SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 February 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-2021-25311	condor_credd in HTCondor before 8.9.11 allows Directory Traversal outside the SEC_CREDENTIAL_DIRECTORY_OAUTH directory, as demonstrated by creating a file under /etc that will later be executed by root.	9.9	More Details
CVE-2020-23359	WeBid 1.2.2 admin/newuser.php has an issue with password rechecking during registration because it uses a loose comparison to check the identicalness of two passwords. Two non-identical passwords can still bypass the check.	9.8	More Details
CVE-2020-20296	An issue was found in CMSWing project version 1.3.8, Because the rechargeAction function does not check the balance parameter, malicious parameters can execute arbitrary SQL commands.	9.8	More Details
CVE-2020-26547	Monal before 4.9 does not implement proper sender verification on MAM and Message Carbon (XEP-0280) results. This allows a remote attacker (able to send stanzas to a victim) to inject arbitrary messages into the local history, with full control over the sender and receiver displayed to the victim.	9.8	More Details
CVE-2020-28194	Variable underflow exists in accel-ppp radius/packet.c when receiving a RADIUS vendor-specific attribute with length field is less than 2. It has an impact only when the attacker controls the RADIUS server, which can lead to arbitrary code execution.	9.8	More Details
CVE-2020-36109	ASUS RT-AX86U router firmware below version under 9.0.0.4_386 has a buffer overflow in the blocking_request.cgi function of the httpd module that can cause code execution when an attacker constructs malicious data.	9.8	More Details
CVE-2021-23330	All versions of package launchpad are vulnerable to Command Injection via stop.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20287	Unrestricted file upload vulnerability in the yccms 3.3 project. The xhUp function's improper judgment of the request parameters, triggers remote code execution.	9.8	More Details
CVE-2020-20289	Sql injection vulnerability in the yccms 3.3 project. The no_top function's improper judgment of the request parameters, triggers a sql injection vulnerability.	9.8	More Details
CVE-2020-20294	An issue was found in CMSWing project version 1.3.8. Because the log function does not check the log parameter, malicious parameters can execute arbitrary commands.	9.8	More Details
CVE-2020-20295	An issue was found in CMSWing project version 1.3.8. Because the updateAction function does not check the detail parameter, malicious parameters can execute arbitrary SQL commands.	9.8	More Details
CVE-2020-21176	SQL injection vulnerability in the model.increment and model.decrement function in ThinkJS 3.2.10 allows remote attackers to execute arbitrary SQL commands via the step parameter.	9.8	More Details
CVE-2020-23360	oscommerce v2.3.4.1 has a functional problem in user registration and password rechecking, where a non-identical password can bypass the checks in /catalog/admin/administrators.php and /catalog/password_reset.php	9.8	More Details
CVE-2020-21179	Sql injection vulnerability in koa2-blog 1.0.0 allows remote attackers to Injecting a malicious SQL statement via the name parameter to the signin page.	9.8	More Details
CVE-2020-21180	Sql injection vulnerability in koa2-blog 1.0.0 allows remote attackers to Injecting a malicious SQL statement via the name parameter to the signup page.	9.8	More Details
CVE-2019-20468	An issue was discovered in SeTracker2 for TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. It has unnecessary permissions such as READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE, and READ_CONTACTS.	9.8	More Details
CVE-2021-3378	FortiLogger 4.4.2.2 is affected by Arbitrary File Upload by sending a "Content-Type: image/png" header to Config/SaveUploadedHotspotLogoFile and then visiting Assets/temp/hotspot/img/logohotspot.asp.	9.8	More Details
CVE-2020-1896	A stack overflow vulnerability in Facebook Hermes 'builtin apply' prior to commit 86543ac47e59c522976b5632b8bf9a2a4583c7d2 (https://github.com/facebook/hermes/commit/86543ac47e59c522976b5632b8bf9a2a4583c7d2) 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-2020-25506	D-Link DNS-320 FW v2.06B01 Revision Ax is affected by command injection in the system_mgr.cgi component, which can lead to remote arbitrary code execution.	9.8	More Details
CVE-2020-18568	The D-Link DSR-250 (3.14) DSR-1000N (2.11B201) UPnP service contains a command injection vulnerability, which can cause remote command execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7775	This affects all versions of package freediskspace. The vulnerability arises out of improper neutralization of arguments in line 71 of freediskspace.js.	9.8	More Details
CVE-2020-15836	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The authentication function passes untrusted data to the operating system without proper sanitization. A crafted request can be sent to execute arbitrary commands as root.	9.8	More Details
CVE-2020-15835	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The authentication function contains undocumented code that provides the ability to authenticate as root without knowing the actual root password. An adversary with the private key can remotely authenticate to the management interface as root.	9.8	More Details
CVE-2020-15833	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The Dropbear SSH daemon has been modified to accept an alternate hard-coded path to a public key that allows root access. This key is stored in a /rom location that cannot be modified by the device owner.	9.8	More Details
CVE-2021-3160	Deserialization of untrusted data in the login page of ASSUWEB 359.3 build 1 subcomponent of ACA ASSUREX RENTES product allows a remote attacker to inject unsecure serialized Java object using a specially crafted HTTP request, resulting in an unauthenticated remote code execution on the server.	9.8	More Details
CVE-2020-23361	phpList 3.5.3 allows type juggling for login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	9.8	More Details
CVE-2021-3325	Monitorix 3.13.0 allows remote attackers to bypass Basic Authentication in a default installation (i.e., an installation without a hosts_deny option). This issue occurred because a new access-control feature was introduced without considering that some exiting installations became unsafe, upon an update to 3.13.0, unless the new feature was immediately configured.	9.8	More Details
CVE-2021-3331	WinSCP before 5.17.10 allows remote attackers to execute arbitrary programs when the URL handler encounters a crafted URL that loads session settings. (For example, this is exploitable in a default installation in which WinSCP is the handler for sftp:// URLs.)	9.8	More Details
CVE-2020-25782	An issue was discovered on Accfly Wireless Security IR Camera 720P System with software versions v3.10.73 through v4.15.77. There is an unauthenticated stack-based buffer overflow in the function CNetClientManage::ServerIP_Proto_Set during incoming message handling.	9.8	More Details
CVE-2020-25783	An issue was discovered on Accfly Wireless Security IR Camera System 720P with software versions v3.10.73 through v4.15.77. There is an unauthenticated heap-based buffer overflow in the function CNetClientTalk::OprMsg during incoming message handling.	9.8	More Details
CVE-2020-25784	An issue was discovered on Accfly Wireless Security IR Camera System 720P with software versions v3.10.73 through v4.15.77. There is an unauthenticated stack-based buffer overflow in the function CNetClientGuard::SubOprMsg during incoming message handling.	9.8	More Details
