SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 May 2020

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-2020-11057	In XWiki Platform 7.2 through 11.10.2, registered users without scripting/programming permissions are able to execute python/groovy scripts while editing personal dashboards. This has been fixed 11.3.7 , 11.10.3 and 12.0.	9.9	More Details
CVE-2020-12746	An issue was discovered on Samsung mobile devices with O(8.X), P(9.0), and Q(10.0) (Exynos chipsets) software. Attackers can bypass the Secure Bootloader protection mechanism via a heap-based buffer overflow to execute arbitrary code. The Samsung ID is SVE-2020-16712 (May 2020).	9.8	More Details
CVE-2020-12022	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. An improper validation vulnerability exists that could allow an attacker to inject specially crafted input into memory where it can be executed.	9.8	More Details
CVE-2020-11530	A blind SQL injection vulnerability is present in Chop Slider 3, a WordPress plugin. The vulnerability is introduced in the id GET parameter supplied to get_script/index.php, and allows an attacker to execute arbitrary SQL queries in the context of the WP database user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11532	Zoho ManageEngine DataSecurity Plus prior to 6.0.1 uses default admin credentials to communicate with a DataEngine Xnode server. This allows an attacker to bypass authentication for this server and execute all operations in the context of admin user.	9.8	More Details
CVE-2020-12637	Zulip Desktop before 5.2.0 has Missing SSL Certificate Validation because all validation was inadvertently disabled during an attempt to recognize the ignoreCerts option.	9.8	More Details
CVE-2020-12766	Gnuteca 3.8 allows action=main:search:simpleSearch SQL Injection via the exemplaryStatusId parameter.	9.8	More Details
CVE-2020-12743	An issue was discovered in Gazie 7.32. A successful installation does not remove or block (or in any other way prevent use of) its own file /setup/install/setup.php, meaning that anyone can request it without authentication. This file allows arbitrary PHP file inclusion via a hidden_req POST parameter.	9.8	More Details
CVE-2020-12747	An issue was discovered on Samsung mobile devices with Q(10.0) (Exynos980 9630 and Exynos990 9830 chipsets) software. The Bootloader has a heap-based buffer overflow because of the mishandling of specific commands. The Samsung IDs are SVE-2020-16981, SVE-2020-16991 (May 2020).	9.8	More Details
CVE-2020-10638	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. Multiple heap-based buffer overflow vulnerabilities exist caused by a lack of proper validation of the length of user-supplied data, which may allow remote code execution.	9.8	More Details
CVE-2020-12753	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. Arbitrary code execution can occur via the bootloader because of an EL1/EL3 coldboot vulnerability involving raw_resources. The LG ID is LVE-SMP-200006 (May 2020).	9.8	More Details
CVE-2018-1285	Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.	9.8	More Details
CVE-2020-8159	There is a vulnerability in actionpack_page-caching gem < v1.2.1 that allows an attacker to write arbitrary files to a web server, potentially resulting in remote code execution if the attacker can write unescaped ERB to a view.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1939	The Apache NuttX (Incubating) project provides an optional separate "apps" repository which contains various optional components and example programs. One of these, ftpd, had a NULL pointer dereference bug. The NuttX RTOS itself is not affected. Users of the optional apps repository are affected only if they have enabled ftpd. Versions 6.15 to 8.2 are affected.	9.8	More Details
CVE-2020-12823	OpenConnect 8.09 has a buffer overflow, causing a denial of service (application crash) or possibly unspecified other impact, via crafted certificate data to get_cert_name in gnutls.c.	9.8	More Details
CVE-2020-6242	SAP Business Objects Business Intelligence Platform (Live Data Connect), versions 1.0, 2.0, 2.1, 2.2, 2.3, allows an attacker to logon on the Central Management Console without password in case of the BIPRWS application server was not protected with some specific certificate, leading to Missing Authentication Check.	9.8	More Details
CVE-2020-12002	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. Multiple stack-based buffer overflow vulnerabilities exist caused by a lack of proper validation of the length of user-supplied data, which may allow remote code execution.	9.8	More Details
CVE-2020-3125	A vulnerability in the Kerberos authentication feature of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to impersonate the Kerberos key distribution center (KDC) and bypass authentication on an affected device that is configured to perform Kerberos authentication for VPN or local device access. The vulnerability is due to insufficient identity verification of the KDC when a successful authentication response is received. An attacker could exploit this vulnerability by spoofing the KDC server response to the ASA device. This malicious response would not have been authenticated by the KDC. A successful attack could allow an attacker to bypass Kerberos authentication.	9.8	More Details
CVE-2020-12735	reset.php in DomainMOD 4.13.0 uses insufficient entropy for password reset requests, leading to account takeover.	9.8	More Details
CVE-2020-4429	IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, and 2.0.6 contains a default password for an IDRM administrative account. A remote attacker could exploit this vulnerability to login and execute arbitrary code on the system with root privileges. IBM X-Force ID: 180534.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3318	Multiple vulnerabilities in Cisco Firepower Management Center (FMC) Software and Cisco Firepower User Agent Software could allow an attacker to access a sensitive part of an affected system with a high-privileged account. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2020-8899	There is a buffer overwrite vulnerability in the Quram qmg library of Samsung's Android OS versions O(8.x), P(9.0) and Q(10.0). An unauthenticated, unauthorized attacker sending a specially crafted MMS to a vulnerable phone can trigger a heap-based buffer overflow in the Quram image codec leading to an arbitrary remote code execution (RCE) without any user interaction. The Samsung ID is SVE-2020-16747.	9.8	More Details
CVE-2019-18868	Blaauw Remote Kiln Control through v3.00r4 allows an unauthenticated attacker to access MySQL credentials in cleartext in /engine/db.inc, /lang/nl.bak, or /lang/en.bak.	9.8	More Details
CVE-2019-18869	Leftover Debug Code in Blaauw Remote Kiln Control through v3.00r4 allows a user to execute arbitrary php code via /default.php?idx=17.	9.8	More Details
CVE-2020-7646	curlrequest through 1.0.1 allows reading any file by populating the file parameter with user input.	9.8	More Details
CVE-2020-7805	An issue was discovered on KT Slim egg IML500 (R7283, R8112, R8424) and IML520 (R8112, R8368, R8411) wifi device. This issue is a command injection allowing attackers to execute arbitrary OS commands.	9.8	More Details
CVE-2020-4427	IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, and 2.0.6 could allow a remote attacker to bypass security restrictions when configured with SAML authentication. By sending a specially crafted HTTP request, an attacker could exploit this vulnerability to bypass the authentication process and gain full administrative access to the system. IBM X-Force ID: 180532.	9.8	More Details
CVE-2020-12006	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. Multiple relative path traversal vulnerabilities exist that may allow a low privilege user to overwrite files outside the application’s control.	9.8	More Details
CVE-2020-10176	ASSA ABLOY Yale WIPC-301W 2.x.2.29 through 2.x.2.43_p1 devices allow Eval Injection of commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10794	Gira TKS-IP-Gateway 4.0.7.7 is vulnerable to unauthenticated path traversal that allows an attacker to download the application database. This can be combined with CVE-2020-10795 for remote root access.	9.8	More Details
CVE-2020-12720	vBulletin before 5.5.6pl1, 5.6.0 before 5.6.0pl1, and 5.6.1 before 5.6.1pl1 has incorrect access control.	9.8	More Details
CVE-2020-3187	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of the HTTP URL. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences. An exploit could allow the attacker to view or delete arbitrary files on the targeted system. When the device is reloaded after exploitation of this vulnerability, any files that were deleted are restored. The attacker can only view and delete files within the web services file system. This file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability can not be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. Reloading the affected device will restore all files within the web services file system.	9.1	More Details
CVE-2020-12761	modules/loaders/loader_ico.c in imlib2 1.6.0 has an integer overflow (with resultant invalid memory allocations and out-of-bounds reads) via an icon with many colors in its color map.	9.1	More Details
CVE-2020-11431	The documentation component in i-net Clear Reports 16.0 to 19.2, HelpDesk 8.0 to 8.3, and PDFC 4.3 to 6.2 allows a remote unauthenticated attacker to read arbitrary system files and directories on the target server via Directory Traversal.	9.1	More Details
CVE-2020-11006	In Shopizer before version 2.11.0, a script can be injected in various forms and saved in the database, then executed when information is fetched from backend. This has been patched in version 2.11.0.	9.1	More Details
CVE-2020-12740	tcprewrite in Tcpreplay through 4.3.2 has a heap-based buffer over-read during a get_c operation. The issue is being triggered in the function get_ipv6_next() at common/get.c.	9.1	More Details
CVE-2020-4428	IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, and 2.0.4 could allow a remote authenticated attacker to execute arbitrary commands on the system. IBM X-Force ID: 180533.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10022	A malformed JSON payload that is received from an UpdateHub server may trigger memory corruption in the Zephyr OS. This could result in a denial of service in the best case, or code execution in the worst case. See NCC-NCC-016 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions. version 2.2.0 and later versions.	9.0	More Details
CVE-2020-11050	In Java-WebSocket less than or equal to 1.4.1, there is an Improper Validation of Certificate with Host Mismatch where WebSocketClient does not perform SSL hostname validation. This has been patched in 1.5.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-7267	Privilege Escalation vulnerability in McAfee VirusScan Enterprise (VSE) for Linux prior to 2.0.3 Hotfix 2635000 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	8.8	More Details
CVE-2020-6094	An exploitable code execution vulnerability exists in the TIFF fillinraster function of the igcore19d.dll library of Accusoft ImageGear 19.4, 19.5 and 19.6. A specially crafted TIFF file can cause an out-of-bounds write, resulting in remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2020-12760	An issue was discovered in OpenNMS Horizon before 26.0.1, and Meridian before 2018.1.19 and 2019 before 2019.1.7. The ActiveMQ channel configuration allowed for arbitrary deserialization of Java objects (aka ActiveMQ Minion payload deserialization), leading to remote code execution for any authenticated channel user regardless of its assigned permissions.	8.8	More Details
