-2021-0132	Missing release of resource after effective lifetime in an API for the Intel(R) Security Library before version 3.3 may allow a privileged user to potentially enable denial of service via network access.	4.9	More Details
CVE-2021-0134	Improper input validation in an API for the Intel(R) Security Library before version 3.3 may allow a privileged user to potentially enable denial of service via network access.	4.9	More Details
CVE-2021-23852	An authenticated attacker with administrator rights Bosch IP cameras can call an URL with an invalid parameter that causes the camera to become unresponsive for a few seconds and cause a Denial of Service (DoS).	4.9	More Details
CVE-2021-27621	Information Disclosure vulnerability in UserAdmin application in SAP NetWeaver Application Server for Java, versions - 7.11,7.20,7.30,7.31,7.40 and 7.50 allows attackers to access restricted information by entering malicious server name.	4.9	More Details
CVE-2021-31839	Improper privilege management vulnerability in McAfee Agent for Windows prior to 5.7.3 allows a local user to modify event information in the MA event folder. This allows a local user to either add false events or remove events from the event logs prior to them being sent to the ePO server.	4.8	More Details
CVE-2021-0001	Observable timing discrepancy in Intel(R) IPP before version 2020 update 1 may allow authorized user to potentially enable information disclosure via local access.	4.7	More Details
CVE-2021-27637	Under certain conditions SAP Enable Now (SAP Workforce Performance Builder - Manager), versions - 1.0, 10 allows an attacker to access information which would otherwise be restricted leading to information disclosure.	4.6	More Details
CVE-2021-34557	XScreenSaver 5.45 can be bypassed if the machine has more than ten disconnectable video outputs. A buffer overflow in update_screen_layout() allows an attacker to bypass the standard screen lock authentication mechanism by crashing XScreenSaver. The attacker must physically disconnect many video outputs.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24507	Improper initialization in a subsystem in the Intel(R) CSME versions before 11.8.86, 11.12.86, 11.22.86, 12.0.81, 13.0.47, 13.30.17, 14.1.53, 14.5.32, 13.50.11 and 15.0.22 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2020-24506	Out of bound read in a subsystem in the Intel(R) CSME versions before 12.0.81, 13.0.47, 13.30.17, 14.1.53 and 14.5.32 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2021-33662	Under certain conditions, the installation of SAP Business One, version - 10.0, discloses sensitive information on the file system allowing an attacker to access information which would otherwise be restricted.	4.4	More Details
CVE-2021-0095	Improper initialization in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2020-12358	Out of bounds write in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2021-0051	Improper input validation in the Intel(R) SPS versions before SPS_E5_04.04.04.023.0, SPS_E5_04.04.03.228.0 or SPS_SoC-A_05.00.03.098.0 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2021-25411	Improper address validation vulnerability in RKP api prior to SMR JUN-2021 Release 1 allows root privileged local attackers to write read-only kernel memory.	4.4	More Details
CVE-2021-31927	An Insecure Direct Object Reference (IDOR) vulnerability in Annex Cloud Loyalty Experience Platform <2021.1.0.1 allows any authenticated attacker to modify any existing user, including users assigned to different environments and clients. It was fixed in v2021.1.0.2.	4.3	More Details
CVE-2021-21663	A missing permission check in Jenkins XebiaLabs XL Deploy Plugin 7.5.8 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing Username/password credentials stored in Jenkins.	4.3	More Details
CVE-2021-22896	Nextcloud Mail before 1.9.5 suffers from improper access control due to a missing permission check allowing other authenticated users to create mail aliases for other users.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24355	In the Simple 301 Redirects by BetterLinks WordPress plugin before 2.0.4, the lack of capability checks and insufficient nonce check on the AJAX actions, simple301redirects/admin/get_wildcard and simple301redirects/admin/wildcard, made it possible for authenticated users to retrieve and update the wildcard value for redirects.	4.3	More Details
CVE-2021-22769	A CWE-552: Files or Directories Accessible to External Parties vulnerability exists in Easergy T300 with firmware V2.7.1 and older that could expose files or directory content when access from an attacker is not restricted or incorrectly restricted.	4.3	More Details
CVE-2021-34547	PRTG Network Monitor 20.1.55.1775 allows /editsettings CSRF for user account creation.	4.3	More Details
CVE-2021-20730	Improper access control vulnerability in WSR-1166DHP3 firmware Ver.1.16 and prior and WSR-1166DHP4 firmware Ver.1.02 and prior allows an attacker to obtain configuration information via unspecified vectors.	4.3	More Details
CVE-2021-31929	Annex Cloud Loyalty Experience Platform <2021.1.0.1 allows any authenticated attacker to modify loyalty campaigns and settings, such as fraud prevention, coupon groups, email templates, or referrals.	4.3	More Details
CVE-2021-21661	Jenkins Kubernetes CLI Plugin 1.10.0 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2021-21662	A missing permission check in Jenkins XebiaLabs XL Deploy Plugin 10.0.1 and earlier allows attackers with Overall/Read permission to enumerate credentials ID of credentials stored in Jenkins.	4.3	More Details
CVE-2021-25390	Intent redirection vulnerability in PhotoTable prior to SMR MAY-2021 Release 1 allows attackers to execute privileged action.	4.0	More Details
CVE-2021-25391	Intent redirection vulnerability in Secure Folder prior to SMR MAY-2021 Release 1 allows attackers to execute privileged action.	4.0	More Details
CVE-2021-25392	Improper protection of backup path configuration in Samsung Dex prior to SMR MAY-2021 Release 1 allows local attackers to get sensitive information via changing the path.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3595	An invalid pointer initialization issue was found in the SLiRP networking implementation of QEMU. The flaw exists in the tftp_input() function and could occur while processing a udp packet that is smaller than the size of the 'tftp_t' structure. This issue may lead to out-of-bounds read access or indirect host memory disclosure to the guest. The highest threat from this vulnerability is to data confidentiality. This flaw affects libslirp versions prior to 4.6.0.	3.8	More Details