CVE-2020-25785	An issue was discovered on Accfly Wireless Security IR Camera System 720P with software versions v3.10.73 through v4.15.77. There is an unauthenticated stack-based buffer overflow in the function CFtpProtocol::FtpLogin during the update procedure.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13859	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.0.8-std devices. A format error in /etc/shadow, coupled with a logic bug in the LuCI - OpenWrt Configuration Interface framework, allows the undocumented system account mofidev to login to the cgi-bin/luci/quick/wizard management interface without a password by abusing a forgotten-password feature.	9.8	More Details
CVE-2020-4682	IBM MQ 7.5, 8.0, 9.0, 9.1, 9.2 LTS, and 9.2 CD could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization of trusted data. An attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 186509.	9.8	More Details
CVE-2021-26305	An issue was discovered in Deserializer::read_vec in the cdr crate before 0.2.4 for Rust. A user-provided Read implementation can gain access to the old contents of newly allocated heap memory, violating soundness.	9.8	More Details
CVE-2021-3346	Foris before 101.1.1, as used in Turris OS, lacks certain HTML escaping in the login template.	9.8	More Details
CVE-2020-29557	An issue was discovered on D-Link DIR-825 R1 devices through 3.0.1 before 2020-11-20. A buffer overflow in the web interface allows attackers to achieve pre-authentication remote code execution.	9.8	More Details
CVE-2020-15568	TerraMaster TOS before 4.1.29 has Invalid Parameter Checking that leads to code injection as root. This is a dynamic class method invocation vulnerability in include/exportUser.php, in which an attacker can trigger a call to the exec method with (for example) OS commands in the opt parameter.	9.8	More Details
CVE-2020-15690	In Nim before 1.2.6, the standard library asyncftpclient lacks a check for whether a message contains a newline character.	9.8	More Details
CVE-2020-13858	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 3.6.1-std and 4.0.8-std devices. They contain two undocumented administrator accounts. The sftp and mofidev accounts are defined in /etc/passwd and the password is not unique across installations.	9.8	More Details
CVE-2021-25912	Prototype pollution vulnerability in 'dotty' versions 0.0.1 through 0.1.0 allows attackers to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-35124	A cross-site scripting (XSS) vulnerability in the assets component of Mautic before 3.2.4 allows remote attackers to inject executable JavaScript through the Referer header of asset downloads.	9.6	More Details
CVE-2021-21276	Polr is an open source URL shortener. in Polr before version 2.3.0, a vulnerability in the setup process allows attackers to gain admin access to site instances, even if they do not possess an existing account. This vulnerability exists regardless of users' settings. If an attacker crafts a request with specific cookie headers to the /setup/finish endpoint, they may be able to obtain admin privileges on the instance. This is caused by a loose comparison (==) in SetupController that is susceptible to attack. The project has been patched to ensure that a strict comparison (===) is used to verify the setup key, and that /setup/finish verifies that no users table exists before performing any migrations or provisioning any new accounts. This is fixed in version 2.3.0. Users can patch this vulnerability without upgrading by adding abort(404) to the very first line of finishSetup in SetupController.php.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35547	A library index page in NuPoint Messenger in Mitel MiCollab before 9.2 FP1 could allow an unauthenticated attacker to gain access (view and modify) to user data.	9.1	More Details
CVE-2020-15097	loklak is an open-source server application which is able to collect messages from various sources, including twitter. The server contains a search index and a peer-to-peer index sharing interface. All messages are stored in an elasticsearch index. In loklak less than or equal to commit 5f48476, a path traversal vulnerability exists. Insufficient input validation in the APIs exposed by the loklak server allowed a directory traversal vulnerability. Any admin configuration and files readable by the app available on the hosted file system can be retrieved by the attacker. Furthermore, user-controlled content could be written to any admin config and files readable by the application. This has been patched in commit 50dd692. Users will need to upgrade their hosted instances of loklak to not be vulnerable to this exploit.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-5626	Logstorage version 8.0.0 and earlier, and ELC Analytics version 3.0.0 and earlier allow remote attackers to execute arbitrary OS commands via a specially crafted log file.	8.8	More Details
CVE-2021-25310	The administration web interface on Belkin Linksys WRT160NL 1.0.04.002_US_20130619 devices allows remote authenticated attackers to execute system commands with root privileges via shell metacharacters in the ui_language POST parameter to the apply.cgi form endpoint. This occurs in do_upgrade_post in mini_httpd. NOTE: This vulnerability only affects products that are no longer supported by the maintaine	8.8	More Details
CVE-2020-29004	The API in the Push extension for MediaWiki through 1.35 did not require an edit token in ApiPushBase.php and therefore facilitated a CSRF attack.	8.8	More Details
CVE-2020-4952	IBM Security Guardium 11.2 could allow an authenticated user to gain root access due to improper access control. IBM X-Force ID: 192028.	8.8	More Details
CVE-2020-28405	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to change the privileges of any user of the application. This can be used to grant himself the administrative role or remove all administrative accounts of the application.	8.8	More Details
CVE-2020-24271	A CSRF vulnerability was discovered in EasyCMS v1.6 that can add an admin account through index.php?s=/admin/rbacuser/insert/navTabId/rbacuser/callbackType/closeCurrent, then post username=***&password=***.	8.8	More Details
CVE-2021-25312	HTCondor before 8.9.11 allows a user to submit a job as another user on the system, because of a flaw in the IDTOKENS authentication method.	8.8	More Details
CVE-2020-25036	UCOPIA Wi-Fi appliances 6.0.5 allow authenticated remote attackers to escape the restricted administration shell CLI, and access a shell with admin user rights, via an unprotected less command.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25016	In OpenDoas from 6.6 to 6.8 the users PATH variable was incorrectly inherited by authenticated executions if the authenticating rule allowed the user to execute any command. Rules that only allowed to authenticated user to execute specific commands were not affected by this issue.	8.8	More Details
CVE-2021-25646	Apache Druid includes the ability to execute user-provided JavaScript code embedded in various types of requests. This functionality is intended for use in high-trust environments, and is disabled by default. However, in Druid 0.20.0 and earlier, it is possible for an authenticated user to send a specially-crafted request that forces Druid to run user-provided JavaScript code for that request, regardless of server configuration. This can be leveraged to execute code on the target machine with the privileges of the Druid server process.	8.8	More Details
CVE-2020-4888	IBM QRadar SIEM 7.4.0 to 7.4.2 Patch 1 and 7.3.0 to 7.3.3 Patch 7 could allow a remote attacker to execute arbitrary commands on the system, caused by insecure deserialization of user-supplied content by the Java deserialization function. By sending a malicious serialized Java object, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 190912.	8.8	More Details