CVE-2020-11108	The Gravity updater in Pi-hole through 4.4 allows an authenticated adversary to upload arbitrary files. This can be abused for Remote Code Execution by writing to a PHP file in the web directory. (Also, it can be used in conjunction with the sudo rule for the www-data user to escalate privileges to root.) The code error is in gravity_DownloadBlocklistFromUrl in gravity.sh.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11531	The DataEngine Xnode Server application in Zoho ManageEngine DataSecurity Plus prior to 6.0.1 does not validate the database schema name when handling a DR-SCHEMA-SYNC request. This allows an authenticated attacker to execute code in the context of the product by writing a JSP file to the webroot directory via directory traversal.	8.8	More Details
CVE-2020-12669	core/get_menudiv.php in Dolibarr before 11.0.4 allows remote authenticated attackers to bypass intended access restrictions via a non-alphanumeric menu parameter.	8.8	More Details
CVE-2020-12689	An issue was discovered in OpenStack Keystone before 15.0.1, and 16.0.0. Any user authenticated within a limited scope (trust/oauth/application credential) can create an EC2 credential with an escalated permission, such as obtaining admin while the user is on a limited viewer role. This potentially allows a malicious user to act as the admin on a project another user has the admin role on, which can effectively grant that user global admin privileges.	8.8	More Details
CVE-2020-12690	An issue was discovered in OpenStack Keystone before 15.0.1, and 16.0.0. The list of roles provided for an OAuth1 access token is silently ignored. Thus, when an access token is used to request a keystone token, the keystone token contains every role assignment the creator had for the project. This results in the provided keystone token having more role assignments than the creator intended, possibly giving unintended escalated access.	8.8	More Details
CVE-2020-12691	An issue was discovered in OpenStack Keystone before 15.0.1, and 16.0.0. Any authenticated user can create an EC2 credential for themselves for a project that they have a specified role on, and then perform an update to the credential user and project, allowing them to masquerade as another user. This potentially allows a malicious user to act as the admin on a project another user has the admin role on, which can effectively grant that user global admin privileges.	8.8	More Details
CVE-2020-6081	An exploitable code execution vulnerability exists in the PLC_Task functionality of 3S-Smart Software Solutions GmbH CODESYS Runtime 3.5.14.30. A specially crafted network request can cause remote code execution. An attacker can send a malicious packet to trigger this vulnerability.	8.8	More Details
CVE-2019-18871	A path traversal in debug.php accessed via default.php in Blaauw Remote Kiln Control through v3.00r4 allows an authenticated attacker to upload arbitrary files, leading to arbitrary remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7266	Privilege Escalation vulnerability in McAfee VirusScan Enterprise (VSE) for Windows prior to 8.8 Patch 14 Hotfix 116778 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	8.8	More Details
CVE-2020-7265	Privilege Escalation vulnerability in McAfee Endpoint Security (ENS) for Mac prior to 10.6.9 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	8.8	More Details
CVE-2020-7264	Privilege Escalation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 Hotfix 199847 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	8.8	More Details
CVE-2020-12026	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. Multiple relative path traversal vulnerabilities exist that may allow a low privilege user to overwrite files outside the application’s control.	8.8	More Details
CVE-2020-6651	Improper Input Validation in Eaton's Intelligent Power Manager (IPM) v 1.67 & prior on file name during configuration file import functionality allows attackers to perform command injection or code execution via specially crafted file names while uploading the configuration file in the application.	8.8	More Details
CVE-2020-9474	The S. Siedle & Soehne SG 150-0 Smart Gateway before 1.2.4 allows remote code execution via the backup functionality in the web frontend. By using an exploit chain, an attacker with access to the network can get root access on the gateway.	8.8	More Details
CVE-2020-5897	In versions 7.1.5-7.1.9, there is use-after-free memory vulnerability in the BIG-IP Edge Client Windows ActiveX component.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10971	An issue was discovered on Wavlink Jetstream devices where a crafted POST request can be sent to adm.cgi that will result in the execution of the supplied command if there is an active session at the same time. The POST request itself is not validated to ensure it came from the active session. Affected devices are: Wavlink WN530HG4, Wavlink WN575A3, Wavlink WN579G3,Wavlink WN531G3, Wavlink WN533A8, Wavlink WN531A6, Wavlink WN551K1, Wavlink WN535G3, Wavlink WN530H4, Wavlink WN57X93, WN572HG3, Wavlink WN578A2, Wavlink WN579G3, Wavlink WN579X3, and Jetstream AC3000/ERAC3000	8.8	More Details
CVE-2020-6075	An exploitable out-of-bounds write vulnerability exists in the store_data_buffer function of the igcore19d.dll library of Accusoft ImageGear 19.5.0. A specially crafted PNG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	8.8	More Details
CVE-2020-6082	An exploitable out-of-bounds write vulnerability exists in the ico_read function of the igcore19d.dll library of Accusoft ImageGear 19.6.0. A specially crafted ICO file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	8.8	More Details
CVE-2020-6262	Service Data Download in SAP Application Server ABAP (ST-PI, before versions 2008_1_46C, 2008_1_620, 2008_1_640, 2008_1_700, 2008_1_710, 740) allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application and the whole ABAP system leading to Code Injection.	8.8	More Details
CVE-2020-12772	An issue was discovered in Ignite Realtime Spark 2.8.3 (and the ROAR plugin for it) on Windows. A chat message can include an IMG element with a SRC attribute referencing an external host's IP address. Upon access to this external host, the (NT)LM hashes of the user are sent with the HTTP request. This allows an attacker to collect these hashes, crack them, and potentially compromise the computer. (ROAR can be configured for automatic access. Also, access can occur if the user clicks.)	8.8	More Details
CVE-2020-6249	The use of an admin backend report within SAP Master Data Governance, versions - S4CORE 101, S4FND 102, 103, 104, SAP_BS_FND 748; allows an attacker to execute crafted database queries, exposing the backend database, leading to SQL Injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6076	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll ICO icoread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted ICO file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	8.8	More Details
CVE-2020-2189	Jenkins SCM Filter Jervis Plugin 0.2.1 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-6243	Under certain conditions, SAP Adaptive Server Enterprise (XP Server on Windows Platform), versions 15.7, 16.0, does not perform the necessary checks for an authenticated user while executing the extended stored procedure, allowing an attacker to read, modify, delete restricted data on connected servers, leading to Code Injection.	8.8	More Details
CVE-2020-6241	SAP Adaptive Server Enterprise, version 16.0, allows an authenticated user to execute crafted database queries to elevate privileges of users in the system, leading to SQL Injection.	8.8	More Details
CVE-2020-11072	In SLP Validate (npm package slp-validate) before version 1.2.1, users could experience false-negative validation outcomes for MINT transaction operations. A poorly implemented SLP wallet could allow spending of the affected tokens which would result in the destruction of a user's minting baton. This has been fixed in slp-validate in version 1.2.1. Additonally, slpjs version 0.27.2 has a related fix under related CVE-2020-11071.	8.6	More Details
CVE-2020-11071	SLPJS (npm package slpjs) before version 0.27.2, has a vulnerability where users could experience false-negative validation outcomes for MINT transaction operations. A poorly implemented SLP wallet could allow spending of the affected tokens which would result in the destruction of a user's minting baton. This is fixed in version 0.27.2.	8.6	More Details
CVE-2020-3283	A vulnerability in the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) handler of Cisco Firepower Threat Defense (FTD) Software when running on the Cisco Firepower 1000 Series platform could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. The vulnerability is due to a communication error between internal functions. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause a buffer underrun, which leads to a crash. The crash causes the affected device to reload.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3189	A vulnerability in the VPN System Logging functionality for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak that can deplete system memory over time, which can cause unexpected system behaviors or device crashes. The vulnerability is due to the system memory not being properly freed for a VPN System Logging event generated when a VPN session is created or deleted. An attacker could exploit this vulnerability by repeatedly creating or deleting a VPN tunnel connection, which could leak a small amount of system memory for each logging event. A successful exploit could allow the attacker to cause system memory depletion, which can lead to a systemwide denial of service (DoS) condition. The attacker does not have any control of whether VPN System Logging is configured or not on the device, but it is enabled by default.	8.6	More Details
CVE-2020-3196	A vulnerability in the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to exhaust memory resources on the affected device, leading to a denial of service (DoS) condition. The vulnerability is due to improper resource management for inbound SSL/TLS connections. An attacker could exploit this vulnerability by establishing multiple SSL/TLS connections with specific conditions to the affected device. A successful exploit could allow the attacker to exhaust the memory on the affected device, causing the device to stop accepting new SSL/TLS connections and resulting in a DoS condition for services on the device that process SSL/TLS traffic. Manual intervention is required to recover an affected device.	8.6	More Details
CVE-2020-3191	A vulnerability in DNS over IPv6 packet processing for Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to unexpectedly reload, resulting in a denial of service (DoS) condition. The vulnerability is due to improper length validation of a field in an IPv6 DNS packet. An attacker could exploit this vulnerability by sending a crafted DNS query over IPv6, which traverses the affected device. An exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to DNS over IPv6 traffic only.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11052	In Sorcery before 0.15.0, there is a brute force vulnerability when using password authentication via Sorcery. The brute force protection submodule will prevent a brute force attack for the defined lockout period, but once expired, protection will not be re-enabled until a user or malicious actor logs in successfully. This does not affect users that do not use the built-in brute force protection submodule, nor users that use permanent account lockout. This has been patched in 0.15.0.	8.3	More Details