CVE-2021-3039	An information exposure through log file vulnerability exists in the Palo Alto Networks Prisma Cloud Compute Console where a secret used to authorize the role of the authenticated user is logged to a debug log file. Authenticated Operator role and Auditor role users with access to the debug log files can use this secret to gain Administrator role access for their active session in Prisma Cloud Compute. Prisma Cloud Compute SaaS versions were automatically upgraded to the fixed release. This issue impacts all Prisma Cloud Compute versions earlier than Prisma Cloud Compute 21.04.412.	3.8	More Details
CVE-2021-3594	An invalid pointer initialization issue was found in the SLiRP networking implementation of QEMU. The flaw exists in the udp_input() function and could occur while processing a udp packet that is smaller than the size of the 'udphdr' structure. This issue may lead to out-of-bounds read access or indirect host memory disclosure to the guest. The highest threat from this vulnerability is to data confidentiality. This flaw affects libslirp versions prior to 4.6.0.	3.8	More Details
CVE-2021-32556	It was discovered that the get_modified_conffiles() function in backends/packaging-apt-dpkg.py allowed injecting modified package names in a manner that would confuse the dpkg(1) call.	3.8	More Details
CVE-2021-3593	An invalid pointer initialization issue was found in the SLiRP networking implementation of QEMU. The flaw exists in the udp6_input() function and could occur while processing a udp packet that is smaller than the size of the 'udphdr' structure. This issue may lead to out-of-bounds read access or indirect host memory disclosure to the guest. The highest threat from this vulnerability is to data confidentiality. This flaw affects libslirp versions prior to 4.6.0.	3.8	More Details
CVE-2021-3592	An invalid pointer initialization issue was found in the SLiRP networking implementation of QEMU. The flaw exists in the bootp_input() function and could occur while processing a udp packet that is smaller than the size of the 'bootp_t' structure. A malicious guest could use this flaw to leak 10 bytes of uninitialized heap memory from the host. The highest threat from this vulnerability is to data confidentiality. This flaw affects libslirp versions prior to 4.6.0.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34682	Receita Federal IRPF 2021 1.7 allows a man-in-the-middle attack against the update feature.	3.7	More Details
CVE-2020-24512	Observable timing discrepancy in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2021-20396	IBM QRadar Analyst Workflow App 1.0 through 1.18.0 for IBM QRadar SIEM allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 196009.	3.3	More Details
CVE-2021-25403	Intent redirection vulnerability in Samsung Account prior to version 10.8.0.4 in Android P(9.0) and below, and 12.2.0.9 in Android Q(10.0) and above allows attacker to access contacts and file provider using SettingWebView component.	3.3	More Details
CVE-2021-25398	Intent redirection vulnerability in Bixby Voice prior to version 3.1.12 allows attacker to access contacts.	3.3	More Details
CVE-2021-3588	The cli_feat_read_cb() function in src/gatt-database.c does not perform bounds checks on the 'offset' variable before using it as an index into an array for reading.	3.3	More Details
CVE-2021-25402	Information Exposure vulnerability in Samsung Notes prior to version 4.2.04.27 allows attacker to access s pen latency information.	3.3	More Details
CVE-2021-25404	Information Exposure vulnerability in SmartThings prior to version 1.7.64.21 allows attacker to access user information via log.	3.3	More Details
CVE-2021-31498	This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 DWF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12744.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31501	This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13310.	3.3	More Details
CVE-2021-33031	In LabCup before <v2_next_18022, it is possible to use the save API to perform unauthorized actions for users without access to user management in order to, after successful exploitation, gain access to a victim's account. A user without the user-management privilege can change another user's email address if the attacker knows details of the victim such as the exact roles and group roles, ID, and remote authentication ID settings. These must be sent in a modified save API request. It was fixed in 6.3.0.03.	3.1	More Details
CVE-2021-28801	An out-of-bounds read vulnerability has been reported to affect certain QNAP switches running QSS. If exploited, this vulnerability allows attackers to read sensitive information on the system. This issue affects: QNAP Systems Inc. QSS versions prior to 1.0.2 build 20210122 on QSW-M2108-2C; versions prior to 1.0.2 build 20210122 on QSW-M2108-2S; versions prior to 1.0.2 build 20210122 on QSW-M2108R-2C.	3.1	More Details
CVE-2021-22898	curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.	3.1	More Details
CVE-2021-25409	Improper access in Notification setting prior to SMR JUN-2021 Release 1 allows physically proximate attackers to set arbitrary notification via physically configuring device.	2.4	More Details
CVE-2021-25389	Improper running task check in S Secure prior to SMR MAY-2021 Release 1 allows attackers to use locked app without authentication.	2.3	More Details