CVE-2020-13569	A cross-site request forgery vulnerability exists in the GACL functionality of OpenEMR 5.0.2 and development version 6.0.0 (commit babec93f600ff1394f91ccd512bcad85832eb6ce). A specially crafted HTTP request can lead to the execution of arbitrary requests in the context of the victim. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2021-20621	Cross-site request forgery (CSRF) vulnerability in Aterm WG2600HP firmware Ver1.0.2 and earlier, and Aterm WG2600HP2 firmware Ver1.0.2 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2021-25909	ZIV Automation 4CCT-EA6-334126BF firmware version 3.23.80.27.36371, allows an unauthenticated, remote attacker to cause a denial of service condition on the device. An attacker could exploit this vulnerability by sending specific packets to the port 7919.	8.6	More Details
CVE-2020-28494	This affects the package total.js before 3.4.7. The issue occurs in the image.pipe and image.stream functions. The type parameter is used to build the command that is then executed using child_process.spawn. The issue occurs because child_process.spawn is called with the option shell set to true and because the type parameter is not properly sanitized.	8.6	More Details
CVE-2021-21277	angular-expressions is "angular's nicest part extracted as a standalone module for the browser and node". In angular-expressions before version 1.1.2 there is a vulnerability which allows Remote Code Execution if you call "expressions.compile(userControlledInput)" where "userControlledInput" is text that comes from user input. The security of the package could be bypassed by using a more complex payload, using a ".constructor.constructor" technique. In terms of impact: If running angular-expressions in the browser, an attacker could run any browser script when the application code calls expressions.compile(userControlledInput). If running angular-expressions on the server, an attacker could run any Javascript expression, thus gaining Remote Code Execution. This is fixed in version 1.1.2 of angular-expressions A temporary workaround might be either to disable user-controlled input that will be fed into angular-expressions in your application or allow only following characters in the userControlledInput.	8.5	More Details
CVE-2020-25037	UCOPIA Wi-Fi appliances 6.0.5 allow arbitrary code execution with admin user privileges via an escape from a restricted command.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35517	A flaw was found in qemu. A host privilege escalation issue was found in the virtio-fs shared file system daemon where a privileged guest user is able to create a device special file in the shared directory and use it to r/w access host devices.	8.2	More Details
CVE-2021-3336	DoTls13CertificateVerify in tls13.c in wolfSSL before 4.7.0 does not cease processing for certain anomalous peer behavior (sending an ED22519, ED448, ECC, or RSA signature without the corresponding certificate). The client side is affected because man-in-the-middle attackers can impersonate TLS 1.3 servers.	8.1	More Details
CVE-2020-28403	A Cross-Site Request Forgery (CSRF) vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an attacker to change the privileges of any user of the application. This can be used to grant himself administrative role or remove the administrative account of the application.	8.0	More Details
CVE-2021-25910	Improper Authentication vulnerability in the cookie parameter of ZIV AUTOMATION 4CCT-EA6-334126BF allows a local attacker to perform modifications in several parameters of the affected device as an authenticated user.	8.0	More Details
CVE-2021-3176	The chat window of the Mitel BusinessCTI Enterprise (MBC-E) Client for Windows before 6.4.15 and 7.x before 7.1.2 could allow an attacker to gain access to user information by sending certain code, due to improper input validation of http links. A successful exploit could allow an attacker to view user information and application data.	8.0	More Details
CVE-2021-23271	The TIBCO EBX Web Server component of TIBCO Software Inc.'s TIBCO EBX contains a vulnerability that theoretically allows a low privileged attacker with network access to execute a Stored Cross Site Scripting (XSS) attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 5.9.12 and below.	8.0	More Details
CVE-2021-3345	_gcry_md_block_write in cipher/hash-common.c in Libgcrypt version 1.9.0 has a heap-based buffer overflow when the digest final function sets a large count value. It is recommended to upgrade to 1.9.1 or later.	7.8	More Details
CVE-2021-3347	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.	7.8	More Details
CVE-2021-25137	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function.	7.8	More Details
CVE-2019-20471	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. When using the device at initial setup, a default password is used (123456) for administrative purposes. There is no prompt to change this password. Note that this password can be used in combination with CVE-2019-20470.	7.8	More Details
CVE-2021-25136	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function.	7.8	More Details
CVE-2021-25135	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22655	Multiple out-of-bounds read issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	7.8	More Details
CVE-2021-22653	Multiple out-of-bounds write issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	7.8	More Details
CVE-2021-22641	A heap-based buffer overflow issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	7.8	More Details
CVE-2021-22639	An uninitialized pointer issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	7.8	More Details
CVE-2021-22637	Multiple stack-based buffer overflow issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	7.8	More Details
CVE-2021-25134	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function.	7.8	More Details
CVE-2020-8672	Out of bound read in BIOS firmware for 8th, 9th Generation Intel(R) Core(TM), Intel(R) Celeron(R) Processor 4000 Series Processors may allow an unauthenticated user to potentially enable elevation of privilege or denial of service via local access.	7.8	More Details
CVE-2021-25247	A DLL hijacking vulnerability Trend Micro HouseCall for Home Networks version 5.3.1063 and below could allow an attacker to use a malicious DLL to escalate privileges and perform arbitrary code execution. An attacker must already have user privileges on the machine to exploit this vulnerability.	7.8	More Details
CVE-2021-25133	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function.	7.8	More Details
CVE-2021-25132	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function.	7.8	More Details
CVE-2021-25131	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function.	7.8	More Details
CVE-2021-25130	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1910	A missing bounds check in WhatsApp for Android prior to v2.21.1.13 and WhatsApp Business for Android prior to v2.21.1.13 could have allowed out-of-bounds read and write if a user applied specific image filters to a specially crafted image and sent the resulting image.	7.8	More Details
CVE-2021-25129	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability.	7.8	More Details
CVE-2021-25128	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability.	7.8	More Details
CVE-2021-25127	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function.	7.8	More Details
CVE-2021-25126	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function.	7.8	More Details
CVE-2020-35145	Acronis True Image for Windows prior to 2021 Update 3 allowed local privilege escalation due to a DLL hijacking vulnerability in multiple components, aka an Untrusted Search Path issue.	7.8	More Details
CVE-2021-25125	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability.	7.8	More Details
CVE-2021-25124	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability.	7.8	More Details
CVE-2021-25123	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice addlicense_func function.	7.8	More Details