CVE-2020-8153	Improper access control in Groupfolders app 4.0.3 allowed to delete hidden directories when when renaming an accessible item to the same name.	8.1	More Details
CVE-2020-3302	A vulnerability in the web UI of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to overwrite files on the file system of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by uploading a crafted file to the web UI on an affected device. A successful exploit could allow the attacker to overwrite files on the file system of the affected device.	8.1	More Details
CVE-2020-12785	cPanel before 86.0.14 allows attackers to obtain access to the current working directory via the account backup feature (SEC-540).	8.1	More Details
CVE-2020-5894	On versions 3.0.0-3.3.0, the NGINX Controller webserver does not invalidate the server-side session token after users log out.	8.1	More Details
CVE-2020-10021	Out-of-bounds Write in the USB Mass Storage memoryWrite handler with unaligned Sizes See NCC-ZEP-024, NCC-ZEP-025, NCC-ZEP-026 This issue affects: zephyrproject-rtos zephyr version 1.14.1 and later versions. version 2.1.0 and later versions.	8.1	More Details
CVE-2020-10019	USB DFU has a potential buffer overflow where the requested length (wLength) is not checked against the buffer size. This could be used by a malicious USB host to exploit the buffer overflow. See NCC-ZEP-002 This issue affects: zephyrproject-rtos zephyr version 1.14.1 and later versions. version 2.1.0 and later versions.	8.1	More Details
CVE-2020-6252	Under certain conditions SAP Adaptive Server Enterprise (Cockpit), version 16.0, allows an attacker with access to local network, to get sensitive and confidential information, leading to Information Disclosure. It can be used to get user account credentials, tamper with system data and impact system availability.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10060	In updatehub_probe, right after JSON parsing is complete, objects\[1] is accessed from the output structure in two different places. If the JSON contained less than two elements, this access would reference unitialized stack memory. This could result in a crash, denial of service, or possibly an information leak. Provided the fix in CVE-2020-10059 is applied, the attack requires compromise of the server. See NCC-ZEP-030 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions. version 2.2.0 and later versions.	8.0	More Details
CVE-2020-10916	This vulnerability allows network-adjacent attackers to escalate privileges on affected installations of TP-Link TL-WA855RE Firmware Ver: 855rev4-up-ver1-0-1-P1[20191213-rel60361] Wi-Fi extenders. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the first-time setup process. The issue results from the lack of proper validation on first-time setup requests. An attacker can leverage this vulnerability to reset the password for the Admin account and execute code in the context of the device. Was ZDI-CAN-10003.	8.0	More Details
CVE-2020-7290	Privilege Escalation vulnerability in McAfee Active Response (MAR) for Linux prior to 2.4.3 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2020-7291	Privilege Escalation vulnerability in McAfee Active Response (MAR) for Mac prior to 2.4.3 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2020-7289	Privilege Escalation vulnerability in McAfee Active Response (MAR) for Windows prior to 2.4.3 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2020-7288	Privilege Escalation vulnerability in McAfee Exploit Detection and Response (EDR) for Mac prior to 3.1.0 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2020-6244	SAP Business Client, version 7.0, allows an attacker after a successful social engineering attack to inject malicious code as a DLL file in untrusted directories that can be executed by the application, due to uncontrolled search path element. An attacker could thereby control the behavior of the application.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7287	Privilege Escalation vulnerability in McAfee Exploit Detection and Response (EDR) for Linux prior to 3.1.0 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2020-7806	Tobesoft Xplatform 9.2.2.250 and earlier version have an arbitrary code execution vulnerability by using method supported by Xplatform ActiveX Control. It allows attacker to cause remote code execution.	7.8	More Details
CVE-2020-5895	On NGINX Controller versions 3.1.0-3.3.0, AVRD uses world-readable and world-writable permissions on its socket, which allows processes or users on the local system to write arbitrary data into the socket. A local system attacker can make AVRD segmentation fault (SIGSEGV) by writing malformed messages to the socket.	7.8	More Details
CVE-2020-7286	Privilege Escalation vulnerability in McAfee Exploit Detection and Response (EDR) for Windows prior to 3.1.0 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2020-7285	Privilege Escalation vulnerability in McAfee MVISION Endpoint prior to 20.5.0.94 allows a malicious script or program to perform functions that the local executing user has not been granted access to.	7.8	More Details
CVE-2019-19166	Tobesoft XPlatform v9.1, 9.2.0, 9.2.1 and 9.2.2 have a vulnerability that can load unauthorized DLL files. It allows attacker to cause remote code execution.	7.8	More Details
CVE-2019-19169	Dext5.ocx ActiveX 5.0.0.116 and eariler versions contain a vulnerability, which could allow remote attacker to download arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution.	7.8	More Details
CVE-2019-19168	Dext5.ocx ActiveX 5.0.0.116 and eariler versions contain a vulnerability, which could allow remote attacker to download and execute remote arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution.	7.8	More Details
CVE-2020-6652	Incorrect Privilege Assignment vulnerability in Eaton's Intelligent Power Manager (IPM) v1.67 & prior allow non-admin users to upload the system configuration files by sending specially crafted requests. This can result in non-admin users manipulating the system configurations via uploading the configurations with incorrect parameters.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12608	An issue was discovered in SolarWinds MSP PME (Patch Management Engine) Cache Service before 1.1.15 in the Advanced Monitoring Agent. There are insecure file permissions for %PROGRAMDATA%\SolarWinds MSP\SolarWinds.MSP.CacheService\config\. This can lead to code execution by changing the CacheService.xml SISServerURL parameter.	7.8	More Details
CVE-2019-19167	Tobesoft Nexacro v2019.9.25.1 and earlier version have an arbitrary code execution vulnerability by using method supported by Nexacro14 ActiveX Control. It allows attacker to cause remote code execution.	7.8	More Details
CVE-2020-7803	IMGTech Co,Ltd ZInsX.ocx ActiveX Control in Zoneplayer 2.0.1.3, version 2.0.1.4 and prior versions on Windows. File Donwload vulnerability in ZInsX.ocx of IMGTech Co,Ltd Zoneplayer allows attacker to cause arbitrary code execution.	7.8	More Details
CVE-2018-20225	An issue was discovered in pip (all versions) because it installs the version with the highest version number, even if the user had intended to obtain a private package from a private index. This only affects use of the --extra-index-url option, and exploitation requires that the package does not already exist in the public index (and thus the attacker can put the package there with an arbitrary version number). NOTE: it has been reported that this is intended functionality and the user is responsible for using --extra-index-url securely	7.8	More Details
CVE-2020-12754	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A crafted application can obtain control of device input via the window system service. The LG ID is LVE-SMP-170011 (May 2020).	7.8	More Details
CVE-2020-5837	Symantec Endpoint Protection, prior to 14.3, may not respect file permissions when writing to log files that are replaced by symbolic links, which can lead to a potential elevation of privilege.	7.8	More Details
CVE-2020-12751	An issue was discovered on Samsung mobile devices with O(8.X), P(9.0), and Q(10.0) software. The Quram image codec library allows attackers to overwrite memory and execute arbitrary code via crafted JPEG data that is mishandled during decoding. The Samsung ID is SVE-2020-16943 (May 2020).	7.8	More Details
CVE-2020-10027	An attacker who has obtained code execution within a user thread is able to elevate privileges to that of the kernel. See NCC-ZEP-001 This issue affects: zephyrproject-rtos zephyr version 1.14.0 and later versions. version 2.1.0 and later versions.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10024	The arm platform-specific code uses a signed integer comparison when validating system call numbers. An attacker who has obtained code execution within a user thread is able to elevate privileges to that of the kernel. See NCC-ZEP-001 This issue affects: zephyrproject-rtos zephyr version 1.14.0 and later versions. version 2.1.0 and later versions.	7.8	More Details
CVE-2020-12762	json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.	7.8	More Details
CVE-2020-5836	Symantec Endpoint Protection, prior to 14.3, can potentially reset the ACLs on a file as a limited user while Symantec Endpoint Protection's Tamper Protection feature is disabled.	7.8	More Details
CVE-2019-19162	A use-after-free vulnerability in the TOBESOFT XPLATFORM versions 9.1 to 9.2.2 may lead to code execution on a system running it.	7.8	More Details
CVE-2020-10028	Multiple syscalls with insufficient argument validation See NCC-ZEP-006 This issue affects: zephyrproject-rtos zephyr version 1.14.0 and later versions. version 2.1.0 and later versions.	7.8	More Details
CVE-2020-5896	On versions 7.1.5-7.1.9, the BIG-IP Edge Client's Windows Installer Service's temporary folder has weak file and folder permissions.	7.8	More Details
CVE-2019-19164	dext5.ocx ActiveX Control in Dext5 Upload 5.0.0.112 and earlier versions contains a vulnerability that could allow remote files to be executed by setting the arguments to the activex method. A remote attacker could induce a user to access a crafted web page, causing damage such as malicious code infection.	7.8	More Details
CVE-2020-12749	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos chipsets) software. The S.LSI Wi-Fi drivers have a buffer overflow. The Samsung ID is SVE-2020-16906 (May 2020).	7.8	More Details
CVE-2020-11866	libEMF (aka ECMA-234 Metafile Library) through 1.0.11 allows a use-after-free.	7.8	More Details
CVE-2020-11865	libEMF (aka ECMA-234 Metafile Library) through 1.0.11 allows out-of-bounds memory access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5538	Improper Access Control in PALLET CONTROL Ver. 6.3 and earlier allows authenticated attackers to execute arbitrary code with the SYSTEM privilege on the computer where PALLET CONTROL is installed via unspecified vectors. PalletControl 7 to 9.1 are not affected by this vulnerability, however under the environment where PLS Management Add-on Module is used, all versions are affected.	7.8	More Details
CVE-2020-10058	Multiple syscalls in the Kscan subsystem perform insufficient argument validation, allowing code executing in userspace to potentially gain elevated privileges. See NCC-ZEP-006 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions.	7.8	More Details
CVE-2020-8154	An Insecure direct object reference vulnerability in Nextcloud Server 18.0.2 allowed an attacker to remote wipe devices of other users when sending a malicious request directly to the endpoint.	7.7	More Details