CVE-2021-3525	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-3913	Rejected reason: 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-2017-3914	Rejected reason: 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-2017-3915	Rejected reason: 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-2017-3916	Rejected reason: 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-2020-13002	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12995	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2017-3919	Rejected reason: 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-2017-3918	Rejected reason: 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-2017-3917	Rejected reason: 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-2020-12989	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2020-12990	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12991	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12992	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2017-3911	Rejected reason: 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-2020-12993	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12994	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12996	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12997	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12998	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12999	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13000	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2020-13001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13006	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-13007	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2017-3925	Rejected reason: 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-2020-6000	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2017-3910	Rejected reason: 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-2017-3909	Rejected reason: 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-2017-3901	Rejected reason: 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-2017-3900	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2017-1080	Rejected reason: 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-2017-1079	Rejected reason: 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-2017-1078	Rejected reason: 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-2017-1077	Rejected reason: 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-2017-1076	Rejected reason: 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-2017-1075	Rejected reason: 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-2017-1074	Rejected reason: 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-2017-1073	Rejected reason: 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-2017-1072	Rejected reason: 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-2017-1071	Rejected reason: 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-2017-1070	Rejected reason: 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-2021-3533	Rejected reason: This vulnerability does not meet the criteria for a security vulnerability	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3532	Rejected reason: This CVE is marked as INVALID and not a bug	N/A	More Details
CVE-2017-3903	Rejected reason: 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-2017-3905	Rejected reason: 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-2017-3906	Rejected reason: 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-2017-3920	Rejected reason: 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-2020-6006	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6002	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5999	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2017-3908	Rejected reason: 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-2020-5998	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5997	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5996	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5995	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5994	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5993	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12984	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2017-3921	Rejected reason: 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-2017-3926	Rejected reason: 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-2017-5742	Rejected reason: 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-2017-5744	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2017-5745	Rejected reason: 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-2017-5746	Rejected reason: 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-2017-5747	Rejected reason: 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-2017-5748	Rejected reason: 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-2017-5749	Rejected reason: 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-2017-5750	Rejected reason: 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-2017-5751	Rejected reason: 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-2017-5752	Rejected reason: 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-2017-5755	Rejected reason: 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-2017-5756	Rejected reason: 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-2017-5757	Rejected reason: 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-2017-5758	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2017-5759	Rejected reason: 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-2017-5760	Rejected reason: 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-2017-5761	Rejected reason: 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-2017-5762	Rejected reason: 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-2017-5763	Rejected reason: 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-2017-5764	Rejected reason: 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-2017-5765	Rejected reason: 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-2017-5779	Rejected reason: 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-2017-3923	Rejected reason: 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-2005-2493	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2005. Notes: none	N/A	More Details
CVE-2008-0885	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2008. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2008-1239	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2008. Notes: none	N/A	More Details
CVE-2008-2660	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2008. Notes: none	N/A	More Details