CVE-2021-25138	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21287	MinIO is a High Performance Object Storage released under Apache License v2.0. In MinIO before version RELEASE.2021-01-30T00-20-58Z there is a server-side request forgery vulnerability. The target application may have functionality for importing data from a URL, publishing data to a URL, or otherwise reading data from a URL that can be tampered with. The attacker modifies the calls to this functionality by supplying a completely different URL or by manipulating how URLs are built (path traversal etc.). In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like HTTP enabled databases, or perform post requests towards internal services which are not intended to be exposed. This is fixed in version RELEASE.2021-01-30T00-20-58Z, all users are advised to upgrade. As a workaround you can disable the browser front-end with "MINIO_BROWSER=off" environment variable.	7.7	More Details
CVE-2021-21286	AVideo Platform is an open-source Audio and Video platform. It is similar to a self-hosted YouTube. In AVideo Platform before version 10.2 there is an authorization bypass vulnerability which enables an ordinary user to get admin control. This is fixed in version 10.2. All queries now remove the pass hash and the recoverPass hash.	7.7	More Details
CVE-2020-29005	The API in the Push extension for MediaWiki through 1.35 used cleartext for ApiPush credentials, allowing for potential information disclosure.	7.5	More Details
CVE-2020-15832	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The poof.cgi script contains undocumented code that provides the ability to remotely reboot the device. An adversary with the private key (but not the root password) can remotely reboot the device.	7.5	More Details
CVE-2021-3341	A path traversal vulnerability in the DxWebEngine component of DH2i DxEnterprise and DxOdyssey for Windows, version 19.5 through 20.x before 20.0.219.0, allows an attacker to read any file on the host file system via an HTTP request.	7.5	More Details
CVE-2021-26306	An issue was discovered in the raw-cpuid crate before 9.0.0 for Rust. It has unsound transmute calls within as_string() methods.	7.5	More Details
CVE-2021-26308	An issue was discovered in the marc crate before 2.0.0 for Rust. A user-provided Read implementation can gain access to the old contents of newly allocated memory, violating soundness.	7.5	More Details
CVE-2020-23352	Z-BlogPHP 1.6.0 Valyria is affected by incorrect access control. PHP loose comparison and a magic hash can be used to bypass authentication. zb_user/plugin/passwordvisit/include.php:passwordvisit_input_password() uses loose comparison to authenticate, which can be bypassed via magic hash values.	7.5	More Details
CVE-2020-24335	An issue was discovered in uIP through 1.0, as used in Contiki and Contiki-NG. Domain name parsing lacks bounds checks, allowing an attacker to corrupt memory with crafted DNS packets.	7.5	More Details
CVE-2020-15834	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The wireless network password is exposed in a QR encoded picture that an unauthenticated adversary can download via the web-management interface.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13860	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.0.8-std devices. The one-time password algorithm for the undocumented system account mofidev generates a predictable six-digit password.	7.5	More Details
CVE-2021-3337	The Hide-Thread-Content plugin through 2021-01-27 for MyBB allows remote attackers to bypass intended content-reading restrictions by clicking on reply or quote in the postbit.	7.5	More Details
CVE-2020-13857	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 3.6.1-std and 4.0.8-std devices. They can be rebooted by sending an unauthenticated poof.cgi HTTP GET request.	7.5	More Details
CVE-2020-13856	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.0.8-std devices. Authentication is not required to download the support file that contains sensitive information such as cleartext credentials and password hashes.	7.5	More Details
CVE-2019-25018	In the rcp client in MIT krb5-appl through 1.0.3, malicious servers could bypass intended access restrictions via the filename of . or an empty filename, similar to CVE-2018-20685 and CVE-2019-7282. The impact is modifying the permissions of the target directory on the client side. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.	7.5	More Details
CVE-2021-20586	Resource management errors vulnerability in a robot controller of MELFA FR Series(controller "CR800-*V*D" of RV-*FR***-D-* all versions, controller "CR800-*HD" of RH-*FRH***-D-* all versions, controller "CR800-*HRD" of RH-*FRHR***-D-* all versions, controller "CR800-*V*R with R16RTCPU" of RV-*FR***-R-* all versions, controller "CR800-*HR with R16RTCPU" of RH-*FRH***-R-* all versions, controller "CR800-*HRR with R16RTCPU" of RH-*FRHR***-R-* all versions, controller "CR800-*V*Q with Q172DSRCPU" of RV-*FR***-Q-* all versions, controller "CR800-*HQ with Q172DSRCPU" of RH-*FRH***-Q-* all versions, controller "CR800-*HRQ with Q172DSRCPU" of RH-*FRHR***-Q-* all versions) and a robot controller of MELFA CR Series(controller "CR800-CVD" of RV-8CRL-D-* all versions, controller "CR800-CHD" of RH-*CRH**-D-* all versions) as well as a cooperative robot ASSISTA(controller "CR800-05VD" of RV-5AS-D-* all versions) allows a remote unauthenticated attacker to cause a DoS of the execution of the robot program and the Ethernet communication by sending a large amount of packets in burst over a short period of time. As a result of DoS, an error may occur. A reset is required to recover it if the error occurs.	7.5	More Details
CVE-2020-23356	dmin/kernel/api/login.class.phpin in nibbleblog v3.7.1c allows type juggling for login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	7.5	More Details
CVE-2020-23355	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** Codiad 2.8.4 /componetns/user/class.user.php:Authenticate() is vulnerable in magic hash authentication bypass. If encrypted or hash value for the passwords form certain formats of magic hash, e.g, 0e123, another hash value 0e234 something can successfully authenticate.	7.5	More Details
CVE-2020-14255	HCL Digital Experience 9.5 containers include vulnerabilities that could expose sensitive data to unauthorized parties via crafted requests. These affect containers only. These do not affect traditional on-premise installations.	7.5	More Details
CVE-2021-23329	The package nested-object-assign before 1.0.4 are vulnerable to Prototype Pollution via the default function, as demonstrated by running the PoC below.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26118	While investigating ARTEMIS-2964 it was found that the creation of advisory messages in the OpenWire protocol head of Apache ActiveMQ Artemis 2.15.0 bypassed policy based access control for the entire session. Production of advisory messages was not subject to access control in error.	7.5	More Details
CVE-2019-20470	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. It performs actions based on certain SMS commands. This can be used to set up a voice communication channel from the watch to any telephone number, initiated by sending a specific SMS and using the default password, e.g., pw,<password>,call,<mobile_number> triggers an outbound call from the watch. The password is sometimes available because of CVE-2019-20471.	7.5	More Details
CVE-2020-20290	Directory traversal vulnerability in the yccms 3.3 project. The delete, deletesite, and deleteAll functions' improper judgment of the request parameters, triggers a directory traversal vulnerability.	7.5	More Details
CVE-2021-3326	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.	7.5	More Details