CVE-2020-10974	An issue was discovered affecting a backup feature where a crafted POST request returns the current configuration of the device in cleartext, including the administrator password. No authentication is required. Affected devices: Wavlink WN575A3, Wavlink WN579G3, Wavlink WN531A6, Wavlink WN535G3, Wavlink WN530H4, Wavlink WN57X93, Wavlink WN572HG3, Wavlink WN575A4, Wavlink WN578A2, Wavlink WN579G3, Wavlink WN579X3, and Jetstream AC3000/ERAC3000	7.5	More Details
CVE-2020-12116	Zoho ManageEngine OpManager Stable build before 124196 and Released build before 125125 allows an unauthenticated attacker to read arbitrary files on the server by sending a crafted request.	7.5	More Details
CVE-2020-10973	An issue was discovered in Wavlink WN530HG4, Wavlink WN531G3, Wavlink WN533A8, and Wavlink WN551K1 affecting /cgi-bin/ExportAllSettings.sh where a crafted POST request returns the current configuration of the device, including the administrator password. No authentication is required. The attacker must perform a decryption step, but all decryption information is readily available.	7.5	More Details
CVE-2020-1763	An out-of-bounds buffer read flaw was found in the pluto daemon of libreswan from versions 3.27 till 3.31 where, an unauthenticated attacker could use this flaw to crash libreswan by sending specially-crafted IKEv1 Informational Exchange packets. The daemon respawns after the crash.	7.5	More Details
CVE-2020-8151	There is a possible information disclosure issue in Active Resource <v5.1.1 that could allow an attacker to create specially crafted requests to access data in an unexpected way and possibly leak information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10972	An issue was discovered where a page is exposed that has the current administrator password in cleartext in the source code of the page. No authentication is required in order to reach the page (a certain live_?.shtml page with the variable syspasswd). Affected Devices: Wavlink WN530HG4, Wavlink WN531G3, and Wavlink WN572HG3	7.5	More Details
CVE-2020-10067	A malicious userspace application can cause a integer overflow and bypass security checks performed by system call handlers. The impact would depend on the underlying system call and can range from denial of service to information leak to memory corruption resulting in code execution within the kernel. See NCC-ZEP-005 This issue affects: zephyrproject-rtos zephyr version 1.14.1 and later versions. version 2.1.0 and later versions.	7.5	More Details
CVE-2020-6240	SAP NetWeaver AS ABAP (Web Dynpro ABAP), versions (SAP_UI 750, 752, 753, 754 and SAP_BASIS 700, 710, 730, 731, 804) allows an unauthenticated attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service leading to Denial of Service	7.5	More Details
CVE-2020-12014	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. Input is not properly sanitized and may allow an attacker to inject SQL commands.	7.5	More Details
CVE-2020-12018	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. An out-of-bounds vulnerability exists that may allow access to unauthorized data.	7.5	More Details
CVE-2020-9840	In SwiftNIO Extras before 1.4.1, a logic issue was addressed with improved restrictions.	7.5	More Details
CVE-2020-12790	In the SEOmatic plugin before 3.2.49 for Craft CMS, helpers/DynamicMeta.php does not properly sanitize the URL. This leads to Server-Side Template Injection and credentials disclosure via a crafted Twig template after a semicolon.	7.5	More Details
CVE-2019-5500	Certain versions of the NetApp Service Processor and Baseboard Management Controller firmware allow a remote unauthenticated attacker to cause a Denial of Service (DoS).	7.5	More Details
CVE-2020-6247	SAP Business Objects Business Intelligence Platform, version 4.2, allows an unauthenticated attacker to prevent legitimate users from accessing a service. Using a specially crafted request, the attacker can crash or flood the Central Management Server, thereby impacting system availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12752	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (with TEEGRIS) software. Attackers can determine user credentials via a brute-force attack against the Gatekeeper trustlet. The Samsung ID is SVE-2020-16908 (May 2020).	7.5	More Details
CVE-2020-12750	An issue was discovered on Samsung mobile devices with Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) via SPEN. The Samsung ID is SVE-2020-17019 (May 2020).	7.5	More Details
CVE-2020-12745	An issue was discovered on Samsung mobile devices with Q(10.0) software. Attackers can bypass the locked-state protection mechanism and access clipboard content via USSD. The Samsung ID is SVE-2019-16556 (May 2020).	7.5	More Details
CVE-2020-9315	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** Oracle iPlanet Web Server 7.0.x has Incorrect Access Control for admingui/version URIs in the Administration console, as demonstrated by unauthenticated read access to encryption keys. NOTE: a related support policy can be found in the www.oracle.com references attached to this CVE.	7.5	More Details
CVE-2020-12783	Exim through 4.93 has an out-of-bounds read in the SPA authenticator that could result in SPA/NTLM authentication bypass in auths/spa.c and auths/auth-spa.c.	7.5	More Details
CVE-2020-12672	GraphicsMagick through 1.3.35 has a heap-based buffer overflow in ReadMNGImage in coders/png.c.	7.5	More Details
CVE-2019-18872	Weak password requirements in Blaauw Remote Kiln Control through v3.00r4 allow a user to set short or guessable passwords (e.g., 1 or 1234).	7.5	More Details
CVE-2020-3255	A vulnerability in the packet processing functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a high rate of IPv4 or IPv6 traffic through an affected device. This traffic would need to match a configured block action in an access control policy. An exploit could allow the attacker to cause a memory exhaustion condition on the affected device, which would result in a DoS for traffic transiting the device, as well as sluggish performance of the management interface. Once the flood is stopped, performance should return to previous states.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10704	A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.	7.5	More Details
CVE-2020-8983	An arbitrary file write issue exists in all versions of Citrix ShareFile StorageZones (aka storage zones) Controller, including the most recent 5.10.x releases as of May 2020, which allows remote code execution. RCE and file access is granted to everything hosted by ShareFile, be it on-premise or inside Citrix Cloud itself (both are internet facing). NOTE: unlike most CVEs, exploitability depends on the product version that was in use when a particular setup step was performed, NOT the product version that is in use during a current assessment of a CVE consumer's product inventory. Specifically, the vulnerability can be exploited if a storage zone was created by one of these product versions: 5.9.0, 5.8.0, 5.7.0, 5.6.0, 5.5.0, or earlier. This CVE differs from CVE-2020-7473 and CVE-2020-8982.	7.5	More Details
CVE-2020-8982	An unauthenticated arbitrary file read issue exists in all versions of Citrix ShareFile StorageZones (aka storage zones) Controller, including the most recent 5.10.x releases as of May 2020. RCE and file access is granted to everything hosted by ShareFile, be it on-premise or inside Citrix Cloud itself (both are internet facing). NOTE: unlike most CVEs, exploitability depends on the product version that was in use when a particular setup step was performed, NOT the product version that is in use during a current assessment of a CVE consumer's product inventory. Specifically, the vulnerability can be exploited if a storage zone was created by one of these product versions: 5.9.0, 5.8.0, 5.7.0, 5.6.0, 5.5.0, or earlier. This CVE differs from CVE-2020-7473 and CVE-2020-8983.	7.5	More Details
CVE-2020-7473	In certain situations, all versions of Citrix ShareFile StorageZones (aka storage zones) Controller, including the most recent 5.10.x releases as of May 2020, allow unauthenticated attackers to access the documents and folders of ShareFile users. NOTE: unlike most CVEs, exploitability depends on the product version that was in use when a particular setup step was performed, NOT the product version that is in use during a current assessment of a CVE consumer's product inventory. Specifically, the vulnerability can be exploited if a storage zone was created by one of these product versions: 5.9.0, 5.8.0, 5.7.0, 5.6.0, 5.5.0, or earlier. This CVE differs from CVE-2020-8982 and CVE-2020-8983 but has essentially the same risk.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18866	Unauthenticated SQL injection via the username in the login mechanism in Blaauw Remote Kiln Control through v3.00r4 allows a user to extract arbitrary data from the rkc database.	7.5	More Details
CVE-2019-18864	/server-info and /server-status in Blaauw Remote Kiln Control through v3.00r4 allow an unauthenticated attacker to gain sensitive information about the host machine.	7.5	More Details
CVE-2019-18867	Browsable directories in Blaauw Remote Kiln Control through v3.00r4 allow an attacker to enumerate sensitive filenames and locations, including source code. This affects /ajax/, /common/, /engine/, /flash/, /images/, /Images/, /jscripts/, /lang/, /layout/, /programs/, and /sms/.	7.5	More Details
CVE-2018-5493	ATTO FibreBridge 7500N firmware versions prior to 2.90 are susceptible to a vulnerability which allows an unauthenticated remote attacker to cause Denial of Service (DoS).	7.5	More Details
CVE-2020-3179	A vulnerability in the generic routing encapsulation (GRE) tunnel decapsulation feature of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory handling error when GRE over IPv6 traffic is processed. An attacker could exploit this vulnerability by sending crafted GRE over IPv6 packets with either IPv4 or IPv6 payload through an affected device. A successful exploit could allow the attacker to cause the device to crash, resulting in a DoS condition.	7.5	More Details
CVE-2020-3254	Multiple vulnerabilities in the Media Gateway Control Protocol (MGCP) inspection feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerabilities are due to inefficient memory management. An attacker could exploit these vulnerabilities by sending crafted MGCP packets through an affected device. An exploit could allow the attacker to cause memory exhaustion resulting in a restart of an affected device, causing a DoS condition for traffic traversing the device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3195	A vulnerability in the Open Shortest Path First (OSPF) implementation in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device. The vulnerability is due to incorrect processing of certain OSPF packets. An attacker could exploit this vulnerability by sending a series of crafted OSPF packets to be processed by an affected device. A successful exploit could allow the attacker to continuously consume memory on an affected device and eventually cause it to reload, resulting in a denial of service (DoS) condition.	7.5	More Details
CVE-2020-3259	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve memory contents on an affected device, which could lead to the disclosure of confidential information. The vulnerability is due to a buffer tracking issue when the software parses invalid URLs that are requested from the web services interface. An attacker could exploit this vulnerability by sending a crafted GET request to the web services interface. A successful exploit could allow the attacker to retrieve memory contents, which could lead to the disclosure of confidential information. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	7.5	More Details