CVE-2009-0785	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2017-5743	Rejected reason: 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-2017-5741	Rejected reason: 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-2009-3893	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2017-5740	Rejected reason: 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-2017-3927	Rejected reason: 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-2017-3928	Rejected reason: 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-2017-3932	Rejected reason: 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-2017-3924	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2017-3937	Rejected reason: 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-2017-3970	Rejected reason: 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-2017-3988	Rejected reason: 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-2017-3996	Rejected reason: 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-2017-4036	Rejected reason: 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-2017-4050	Rejected reason: 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-2017-4051	Rejected reason: 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-2017-5680	Rejected reason: 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-2017-5687	Rejected reason: 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-2017-5690	Rejected reason: 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-2017-5702	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2017-5713	Rejected reason: 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-2017-5714	Rejected reason: 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-2017-5718	Rejected reason: 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-2017-5720	Rejected reason: 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-2017-5723	Rejected reason: 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-2017-5724	Rejected reason: 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-2017-5725	Rejected reason: 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-2017-5726	Rejected reason: 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-2017-5728	Rejected reason: 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-2017-5730	Rejected reason: 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-2017-5737	Rejected reason: 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-2017-5739	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2009-2900	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2017-3922	Rejected reason: 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-2020-12979	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12909	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12913	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12914	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12915	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12916	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12917	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12919	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12921	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12922	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2020-12923	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12924	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12925	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12935	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12936	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12941	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12957	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12959	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12968	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12969	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12970	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12971	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2020-12972	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12973	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12974	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12975	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12976	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12977	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12978	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12910	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-12906	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2009-4278	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2020-12896	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2009-4279	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4280	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4281	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4282	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4283	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4284	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4285	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4286	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4287	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4288	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4289	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2009-4290	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2009-4291	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details
CVE-2017-3904	Rejected reason: 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-2017-5766	Rejected reason: 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-2017-5767	Rejected reason: 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-2017-5768	Rejected reason: 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-2017-5769	Rejected reason: 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-2017-5770	Rejected reason: 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-2017-5771	Rejected reason: 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-2017-5772	Rejected reason: 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-2017-5773	Rejected reason: 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 Number	Description	Base Score	Reference
CVE-2017-5774	Rejected reason: 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-2017-5775	Rejected reason: 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-2017-5776	Rejected reason: 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-2017-5777	Rejected reason: 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-2017-5778	Rejected reason: 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-2009-4277	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2009. Notes: none	N/A	More Details