CVE-2021-21293	blaze is a Scala library for building asynchronous pipelines, with a focus on network IO. All servers running blaze-core before version 0.14.15 are affected by a vulnerability in which unbounded connection acceptance leads to file handle exhaustion. Blaze, accepts connections unconditionally on a dedicated thread pool. This has the net effect of amplifying degradation in services that are unable to handle their current request load, since incoming connections are still accepted and added to an unbounded queue. Each connection allocates a socket handle, which drains a scarce OS resource. This can also confound higher level circuit breakers which work based on detecting failed connections. The vast majority of affected users are using it as part of http4s-blaze-server <= 0.21.16. http4s provides a mechanism for limiting open connections, but is enforced inside the Blaze accept loop, after the connection is accepted and the socket opened. Thus, the limit only prevents the number of connections which can be simultaneously processed, not the number of connections which can be held open. The issue is fixed in version 0.14.15 for "NIO1SocketServerGroup". A "maxConnections" parameter is added, with a default value of 512. Concurrent connections beyond this limit are rejected. To run unbounded, which is not recommended, set a negative number. The "NIO2SocketServerGroup" has no such setting and is now deprecated. There are several possible workarounds described in the refrenced GitHub Advisory GHSA-xmw9-q7x9-j5qc.	7.5	More Details
CVE-2021-3283	HashiCorp Nomad and Nomad Enterprise up to 0.12.9 exec and java task drivers can access processes associated with other tasks on the same node. Fixed in 0.12.10, and 1.0.3.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21294	Http4s (http4s-blaze-server) is a minimal, idiomatic Scala interface for HTTP services. Http4s before versions 0.21.17, 0.22.0-M2, and 1.0.0-M14 have a vulnerability which can lead to a denial-of-service. Blaze-core, a library underlying http4s-blaze-server, accepts connections unboundedly on its selector pool. This has the net effect of amplifying degradation in services that are unable to handle their current request load, since incoming connections are still accepted and added to an unbounded queue. Each connection allocates a socket handle, which drains a scarce OS resource. This can also confound higher level circuit breakers which work based on detecting failed connections. http4s provides a general "MaxActiveRequests" middleware mechanism for limiting open connections, but it is enforced inside the Blaze accept loop, after the connection is accepted and the socket opened. Thus, the limit only prevents the number of connections which can be simultaneously processed, not the number of connections which can be held open. In 0.21.17, 0.22.0-M2, and 1.0.0-M14, a new "maxConnections" property, with a default value of 1024, has been added to the `BlazeServerBuilder`. Setting the value to a negative number restores unbounded behavior, but is strongly disrecommended. The NIO2 backend does not respect `maxConnections`. Its use is now deprecated in http4s-0.21, and the option is removed altogether starting in http4s-0.22. There are several possible workarounds described in the refrenced GitHub Advisory GHSA-xhv5-w9c5-2r2w.	7.5	More Details
CVE-2021-3282	HashiCorp Vault Enterprise 1.6.0 & 1.6.1 allowed the `remove-peer` raft operator command to be executed against DR secondaries without authentication. Fixed in 1.6.2.	7.5	More Details
CVE-2021-26117	The optional ActiveMQ LDAP login module can be configured to use anonymous access to the LDAP server. In this case, for Apache ActiveMQ Artemis prior to version 2.16.0 and Apache ActiveMQ prior to versions 5.16.1 and 5.15.14, the anonymous context is used to verify a valid users password in error, resulting in no check on the password.	7.5	More Details
CVE-2021-21289	Mechanize is an open-source ruby library that makes automated web interaction easy. In Mechanize from version 2.0.0 and before version 2.7.7 there is a command injection vulnerability. Affected versions of mechanize allow for OS commands to be injected using several classes' methods which implicitly use Ruby's Kernel.open method. Exploitation is possible only if untrusted input is used as a local filename and passed to any of these calls: Mechanize::CookieJar#load, Mechanize::CookieJar#save_as, Mechanize#download, Mechanize::Download#save, Mechanize::File#save, and Mechanize::FileResponse#read_body. This is fixed in version 2.7.7.	7.4	More Details
CVE-2020-28426	All versions of package kill-process-on-port are vulnerable to Command Injection via a.getProcessPortId.	7.3	More Details
CVE-2020-28495	This affects the package total.js before 3.4.7. The set function can be used to set a value into the object according to the path. However the keys of the path being set are not properly sanitized, leading to a prototype pollution vulnerability. The impact depends on the application. In some cases it is possible to achieve Denial of service (DoS), Remote Code Execution or Property Injection.	7.3	More Details
CVE-2020-5427	In Spring Cloud Data Flow, versions 2.6.x prior to 2.6.5, versions 2.5.x prior 2.5.4, an application is vulnerable to SQL injection when requesting task execution.	7.2	More Details
CVE-2020-35754	OpenSolution Quick.CMS < 6.7 and Quick.Cart < 6.7 allow an authenticated user to perform code injection (and consequently Remote Code Execution) via the input fields of the Language tab.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20187	It was found in Moodle before version 3.10.1, 3.9.4, 3.8.7 and 3.5.16 that it was possible for site administrators to execute arbitrary PHP scripts via a PHP include used during Shibboleth authentication.	7.2	More Details
CVE-2020-14418	A TOCTOU vulnerability exists in madCodeHook before 2020-07-16 that allows local attackers to elevate their privileges to SYSTEM. This occurs because path redirection can occur via vectors involving directory junctions.	7.0	More Details
CVE-2021-3348	nbd_add_socket in drivers/block/nbd.c in the Linux kernel through 5.10.12 has an ndb_queue_rq use-after-free that could be triggered by local attackers (with access to the nbd device) via an I/O request at a certain point during device setup, aka CID-b98e762e3d71.	7.0	More Details
CVE-2020-8101	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in HTTP interface of ADT LifeShield DIY HD Video Doorbell allows an attacker on the same network to execute commands on the device. This issue affects: ADT LifeShield DIY HD Video Doorbell version 1.0.02R09 and prior versions.	6.9	More Details
CVE-2019-20473	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. Any SIM card used with the device cannot have a PIN configured. If a PIN is configured, the device simply produces a "Remove PIN and restart!" message, and cannot be used. This makes it easier for an attacker to use the SIM card by stealing the device.	6.8	More Details
CVE-2020-28498	The package elliptic before 6.5.4 are vulnerable to Cryptographic Issues via the secp256k1 implementation in elliptic/ec/key.js. There is no check to confirm that the public key point passed into the derive function actually exists on the secp256k1 curve. This results in the potential for the private key used in this implementation to be revealed after a number of ECDH operations are performed.	6.8	More Details
CVE-2021-21284	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability involving the --userns-remap option in which access to remapped root allows privilege escalation to real root. When using "--userns-remap", if the root user in the remapped namespace has access to the host filesystem they can modify files under "/var/lib/docker/<remapping>" that cause writing files with extended privileges. Versions 20.10.3 and 19.03.15 contain patches that prevent privilege escalation from remapped user.	6.8	More Details
CVE-2020-25035	UCOPIA Wi-Fi appliances 6.0.5 allow arbitrary code execution with root privileges using chroothole_client's PHP call, a related issue to CVE-2017-11322.	6.7	More Details