CVE-2020-3298	A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper memory protection mechanisms while processing certain OSPF packets. An attacker could exploit this vulnerability by sending a series of malformed OSPF packets in a short period of time to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.	7.5	More Details
CVE-2020-3303	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3305	A vulnerability in the implementation of the Border Gateway Protocol (BGP) module in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain BGP packets. An attacker could exploit this vulnerability by sending a crafted BGP packet. A successful exploit could allow the attacker to cause a DoS condition on the affected device.	7.5	More Details
CVE-2020-3306	A vulnerability in the DHCP module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to incorrect processing of certain DHCP packets. An attacker could exploit this vulnerability by sending a crafted DHCP packet to the affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.	7.5	More Details
CVE-2020-3312	A vulnerability in the application policy configuration of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data on an affected device. The vulnerability is due to insufficient application identification. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain unauthorized read access to sensitive data.	7.5	More Details
CVE-2020-11060	In GLPI before 9.4.6, an attacker can execute system commands by abusing the backup functionality. Theoretically, this vulnerability can be exploited by an attacker without a valid account by using a CSRF. Due to the difficulty of the exploitation, the attack is only conceivable by an account having Maintenance privileges and the right to add WIFI networks. This is fixed in version 9.4.6.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3334	A vulnerability in the ARP packet processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Security Appliances could allow an unauthenticated, adjacent attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect processing of ARP packets received by the management interface of an affected device. An attacker could exploit this vulnerability by sending a series of unicast ARP packets in a short timeframe that would reach the management interface of an affected device. A successful exploit could allow the attacker to consume resources on an affected device, which would prevent the device from sending internal system keepalives and eventually cause the device to reload, resulting in a denial of service (DoS) condition.	7.4	More Details
CVE-2020-11056	In Sprout Forms before 3.9.0, there is a potential Server-Side Template Injection vulnerability when using custom fields in Notification Emails which could lead to the execution of Twig code. This has been fixed in 3.9.0.	7.4	More Details
CVE-2020-5745	Cross-site request forgery in TCExam 14.2.2 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link.	7.4	More Details
CVE-2015-7946	Information Exposure vulnerability in Unity8 as used on the Ubuntu phone and possibly also in Unity8 shipped elsewhere. This allows an attacker to enable the MTP service by opening the emergency dialer. Fixed in 8.11+16.04.20160111.1-0ubuntu1 and 8.11+15.04.20160122-0ubuntu1.	7.3	More Details
CVE-2020-5741	Deserialization of Untrusted Data in Plex Media Server on Windows allows a remote, authenticated attacker to execute arbitrary Python code.	7.2	More Details
CVE-2020-3309	A vulnerability in Cisco Firepower Device Manager (FDM) On-Box software could allow an authenticated, remote attacker to overwrite arbitrary files on the underlying operating system of an affected device. The vulnerability is due to improper input validation. An attacker could exploit this vulnerability by uploading a malicious file to an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on as well as modify the underlying operating system of an affected device.	7.2	More Details
CVE-2020-6248	SAP Adaptive Server Enterprise (Backup Server), version 16.0, does not perform the necessary validation checks for an authenticated user while executing DUMP or LOAD command allowing arbitrary code execution or Code Injection.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6253	Under certain conditions, SAP Adaptive Server Enterprise (Web Services), versions 15.7, 16.0, allows an authenticated user to execute crafted database queries to elevate their privileges, modify database objects, or execute commands they are not otherwise authorized to execute, leading to SQL Injection.	7.2	More Details
CVE-2020-5248	GLPI before before version 9.4.6 has a vulnerability involving a default encryption key. GLPIKEY is public and is used on every instance. This means anyone can decrypt sensitive data stored using this key. It is possible to change the key before installing GLPI. But on existing instances, data must be reencrypted with the new key. Problem is we can not know which columns or rows in the database are using that; espcially from plugins. Changing the key without updating data would lend in bad password sent from glpi; but storing them again from the UI will work.	7.2	More Details
CVE-2020-12719	XXE during an EventPublisher update can occur in Management Console in WSO2 API Manager 3.0.0 and earlier, API Manager Analytics 2.5.0 and earlier, API Microgateway 2.2.0, Enterprise Integrator 6.4.0 and earlier, IS as Key Manager 5.9.0 and earlier, Identity Server 5.9.0 and earlier, and Identity Server Analytics 5.6.0 and earlier.	7.2	More Details
CVE-2020-10795	Gira TKS-IP-Gateway 4.0.7.7 is vulnerable to authenticated remote code execution via the backup functionality of the web frontend. This can be combined with CVE-2020-10794 for remote root access.	7.2	More Details
CVE-2020-12010	Advantech WebAccess Node, Version 8.4.4 and prior, Version 9.0.0. Multiple relative path traversal vulnerabilities exist that may allow an authenticated user to use a specially crafted file to delete files outside the application’s control.	7.1	More Details
CVE-2020-1718	A flaw was found in the reset credential flow in all Keycloak versions before 8.0.0. This flaw allows an attacker to gain unauthorized access to the application.	7.1	More Details
CVE-2020-12825	libcroco through 0.6.13 has excessive recursion in cr_parser_parse_any_core in cr-parser.c, leading to stack consumption.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11053	In OAuth2 Proxy before 5.1.1, there is an open redirect vulnerability. Users can provide a redirect address for the proxy to send the authenticated user to at the end of the authentication flow. This is expected to be the original URL that the user was trying to access. This redirect URL is checked within the proxy and validated before redirecting the user to prevent malicious actors providing redirects to potentially harmful sites. However, by crafting a redirect URL with HTML encoded whitespace characters the validation could be bypassed and allow a redirect to any URL provided. This has been patched in 5.1.1.	7.1	More Details
CVE-2020-5835	Symantec Endpoint Protection Manager, prior to 14.3, has a race condition in client remote deployment which may result in an elevation of privilege on the remote machine.	7.0	More Details
CVE-2020-9475	The S. Siedle & Soehne SG 150-0 Smart Gateway before 1.2.4 allows local privilege escalation via a race condition in logrotate. By using an exploit chain, an attacker with access to the network can get root access on the gateway.	7.0	More Details
CVE-2019-14898	The fix for CVE-2019-11599, affecting the Linux kernel before 5.0.10 was not complete. A local user could use this flaw to obtain sensitive information, cause a denial of service, or possibly have other unspecified impacts by triggering a race condition with mmget_not_zero or get_task_mm calls.	7.0	More Details
CVE-2020-8156	A missing verification of the TLS host in Nextcloud Mail 1.1.3 allowed a man in the middle attack.	7.0	More Details
CVE-2020-10023	The shell subsystem contains a buffer overflow, whereby an adversary with physical access to the device is able to cause a memory corruption, resulting in denial of service or possibly code execution within the Zephyr kernel. See NCC-NCC-019 This issue affects: zephyrproject-rtos zephyr version 1.14.0 and later versions. version 2.1.0 and later versions.	6.9	More Details
CVE-2020-6250	SAP Adaptive Server Enterprise, version 16.0, allows an authenticated attacker to exploit certain misconfigured endpoints exposed over the adjacent network, to read system administrator password leading to Information Disclosure. This could help the attacker to read/write any data and even stop the server like an administrator.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3253	A vulnerability in the support tunnel feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to access the shell of an affected device even though expert mode is disabled. The vulnerability is due to improper configuration of the support tunnel feature. An attacker could exploit this vulnerability by enabling the support tunnel, setting a key, and deriving the tunnel password. A successful exploit could allow the attacker to run any system command with root access on an affected device.	6.7	More Details
CVE-2020-6245	SAP Business Objects Business Intelligence Platform, version 4.2, allows an attacker with access to local instance, to inject file or code that can be executed by the application due to Improper Control of Resource Identifiers.	6.7	More Details
CVE-2020-12770	An issue was discovered in the Linux kernel through 5.6.11. sg_write lacks an sg_remove_request call in a certain failure case, aka CID-83c6f2390040.	6.7	More Details
CVE-2019-10170	A flaw was found in the Keycloak admin console, where the realm management interface permits a script to be set via the policy. This flaw allows an attacker with authenticated user and realm management permissions to configure a malicious script to trigger and execute arbitrary code with the permissions of the application user.	6.6	More Details
CVE-2019-10169	A flaw was found in Keycloak's user-managed access interface, where it would permit a script to be set in the UMA policy. This flaw allows an authenticated attacker with UMA permissions to configure a malicious script to trigger and execute arbitrary code with the permissions of the user running application.	6.6	More Details
CVE-2020-2181	Jenkins Credentials Binding Plugin 1.22 and earlier does not mask (i.e., replace with asterisks) secrets in the build log when the build contains no build steps.	6.5	More Details
CVE-2020-2183	Jenkins Copy Artifact Plugin 1.43.1 and earlier performs improper permission checks, allowing attackers to copy artifacts from jobs they have no permission to access.	6.5	More Details
CVE-2020-12108	/options/mailman in GNU Mailman before 2.1.31 allows Arbitrary Content Injection.	6.5	More Details
CVE-2019-4478	IBM Maximo Asset Management 7.6.0, and 7.6.1 could allow an authenticated user to obtain highly sensitive information that they should not normally have access to. IBM X-Force ID: 163998.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6251	Under certain conditions or error scenarios SAP Business Objects Business Intelligence Platform, version 4.2, allows an attacker to access information which would otherwise be restricted.	6.5	More Details
CVE-2020-10690	There is a use-after-free in kernel versions before 5.5 due to a race condition between the release of ptp_clock and cdev while resource deallocation. When a (high privileged) process allocates a ptp device file (like /dev/ptpX) and voluntarily goes to sleep. During this time if the underlying device is removed, it can cause an exploitable condition as the process wakes up to terminate and clean all attached files. The system crashes due to the cdev structure being invalid (as already freed) which is pointed to by the inode.	6.5	More Details
CVE-2020-6258	SAP Identity Management, version 8.0, does not perform necessary authorization checks for an authenticated user, allowing the attacker to view certain sensitive information of the victim, leading to Missing Authorization Check.	6.5	More Details
CVE-2019-18870	A path traversal via the iniFile parameter in excel.php in Blaauw Remote Kiln Control through v3.00r4 allows an authenticated attacker to download arbitrary files from the host machine.	6.5	More Details
CVE-2020-12737	An issue was discovered in Maxum Rumpus before 8.2.12 on macOS. Authenticated users can perform a path traversal using double escaped characters, enabling read access to arbitrary files on the server.	6.5	More Details
CVE-2020-6616	Some Broadcom chips mishandle Bluetooth random-number generation because a low-entropy Pseudo Random Number Generator (PRNG) is used in situations where a Hardware Random Number Generator (HRNG) should have been used to prevent spoofing. This affects, for example, Samsung Galaxy S8, S8+, and Note8 devices with the BCM4361 chipset. The Samsung ID is SVE-2020-16882 (May 2020).	6.5	More Details
CVE-2020-12687	An issue was discovered in Serpico before 1.3.3. The /admin/attacments_backup endpoint can be requested by non-admin authenticated users. This means that an attacker with a user account can retrieve all of the attachments of all users (including administrators) from the database.	6.5	More Details
CVE-2020-6259	Under certain conditions SAP Adaptive Server Enterprise, versions 15.7, 16.0, allows an attacker to access information which would otherwise be restricted leading to Missing Authorization Check.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11055	In BookStack greater than or equal to 0.18.0 and less than 0.29.2, there is an XSS vulnerability in comment creation. A user with permission to create comments could POST HTML directly to the system to be saved in a comment, which would then be executed/displayed to others users viewing the comment. Through this vulnerability custom JavaScript code could be injected and therefore ran on other user machines. This most impacts scenarios where not-trusted users are given permission to create comments. This has been fixed in 0.29.2.	6.3	More Details
CVE-2020-10706	A flaw was found in OpenShift Container Platform where OAuth tokens are not encrypted when the encryption of data at rest is enabled. This flaw allows an attacker with access to a backup to obtain OAuth tokens and then use them to log into the cluster as any user who logged into the cluster via the WebUI or via the command line in the last 24 hours. Once the backup is older than 24 hours the OAuth tokens are no longer valid.	6.3	More Details
CVE-2020-6254	SAP Enterprise Threat Detection, versions 1.0, 2.0, does not sufficiently encode error response pages in case of errors, allowing XSS payload reflecting in the response, leading to reflected Cross Site Scripting.	6.1	More Details
CVE-2020-5748	Insufficient output sanitization in TCExam 14.2.2 allows a remote, unauthenticated attacker to conduct persistent cross-site scripting (XSS) attacks via the self-registration feature.	6.1	More Details
CVE-2020-3313	A vulnerability in the web UI of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the FMC Software. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or to access sensitive, browser-based information.	6.1	More Details
CVE-2020-5750	Insufficient output sanitization in TCExam 14.2.2 allows a remote, unauthenticated attacker to conduct persistent cross-site scripting (XSS) attacks via the self-registration feature.	6.1	More Details
CVE-2020-3311	A vulnerability in the web interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by intercepting and modifying an HTTP request from a user. A successful exploit could allow the attacker to redirect the user to a specific malicious web page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11727	A cross-site scripting (XSS) vulnerability in the AlgolPlus Advanced Order Export For WooCommerce plugin 3.1.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the view/settings-form.php woe_post_type parameter.	6.1	More Details
CVE-2020-12703	UliCMS before 2020.2 has XSS during PackageController uninstall.	6.1	More Details
CVE-2020-12704	UliCMS before 2020.2 has PageController stored XSS.	6.1	More Details
CVE-2020-12705	Multiple cross-site scripting (XSS) vulnerabilities exist in LeptonCMS before 4.6.0.	6.1	More Details
CVE-2020-3178	Multiple vulnerabilities in the web-based GUI of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA) could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerabilities are due to improper input validation of the parameters of an HTTP request. An attacker could exploit these vulnerabilities by intercepting an HTTP request and modifying it to redirect a user to a specific malicious URL. A successful exploit could allow the attacker to redirect a user to a malicious web page or to obtain sensitive browser-based information. This type of attack is commonly referred to as an open redirect attack and is used in phishing attacks to get users to unknowingly visit malicious sites.	6.1	More Details
CVE-2020-12696	The iframe plugin before 4.5 for WordPress does not sanitize a URL.	6.1	More Details
CVE-2020-12679	A reflected cross-site scripting (XSS) vulnerability in the Mitel ShoreTel Conference Web Application 19.50.1000.0 before MiVoice Connect 18.7 SP2 allows remote attackers to inject arbitrary JavaScript and HTML via the PATH_INFO to home.php.	6.1	More Details
CVE-2020-12707	An XSS vulnerability exists in modules/wysiwyg/save.php of LeptonCMS 4.5.0. This can be exploited because the only security measure used against XSS is the stripping of SCRIPT elements. A malicious actor can use HTML event handlers to run JavaScript instead of using SCRIPT elements.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12708	Multiple cross-site scripting vulnerabilities in PHP-Fusion 9.03.50 allow remote attackers to inject arbitrary web script or HTML via the cat_id parameter to downloads/downloads.php or article.php. NOTE: this might overlap CVE-2012-6043.	6.1	More Details
CVE-2020-11062	In GLPI after 0.68.1 and before 9.4.6, multiple reflexive XSS occur in Dropdown endpoints due to an invalid Content-Type. This has been fixed in version 9.4.6.	6.0	More Details
CVE-2019-4667	IBM UrbanCode Deploy (UCD) 7.0.5.2 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: 171249.	5.9	More Details
CVE-2014-1423	signond before 8.57+15.04.20141127.1-0ubuntu1, as used in Ubuntu Touch, did not properly restrict applications from querying oath tokens due to incorrect checks and the missing installation of the signon-apparmor-extension. An attacker could use this create a malicious click app that collects oauth tokens for other applications, exposing sensitive information.	5.9	More Details
CVE-2020-3285	A vulnerability in the Transport Layer Security version 1.3 (TLS 1.3) policy with URL category functionality for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured TLS 1.3 policy to block traffic for a specific URL. The vulnerability is due to a logic error with Snort handling of the connection with the TLS 1.3 policy and URL category configuration. An attacker could exploit this vulnerability by sending crafted TLS 1.3 connections to an affected device. A successful exploit could allow the attacker to bypass the TLS 1.3 policy and access URLs that are outside the affected device and normally would be dropped.	5.8	More Details
CVE-2020-2185	Jenkins Amazon EC2 Plugin 1.50.1 and earlier does not validate SSH host keys when connecting agents, enabling man-in-the-middle attacks.	5.6	More Details
CVE-2020-2187	Jenkins Amazon EC2 Plugin 1.50.1 and earlier unconditionally accepts self-signed certificates and does not perform hostname validation, enabling man-in-the-middle attacks.	5.6	More Details
CVE-2020-12769	An issue was discovered in the Linux kernel before 5.4.17. drivers/spi/spi-dw.c allows attackers to cause a panic via concurrent calls to dw_spi_irq and dw_spi_transfer_one, aka CID-19b61392c5a8.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12767	exif_entry_get_value in exif-entry.c in libexif 0.6.21 has a divide-by-zero error.	5.5	More Details
CVE-2020-11864	libEMF (aka ECMA-234 Metafile Library) through 1.0.11 allows denial of service (issue 2 of 2).	5.5	More Details
CVE-2020-12771	An issue was discovered in the Linux kernel through 5.6.11. btree_gc_coalesce in drivers/md/bcache/btree.c has a deadlock if a coalescing operation fails.	5.5	More Details
CVE-2020-6861	A flawed protocol design in the Ledger Monero app before 1.5.1 for Ledger Nano and Ledger S devices allows a local attacker to extract the master spending key by sending crafted messages to this app selected on a PIN-entered Ledger connected to a host PC.	5.5	More Details
CVE-2020-11863	libEMF (aka ECMA-234 Metafile Library) through 1.0.11 allows denial of service (issue 1 of 2).	5.5	More Details
CVE-2020-5898	In versions 7.1.5-7.1.9, BIG-IP Edge Client Windows Stonewall driver does not sanitize the pointer received from the userland. A local user on the Windows client system can send crafted DeviceIoControl requests to \\.\urvpndrv device causing the Windows kernel to crash.	5.5	More Details
CVE-2020-12768	An issue was discovered in the Linux kernel before 5.6. svm_cpu_uninit in arch/x86/kvm/svm.c has a memory leak, aka CID-d80b64ff297e. NOTE: third parties dispute this issue because it's a one-time leak at the boot, the size is negligible, and it can't be triggered at will	5.5	More Details
CVE-2020-11541	In TechSmith SnagIt 11.2.1 through 20.0.3, an XML External Entity (XXE) injection issue exists that would allow a local attacker to exfiltrate data under the local Administrator account.	5.5	More Details
CVE-2020-11042	In FreeRDP greater than 1.1 and before 2.0.0, there is an out-of-bounds read in update_read_icon_info. It allows reading a attacker-defined amount of client memory (32bit unsigned -> 4GB) to an intermediate buffer. This can be used to crash the client or store information for later retrieval. This has been patched in 2.0.0.	5.5	More Details
CVE-2020-11046	In FreeRDP after 1.0 and before 2.0.0, there is a stream out-of-bounds seek in update_read_synchronize that could lead to a later out-of-bounds read.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11047	In FreeRDP after 1.1 and before 2.0.0, there is an out-of-bounds read in autodetect_recv_bandwidth_measure_results. A malicious server can extract up to 8 bytes of client memory with a manipulated message by providing a short input and reading the measurement result data. This has been patched in 2.0.0.	5.5	More Details
CVE-2020-11049	In FreeRDP after 1.1 and before 2.0.0, there is an out-of-bound read of client memory that is then passed on to the protocol parser. This has been patched in 2.0.0.	5.5	More Details