CVE-2020-8734	Improper input validation in the firmware for Intel(R) Server Board M10JNP2SB before version 7.210 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-21254	CKEditor 5 is an open source rich text editor framework with a modular architecture. The CKEditor 5 Markdown plugin (@ckeditor/ckeditor5-markdown-gfm) before version 25.0.0 has a regex denial of service (ReDoS) vulnerability. The vulnerability allowed to abuse link recognition regular expression, which could cause a significant performance drop resulting in browser tab freeze. It affects all users using CKEditor 5 Markdown plugin at version <= 24.0.0. The problem has been recognized and patched. The fix will be available in version 25.0.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35652	An issue was discovered in res_pjsip_diversion.c in Sangoma Asterisk before 13.38.0, 14.x through 16.x before 16.15.0, 17.x before 17.9.0, and 18.x before 18.1.0. A crash can occur when a SIP message is received with a History-Info header that contains a tel-uri, or when a SIP 181 response is received that contains a tel-uri in the Diversion header.	6.5	More Details
CVE-2020-4789	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1, 7.4.0 to 7.4.1 Patch 1, and 7.3.0 to 7.3.3 Patch 5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 189302.	6.5	More Details
CVE-2019-25014	A NULL pointer dereference was found in pkg/proxy/envoy/v2/debug.go getResourceVersion in Istio pilot before 1.5.0-alpha.0. If a particular HTTP GET request is made to the pilot API endpoint, it is possible to cause the Go runtime to panic (resulting in a denial of service to the istio-pilot application).	6.5	More Details
CVE-2020-29604	An issue was discovered in MantisBT before 2.24.4. A missing access check in bug_actiongroup.php allows an attacker (with rights to create new issues) to use the COPY group action to create a clone, including all bugnotes and attachments, of any private issue (i.e., one having Private view status, or belonging to a private Project) via the bug_arr[] parameter. This provides full access to potentially confidential information.	6.5	More Details
CVE-2020-28406	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access details about jobs he should not have access to via the Audit Trail Feature.	6.5	More Details
CVE-2020-28404	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access the Billing page without the appropriate privileges.	6.5	More Details
CVE-2020-28401	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access WIP details about jobs he should not have access to.	6.5	More Details
CVE-2021-21285	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability in which pulling an intentionally malformed Docker image manifest crashes the dockerd daemon. Versions 20.10.3 and 19.03.15 contain patches that prevent the daemon from crashing.	6.5	More Details
CVE-2020-24665	The Dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains an XML Entity Expansion injection vulnerability, which allows an authenticated remote users to trigger a denial of service (DoS) condition. Specifically, the vulnerability lies in the 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, >= 8.3.0.0 GA	6.5	More Details
CVE-2020-24490	Improper buffer restrictions in BlueZ may allow an unauthenticated user to potentially enable denial of service via adjacent access. This affects all Linux kernel versions that support BlueZ.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21266	openHAB is a vendor and technology agnostic open source automation software for your home. In openHAB before versions 2.5.12 and 3.0.1 the XML external entity (XXE) attack allows attackers in the same network as the openHAB instance to retrieve internal information like the content of files from the file system. Responses to SSDP requests can be especially malicious. All add-ons that use SAX or JAXB parsing of externally received XML are potentially subject to this kind of attack. In openHAB, the following add-ons are potentially impacted: AvmFritz, BoseSoundtouch, DenonMarantz, DLinkSmarthome, Enigma2, FmiWeather, FSInternetRadio, Gce, Homematic, HPPrinter, IHC, Insteon, Onkyo, Roku, SamsungTV, Sonos, Roku, Tellstick, TR064, UPnPControl, Vitotronic, Wemo, YamahaReceiver and XPath Tranformation. The vulnerabilities have been fixed in versions 2.5.12 and 3.0.1 by a more strict configuration of the used XML parser.	6.4	More Details
CVE-2020-17380	A heap-based buffer overflow was found in QEMU through 5.0.0 in the SDHCI device emulation support. It could occur while doing a multi block SDMA transfer via the sdhci_sdma_transfer_multi_blocks() routine in hw/sd/sdhci.c. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition, or potentially execute arbitrary code with privileges of the QEMU process on the host.	6.3	More Details
CVE-2020-4820	IBM Cloud Pak for Security (CP4S) 1.4.0.0 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.	6.1	More Details
CVE-2020-4081	In Digital Experience 8.5, 9.0, and 9.5, WSRP consumer is vulnerable to cross-site scripting (XSS).	6.1	More Details
CVE-2021-20620	Cross-site scripting vulnerability in Aterm WF800HP firmware Ver1.0.9 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-21043	ACS Commons version 4.9.2 (and earlier) suffers from a Reflected Cross-site Scripting (XSS) vulnerability in version-compare and page-compare due to invalid JCR characters that are not handled correctly. An attacker could potentially exploit this vulnerability to inject malicious JavaScript content into vulnerable form fields and execute it within the context of the victim's browser. Exploitation of this issue requires user interaction in order to be successful.	6.1	More Details
CVE-2021-22874	Revive Adserver before 5.1.1 is vulnerable to a reflected XSS vulnerability in userlog-index.php via the `period_preset` parameter.	6.1	More Details
CVE-2021-20622	Cross-site scripting vulnerability in Aterm WG2600HP firmware Ver1.0.2 and earlier, and Aterm WG2600HP2 firmware Ver1.0.2 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-3350	deleteaccount.php in the Delete Account plugin 1.4 for MyBB allows XSS via the deletereason parameter.	6.1	More Details
CVE-2021-3318	attach/ajax.php in DzzOffice through 2.02.1 allows XSS via the editorid parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26303	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the user-profile.php Full Name field.	6.1	More Details
CVE-2020-13562	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnaerability in the phpGACL template action parameter.	6.1	More Details
CVE-2020-13563	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnerability in the phpGACL template group_id parameter.	6.1	More Details
CVE-2020-13564	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnerability in the phpGACL template acl_id parameter.	6.1	More Details
CVE-2020-1723	A flaw was found in Keycloak Gatekeeper (Louketo). The logout endpoint can be abused to redirect logged-in users to arbitrary web pages. Affected versions of Keycloak Gatekeeper (Louketo): 6.0.1, 7.0.0	6.1	More Details
CVE-2021-3340	A cross-site scripting (XSS) vulnerability in many forms of Wikindx before 5.7.0 and 6.x through 6.4.0 allows remote attackers to inject arbitrary web script or HTML via the message parameter to index.php?action=initLogon or modules/admin/DELETEIMAGES.php.	6.1	More Details
CVE-2021-22875	Revive Adserver before 5.1.1 is vulnerable to a reflected XSS vulnerability in stats.php via the `setPerPage` parameter.	6.1	More Details
CVE-2020-5428	In applications using Spring Cloud Task 2.2.4.RELEASE and below, may be vulnerable to SQL injection when exercising certain lookup queries in the TaskExplorer.	6.0	More Details
CVE-2021-20199	Rootless containers run with Podman, receive all traffic with a source IP address of 127.0.0.1 (including from remote hosts). This impacts containerized applications that trust localhost (127.0.01) connections by default and do not require authentication. This issue affects Podman 1.8.0 onwards.	5.9	More Details