CVE-2020-12680	Avira Free Antivirus through 15.0.2005.1866 allows local users to discover user credentials. The functions of the executable file Avira.PWM.NativeMessaging.exe are aimed at collecting credentials stored in Chrome, Firefox, Opera, and Edge. The executable does not verify the calling program and thus a request such as fetchChromePasswords or fetchCredentials will succeed. NOTE: some third parties have stated that this is "not a vulnerability.	5.5	More Details
CVE-2020-5751	Insufficient output sanitization in TCExam 14.2.2 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks by creating a crafted operator.	5.4	More Details
CVE-2020-4195	IBM API Connect V2018.4.1.0 through 2018.4.1.10 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: 174859.	5.4	More Details
CVE-2020-12692	An issue was discovered in OpenStack Keystone before 15.0.1, and 16.0.0. The EC2 API doesn't have a signature TTL check for AWS Signature V4. An attacker can sniff the Authorization header, and then use it to reissue an OpenStack token an unlimited number of times.	5.4	More Details
CVE-2020-4421	IBM WebSphere Application Liberty 19.0.0.5 through 20.0.0.4 could allow an authenticated user using openidconnect to spoof another users identify. IBM X-Force ID: 180084.	5.4	More Details
CVE-2020-4384	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 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: 179265.	5.4	More Details
CVE-2020-8155	An outdated 3rd party library in the Files PDF viewer for Nextcloud Server 18.0.2 caused a Cross-site scripting vulnerability when opening a malicious PDF.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12683	Katyshop2 before 2.12 has multiple stored XSS issues.	5.4	More Details
CVE-2020-12718	In administration/comments.php in PHP-Fusion 9.03.50, an authenticated attacker can take advantage of a stored XSS vulnerability in the Preview Comment feature. The protection mechanism can be bypassed by using HTML event handlers such as ontoggle.	5.4	More Details
CVE-2020-12706	Multiple Cross-site scripting vulnerabilities in PHP-Fusion 9.03.50 allow remote attackers to inject arbitrary web script or HTML via the go parameter to faq/faq_admin.php or shoutbox_panel/shoutbox_admin.php	5.4	More Details
CVE-2020-6257	SAP Business Objects Business Intelligence Platform (CMC and BI Launchpad) 4.2 does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability.	5.4	More Details
CVE-2020-5746	Insufficient output sanitization in TCExam 14.2.2 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks by creating a crafted test.	5.4	More Details
CVE-2020-5747	Insufficient output sanitization in TCExam 14.2.2 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks by creating a crafted test.	5.4	More Details
CVE-2020-5749	Insufficient output sanitization in TCExam 14.2.2 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks by creating a crafted group.	5.4	More Details
CVE-2020-10693	A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.	5.3	More Details
CVE-2020-12784	cPanel before 86.0.14 allows remote attackers to trigger a bandwidth suspension via mail log strings (SEC-505).	5.3	More Details
CVE-2020-4346	IBM API Connect's V2018.4.1.0 through 2018.4.1.10 management server has an unsecured api which can be exploited by an unauthenticated attacker to obtain sensitive information. IBM X-Force ID: 178322.	5.3	More Details
CVE-2020-12448	GitLab EE 12.8 and later allows Exposure of Sensitive Information to an Unauthorized Actor via NuGet.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4092	"If port encryption is not enabled on the Domino Server, HCL Nomad on Android and iOS Platforms will communicate in clear text and does not currently have a user interface option to change the setting to request an encrypted communication channel with the Domino server. This can potentially expose sensitive information including but not limited to server names, user IDs and document content."	5.3	More Details
CVE-2020-12826	A signal access-control issue was discovered in the Linux kernel before 5.6.5, aka CID-7395ea4e65c2. Because exec_id in include/linux/sched.h is only 32 bits, an integer overflow can interfere with a do_notify_parent protection mechanism. A child process can send an arbitrary signal to a parent process in a different security domain. Exploitation limitations include the amount of elapsed time before an integer overflow occurs, and the lack of scenarios where signals to a parent process present a substantial operational threat.	5.3	More Details
CVE-2019-18865	Information disclosure via error message discrepancies in authentication functions in Blaauw Remote Kiln Control through v3.00r4 allows an unauthenticated attacker to enumerate valid usernames.	5.3	More Details
CVE-2020-3186	A vulnerability in the management access list configuration of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured management interface access list on an affected system. The vulnerability is due to the configuration of different management access lists, with ports allowed in one access list and denied in another. An attacker could exploit this vulnerability by sending crafted remote management traffic to the local IP address of an affected system. A successful exploit could allow the attacker to bypass the configured management access list policies, and traffic to the management interface would not be properly denied.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3188	A vulnerability in how Cisco Firepower Threat Defense (FTD) Software handles session timeouts for management connections could allow an unauthenticated, remote attacker to cause a buildup of remote management connections to an affected device, which could result in a denial of service (DoS) condition. The vulnerability exists because the default session timeout period for specific to-the-box remote management connections is too long. An attacker could exploit this vulnerability by sending a large and sustained number of crafted remote management connections to an affected device, resulting in a buildup of those connections over time. A successful exploit could allow the attacker to cause the remote management interface or Cisco Firepower Device Manager (FDM) to stop responding and cause other management functions to go offline, resulting in a DoS condition. The user traffic that is flowing through the device would not be affected, and the DoS condition would be isolated to remote management only.	5.3	More Details
CVE-2020-7647	All versions before 1.6.7 and all versions after 2.0.0 inclusive and before 2.8.2 of io.jooby:jooby and org.jooby:jooby are vulnerable to Directory Traversal via two separate vectors.	5.3	More Details
CVE-2020-5834	Symantec Endpoint Protection Manager, prior to 14.3, may be susceptible to a directory traversal attack that could allow a remote actor to determine the size of files in the directory.	5.3	More Details
CVE-2018-8956	ntpd in ntp 4.2.8p10, 4.2.8p11, 4.2.8p12 and 4.2.8p13 allow remote attackers to prevent a broadcast client from synchronizing its clock with a broadcast NTP server via soofed mode 3 and mode 5 packets. The attacker must either be a part of the same broadcast network or control a slave in that broadcast network that can capture certain required packets on the attacker's behalf and send them to the attacker.	5.3	More Details
CVE-2020-12748	An issue was discovered on Samsung mobile devices with Q(10.0) software. Attackers can bypass the locked-state protection mechanism and designate a different preferred SIM card. The Samsung ID is SVE-2020-16594 (May 2020).	5.3	More Details
CVE-2020-12764	Gnuteca 3.8 allows file.php?folder=/&file= Directory Traversal.	5.3	More Details
CVE-2020-12765	Solis Miolo 2.0 allows index.php?module=install&action=view&item= Directory Traversal.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3315	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass the configured file policies on an affected system. The vulnerability is due to errors in how the Snort detection engine handles specific HTTP responses. An attacker could exploit this vulnerability by sending crafted HTTP packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured file policies and deliver a malicious payload to the protected network.	5.3	More Details
CVE-2020-3307	A vulnerability in the web UI of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to write arbitrary entries to the log file on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to send incorrect information to the system log on the affected system.	5.3	More Details
CVE-2020-1698	A flaw was found in keycloak in versions before 9.0.0. A logged exception in the HttpMethod class may leak the password given as parameter. The highest threat from this vulnerability is to data confidentiality.	5.0	More Details
CVE-2020-1746	A flaw was found in the Ansible Engine affecting Ansible Engine versions 2.7.x before 2.7.17 and 2.8.x before 2.8.11 and 2.9.x before 2.9.7 as well as Ansible Tower before and including versions 3.4.5 and 3.5.5 and 3.6.3 when the ldap_attr and ldap_entry community modules are used. The issue discloses the LDAP bind password to stdout or a log file if a playbook task is written using the bind_pw in the parameters field. The highest threat from this vulnerability is data confidentiality.	5.0	More Details
CVE-2020-10685	A flaw was found in Ansible Engine affecting Ansible Engine versions 2.7.x before 2.7.17 and 2.8.x before 2.8.11 and 2.9.x before 2.9.7 as well as Ansible Tower before and including versions 3.4.5 and 3.5.5 and 3.6.3 when using modules which decrypts vault files such as assemble, script, unarchive, win_copy, aws_s3 or copy modules. The temporary directory is created in /tmp leaves the s ts unencrypted. On Operating Systems which /tmp is not a tmpfs but part of the root partition, the directory is only cleared on boot and the decryp emains when the host is switched off. The system will be vulnerable when the system is not running. So decrypted data must be cleared as soon as possible and the data which normally is encrypted ble.	5.0	More Details
CVE-2012-0953	A race condition was discovered in the Linux drivers for Nvidia graphics which allowed an attacker to exfiltrate kernel memory to userspace. This issue was fixed in version 295.53.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-0952	A heap buffer overflow was discovered in the device control ioctl in the Linux driver for Nvidia graphics cards, which may allow an attacker to overflow 49 bytes. This issue was fixed in version 295.53.	5.0	More Details
CVE-2020-5744	Relative Path Traversal in TCExam 14.2.2 allows a remote, authenticated attacker to read the contents of arbitrary files on disk.	4.9	More Details
CVE-2020-3310	A vulnerability in the XML parser code of Cisco Firepower Device Manager On-Box software could allow an authenticated, remote attacker to cause an affected system to become unstable or reload. The vulnerability is due to insufficient hardening of the XML parser configuration. An attacker could exploit this vulnerability in multiple ways using a malicious file: An attacker with administrative privileges could upload a malicious XML file on the system and cause the XML code to parse the malicious file. An attacker with Clientless Secure Sockets Layer (SSL) VPN access could exploit this vulnerability by sending a crafted XML file. A successful exploit would allow the attacker to crash the XML parser process, which could cause system instability, memory exhaustion, and in some cases lead to a reload of the affected system.	4.9	More Details