CVE-2019-25017	An issue was discovered in rcp in MIT krb5-appl through 1.0.3. Due to the rcp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the rcp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious rcp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the rcp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file). This issue is similar to CVE-2019-6111 and CVE-2019-7283. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.	5.9	More Details
CVE-2020-4816	IBM Cloud Pak for Security (CP4S) 1.4.0.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 189703.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23328	This affects all versions of package iniparserjs. This vulnerability relates when ini_parser.js is concentrating arrays. Depending on if user input is provided, an attacker can overwrite and pollute the object prototype of a program.	5.6	More Details
CVE-2021-21292	Traccar is an open source GPS tracking system. In Traccar before version 4.12 there is an unquoted Windows binary path vulnerability. Only Windows versions are impacted. Attacker needs write access to the filesystem on the host machine. If Java path includes a space, then attacker can lift their privilege to the same as Traccar service (system). This is fixed in version 4.12.	5.5	More Details
CVE-2021-3272	jp2_decode in jp2/jp2_dec.c in libjasper in JasPer 2.0.24 has a heap-based buffer over-read when there is an invalid relationship between the number of channels and the number of image components.	5.5	More Details
CVE-2021-25226	A memory exhaustion vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow a local attacker to craft specific files that can cause a denial-of-service on the affected product. The specific flaw exists within a scan engine component. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	5.5	More Details
CVE-2021-25225	A memory exhaustion vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow a local attacker to craft specific files that can cause a denial-of-service on the affected product. The specific flaw exists within a scheduled scan component. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	5.5	More Details
CVE-2020-8585	OnCommand Unified Manager Core Package versions prior to 5.2.5 may disclose sensitive account information to unauthorized users via the use of PuTTY Link (plink).	5.5	More Details
CVE-2021-26307	An issue was discovered in the raw-cpuid crate before 9.0.0 for Rust. It allows __cpuid_count() calls even if the processor does not support the CPUID instruction, which is unsound and causes a deterministic crash.	5.5	More Details
CVE-2021-25224	A memory exhaustion vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow a local attacker to craft specific files that can cause a denial-of-service on the affected product. The specific flaw exists within a manual scan component. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	5.5	More Details
CVE-2020-4855	IBM Jazz Foundation products 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: 190457.	5.4	More Details
CVE-2020-4865	IBM Jazz Foundation products 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: 190741.	5.4	More Details
CVE-2021-20357	IBM Jazz Foundation products 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: 194963.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1725	A flaw was found in keycloak before version 13.0.0. In some scenarios a user still has access to a resource after changing the role mappings in Keycloak and after expiration of the previous access token.	5.4	More Details
CVE-2020-4547	IBM Jazz Foundation products could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 183315.	5.4	More Details
CVE-2020-24669	The New Analysis Report in Hitachi Vantara Pentaho through 7.x - 8.x contains a DOM-based Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Analysis Report Description' field in 'About this Report' section. Remediated in >= 8.3.0.9, >= 9.0.0.1, and >= 9.1.0.0 GA.	5.4	More Details
CVE-2020-26272	The Electron framework lets you write cross-platform desktop applications using JavaScript, HTML and CSS. In affected versions of Electron IPC messages sent from the main process to a subframe in the renderer process, through webContents.sendToFrame, event.reply or when using the remote module, can in some cases be delivered to the wrong frame. If your app uses remote, calls webContents.sendToFrame, or calls event.reply in an IPC message handler then it is impacted by this issue. This has been fixed in versions 9.4.0, 10.2.0, 11.1.0, and 12.0.0-beta.9. There are no workarounds for this issue.	5.4	More Details
CVE-2021-20183	It was found in Moodle before version 3.10.1 that some search inputs were vulnerable to reflected XSS due to insufficient escaping of search queries.	5.4	More Details
CVE-2020-4524	IBM Jazz Foundation products 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: 182434.	5.4	More Details
CVE-2021-20186	It was found in Moodle before version 3.10.1, 3.9.4, 3.8.7 and 3.5.16 that if the TeX notation filter was enabled, additional sanitizing of TeX content was required to prevent the risk of stored XSS.	5.4	More Details
CVE-2021-3395	A cross-site scripting (XSS) vulnerability in Pryaniki 6.44.3 allows remote authenticated users to upload an arbitrary file. The JavaScript code will execute when someone visits the attachment.	5.4	More Details
CVE-2021-25647	Mobile application "Testes de Codigo" v11.3 and prior allows stored XSS by injecting a payload in the "feedback" message field causing it to be stored in the remote database and leading to its execution on client devices when loading the "feedback list", either by accessing the website directly or using the mobile application.	5.4	More Details
CVE-2020-24670	The Dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'type' attribute of 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, and >= 8.3.0.0 GA.	5.4	More Details
CVE-2020-36115	Stored Cross Site Scripting (XSS) vulnerability in EGavilan Media CRUD Operation with PHP, MySQL, Bootstrap, and Dompdf via First Name or Last Name parameter in the 'Add New Record Feature'.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24664	The dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'pho:title' attribute of 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, and >= 8.3.0.0 GA.	5.4	More Details
CVE-2021-26304	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the add-expense.php Item parameter.	5.4	More Details
CVE-2021-3298	Collabtive 3.1 allows XSS when an authenticated user enters an XSS payload into the address section of the profile edit page, aka the manageuser.php?action=edit address1 parameter.	5.4	More Details
CVE-2020-28402	An improper authorization vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an unauthorized user to access Launcher Configuration Panel.	5.4	More Details
CVE-2020-24666	The Analysis Report in Hitachi Vantara Pentaho through 7.x - 8.x contains a stored Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Display Name' parameter. Remediated in >= 9.1.0.1	5.4	More Details
CVE-2021-26067	Affected versions of Atlassian Bamboo allow an unauthenticated remote attacker to view a stack trace that may reveal the path for the home directory in disk and if certain files exists on the tmp directory, via a Sensitive Data Exposure vulnerability in the /chart endpoint. The affected versions are before version 7.2.2.	5.3	More Details
CVE-2021-3281	In Django 2.2 before 2.2.18, 3.0 before 3.0.12, and 3.1 before 3.1.6, the django.utils.archive.extract method (used by "startapp --template" and "startproject --template") allows directory traversal via an archive with absolute paths or relative paths with dot segments.	5.3	More Details
CVE-2020-29535	Archer before 6.8 P4 (6.8.0.4) contains a stored XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When application users access the corrupted data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	5.3	More Details
CVE-2020-29662	In Harbor 2.0 before 2.0.5 and 2.1.x before 2.1.2 the catalog’s registry API is exposed on an unauthenticated path.	5.3	More Details
CVE-2020-25594	HashiCorp Vault and Vault Enterprise allowed for enumeration of Secrets Engine mount paths via unauthenticated HTTP requests. Fixed in 1.6.2 & 1.5.7.	5.3	More Details
CVE-2020-4815	IBM Cloud Pak for Security (CP4S) 1.4.0.0 could allow a remote user to obtain sensitive information from HTTP response headers that could be used in further attacks against the system.	5.3	More Details
CVE-2020-28493	This affects the package jinja2 from 0.0.0 and before 2.11.3. The ReDoS vulnerability is mainly due to the `_punctuation_re regex` operator and its use of multiple wildcards. The last wildcard is the most exploitable as it searches for trailing punctuation. This issue can be mitigated by Markdown to format user content instead of the urlize filter, or by implementing request timeouts and limiting process memory.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4628	IBM Cloud Pak for Security (CP4S) 1.3.0.1 and 1.4.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 185369.	5.3	More Details
CVE-2021-3024	HashiCorp Vault and Vault Enterprise disclosed the internal IP address of the Vault node when responding to some invalid, unauthenticated HTTP requests. Fixed in 1.6.2 & 1.5.7.	5.3	More Details
CVE-2021-20185	It was found in Moodle before version 3.10.1, 3.9.4, 3.8.7 and 3.5.16 that messaging did not impose a character limit when sending messages, which could result in client-side (browser) denial of service for users receiving very large messages.	5.3	More Details
CVE-2021-26276	scripts/cli.js in the GoDaddy node-config-shield (aka Config Shield) package before 0.2.2 for Node.js calls eval when processing a set command. NOTE: the vendor reportedly states that this is not a vulnerability. The set command was not intended for use with untrusted data	5.3	More Details
CVE-2020-14221	HCL Digital Experience 8.5, 9.0, and 9.5 exposes information about the server to unauthorized users.	4.9	More Details
CVE-2020-29538	Archer before 6.9 P1 (6.9.0.1) contains an improper access control vulnerability in an API. A remote authenticated malicious administrative user can potentially exploit this vulnerability to gather information about the system, and may use this information in subsequent attacks.	4.9	More Details
CVE-2020-36012	Stored XSS vulnerability in BDTASK Multi-Store Inventory Management System 1.0 allows a local admin to inject arbitrary code via the Customer Name Field.	4.8	More Details
CVE-2021-21291	OAuth2 Proxy is an open-source reverse proxy and static file server that provides authentication using Providers (Google, GitHub, and others) to validate accounts by email, domain or group. In OAuth2 Proxy before version 7.0.0, for users that use the whitelist domain feature, a domain that ended in a similar way to the intended domain could have been allowed as a redirect. For example, if a whitelist domain was configured for ".example.com", the intention is that subdomains of example.com are allowed. Instead, "example.com" and "badexample.com" could also match. This is fixed in version 7.0.0 onwards. As a workaround, one can disable the whitelist domain feature and run separate OAuth2 Proxy instances for each subdomain.	4.7	More Details
CVE-2020-29537	Archer before 6.8 P2 (6.8.0.2) is affected by an open redirect vulnerability. A remote privileged attacker may potentially redirect legitimate users to arbitrary web sites and conduct phishing attacks. The attacker could then steal the victims' credentials and silently authenticate them to the Archer application without the victims realizing an attack occurred.	4.6	More Details
CVE-2020-4967	IBM Cloud Pak for Security (CP4S) 1.3.0.1 could disclose sensitive information through HTTP headers which could be used in further attacks against the system. IBM X-Force ID: 192425.	4.3	More Details
CVE-2020-4786	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1, 7.4.0 to 7.4.1 Patch 1, and 7.3.0 to 7.3.3 Patch 5 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 189221.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4189	IBM Security Guardium 11.2 discloses sensitive information in the response headers that could be used in further attacks against the system. IBM X-Force ID: 174850.	4.3	More Details
CVE-2020-4934	IBM Content Navigator 3.0.CD could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 191752.	4.3	More Details
CVE-2020-29605	An issue was discovered in MantisBT before 2.24.4. Due to insufficient access-level checks, any logged-in user allowed to perform Group Actions can get access to the Summary fields of private Issues via bug_arr[]= in a crafted bug_actiongroup_page.php URL. (The target Issues can have Private view status, or belong to a private Project.)	4.3	More Details
CVE-2020-29536	Archer before 6.8 P2 (6.8.0.2) is affected by a path exposure vulnerability. A remote authenticated malicious attacker with access to service files may obtain sensitive information to use it in further attacks.	4.3	More Details
CVE-2021-20184	It was found in Moodle before version 3.10.1, 3.9.4 and 3.8.7 that a insufficient capability checks in some grade related web services meant students were able to view other students grades.	4.3	More Details
CVE-2020-14192	Affected versions of Atlassian Fisheye and Crucible allow remote attackers to view a product's SEN via an Information Disclosure vulnerability in the x-asen response header from Atlassian Analytics. The affected versions are before version 4.8.4.	4.3	More Details
CVE-2020-36231	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view the metadata of boards they should not have access to via an Insecure Direct Object References (IDOR) vulnerability. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.2.	4.3	More Details
CVE-2020-29603	In manage_proj_edit_page.php in MantisBT before 2.24.4, any unprivileged logged-in user can retrieve Private Projects' names via the manage_proj_edit_page.php project_id parameter, without having access to them.	4.3	More Details
CVE-2021-3349	GNOME Evolution through 3.38.3 produces a "Valid signature" message for an unknown identifier on a previously trusted key because Evolution does not retrieve enough information from the GnuPG API. NOTE: third parties dispute the significance of this issue, and dispute whether Evolution is the best place to change this behavior	3.3	More Details
CVE-2020-4787	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1, 7.4.0 to 7.4.1 Patch 1, and 7.3.0 to 7.3.3 Patch 5 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 189224.	2.3	More Details
CVE-2020-16111	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16112	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16110	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. 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-2020-16113	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16108	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16114	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16107	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16106	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16115	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-16105	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-0237	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-3142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-35128. Reason: This candidate is a reservation duplicate of CVE-2020-35128. Notes: All CVE users should reference CVE-2020-35128 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-20207	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs:CVE-2021-3348. Reason: This candidate is a reservation duplicate of CVE-2021-3348. Notes: All CVE users should reference CVE-2021-3348 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-16109	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details