CVE-2020-3308	A vulnerability in the Image Signature Verification feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker with administrator-level credentials to install a malicious software patch on an affected device. The vulnerability is due to improper verification of digital signatures for patch images. An attacker could exploit this vulnerability by crafting an unsigned software patch to bypass signature checks and loading it on an affected device. A successful exploit could allow the attacker to boot a malicious software patch image.	4.9	More Details
CVE-2020-3256	A vulnerability in the web-based management interface of Cisco Hosted Collaboration Mediation Fulfillment (HCM-F) Software could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. To exploit this vulnerability, an attacker would need administrative privileges on the Cisco HCM-F Software. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by sending malicious requests that contain references in XML entities to an affected system. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9314	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** Oracle iPlanet Web Server 7.0.x allows image injection in the Administration console via the productNameSrc parameter to an admingui URI. This issue exists because of an incomplete fix for CVE-2012-0516. NOTE: a related support policy can be found in the www.oracle.com references attached to this CVE.	4.8	More Details
CVE-2020-10059	The UpdateHub module disables DTLS peer checking, which allows for a man in the middle attack. This is mitigated by firmware images requiring valid signatures. However, there is no benefit to using DTLS without the peer checking. See NCC-ZEP-018 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions.	4.8	More Details
CVE-2019-20794	An issue was discovered in the Linux kernel 4.18 through 5.6.11 when unprivileged user namespaces are allowed. A user can create their own PID namespace, and mount a FUSE filesystem. Upon interaction with this FUSE filesystem, if the userspace component is terminated via a kill of the PID namespace's pid 1, it will result in a hung task, and resources being permanently locked up until system reboot. This can result in resource exhaustion.	4.7	More Details
CVE-2020-7921	Improper serialization of internal state in the authorization subsystem in MongoDB Server's authorization subsystem permits a user with valid credentials to bypass IP whitelisting protection mechanisms following administrative action. This issue affects MongoDB Server v4.2 versions prior to 4.2.3; MongoDB Server v4.0 versions prior to 4.0.15; MongoDB Server v4.3 versions prior to 4.3.3and MongoDB Server v3.6 versions prior to 3.6.18.	4.6	More Details
CVE-2020-3301	Multiple vulnerabilities in Cisco Firepower Management Center (FMC) Software and Cisco Firepower User Agent Software could allow an attacker to access a sensitive part of an affected system with a high-privileged account. For more information about these vulnerabilities, see the Details section of this advisory.	4.4	More Details
CVE-2019-20795	iproute2 before 5.1.0 has a use-after-free in get_netnsid_from_name in ip/ipnetns.c. NOTE: security relevance may be limited to certain uses of setuid that, although not a default, are sometimes a configuration option offered to end users. Even when setuid is used, other factors (such as C library configuration) may block exploitability.	4.4	More Details
CVE-2020-2184	A cross-site request forgery vulnerability in Jenkins CVS Plugin 2.15 and earlier allows attackers to create and manipulate tags, and to connect to an attacker-specified URL.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5743	Improper Control of Resource Identifiers in TCExam 14.2.2 allows a remote, authenticated attacker to access test metadata for which they don't have permission.	4.3	More Details
CVE-2020-4446	IBM Business Process Manager 8.0, 8.5, and 8.6 and IBM Business Automation Workflow 18.0 and 19.0 could allow a remote attacker to bypass security restrictions, caused by the failure to perform insufficient authorization checks. IBM X-Force ID: 181126.	4.3	More Details
CVE-2020-3329	A vulnerability in role-based access control of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow a read-only authenticated, remote attacker to disable user accounts on an affected system. The vulnerability is due to incorrect allocation of the enable/disable action button under the role-based access control code on an affected system. An attacker could exploit this vulnerability by authenticating as a read-only user and then updating the roles of other users to disable them. A successful exploit could allow the attacker to disable users, including administrative users.	4.3	More Details
CVE-2020-4430	IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, and 2.0.4 could allow a remote authenticated attacker to traverse directories on the system. An attacker could send a specially-crafted URL request to download arbitrary files from the system. IBM X-Force ID: 180535.	4.3	More Details
CVE-2020-2188	A missing permission check in Jenkins Amazon EC2 Plugin 1.50.1 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	4.3	More Details
CVE-2020-2182	Jenkins Credentials Binding Plugin 1.22 and earlier does not mask (i.e., replace with asterisks) secrets containing a `$` character in some circumstances.	4.3	More Details
CVE-2020-3246	A vulnerability in the web server of Cisco Umbrella could allow an unauthenticated, remote attacker to perform a carriage return line feed (CRLF) injection attack against a user of an affected service. The vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user to access a crafted URL. A successful exploit could allow the attacker to inject arbitrary HTTP headers into valid HTTP responses sent to the browser of the user.	4.3	More Details
CVE-2020-2186	A cross-site request forgery vulnerability in Jenkins Amazon EC2 Plugin 1.50.1 and earlier allows attackers to provision instances.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6256	SAP Master Data Governance, versions - 748, 749, 750, 751, 752, 800, 801, 802, 803, 804, allows users to display change request details without having required authorizations, due to Missing Authorization Check.	4.3	More Details
CVE-2020-1724	A flaw was found in Keycloak in versions before 9.0.2. This flaw allows a malicious user that is currently logged in, to see the personal information of a previously logged out user in the account manager section.	4.3	More Details
CVE-2020-11054	In qutebrowser versions less than 1.11.1, reloading a page with certificate errors shows a green URL. After a certificate error was overridden by the user, qutebrowser displays the URL as yellow (colors.statusbar.url.warn.fg). However, when the affected website was subsequently loaded again, the URL was mistakenly displayed as green (colors.statusbar.url.success_https). While the user already has seen a certificate error prompt at this point (or set content.ssl_strict to false, which is not recommended), this could still provide a false sense of security. This has been fixed in 1.11.1 and 1.12.0. All versions of qutebrowser are believed to be affected, though versions before v0.11.x couldn't be tested. Backported patches for older versions (greater than or equal to 1.4.0 and less than or equal to 1.10.2) are available, but no further releases are planned.	3.5	More Details
CVE-2020-5833	Symantec Endpoint Protection Manager, prior to 14.3, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	3.3	More Details
CVE-2020-12755	fishProtocol::establishConnection in fish/fish.cpp in KDE kio-extras through 20.04.0 makes a cacheAuthentication call even if the user had not set the keepPassword option. This may lead to unintended KWallet storage of a password.	3.3	More Details
CVE-2019-4266	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 does not have device jailbreak detection which could result in an attacker gaining sensitive information about the device. IBM X-Force ID: 160199.	2.4	More Details
CVE-2020-11048	In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bounds read. It only allows to abort a session. No data extraction is possible. This has been fixed in 2.0.0.	2.2	More Details
CVE-2020-11045	In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bound read in in update_read_bitmap_data that allows client memory to be read to an image buffer. The result displayed on screen as colour.	2.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11044	In FreeRDP greater than 1.2 and before 2.0.0, a double free in update_read_cache_bitmap_v3_order crashes the client application if corrupted data from a manipulated server is parsed. This has been patched in 2.0.0.	2.2	More Details
CVE-2020-11058	In FreeRDP after 1.1 and before 2.0.0, a stream out-of-bounds seek in rdp_read_font_capability_set could lead to a later out-of-bounds read. As a result, a manipulated client or server might force a disconnect due to an invalid data read. This has been fixed in 2.0.0.	2.2	More Details
CVE-2019-17287	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17288	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17289	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17290	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17291	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-12678	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-12677. Reason: This candidate is a reservation duplicate of CVE-2020-12677. Notes: All CVE users should reference CVE-2020-12677 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2019-17277	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17285	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-17286	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-9310	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-2018-5484	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-13654	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-13653	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-1962	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-5499	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17279	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-5491	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-5480	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-15514	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-14200	Rejected reason: Unused CVE for 2017	N/A	More Details
CVE-2017-13657	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-13656	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-13655	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-10026	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-10021. Reason: This candidate is a reservation duplicate of CVE-2020-10021. Notes: All CVE users should reference CVE-2020-10021 instead of this candidate	N/A	More Details
CVE-2019-17280	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-13651	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-12650	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was intended behavior. Notes: none	N/A	More Details
CVE-2019-17281	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17282	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17283	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-17284	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-17278	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-10741	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-12826. Reason: This candidate is a duplicate of CVE-2020-12826. Notes: All CVE users should reference CVE-2020-12826 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-10025	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-10067. Reason: This candidate is a reservation duplicate of CVE-2020-10067. Notes: All CVE users should reference CVE-2020-10067 instead of this candidate	N/A	More Details