SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 November 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-2020-26824	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the Upgrade Legacy Ports Service, this has an impact to the integrity and availability of the service.	10.0	More Details
CVE-2020-26823	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the Upgrade Diagnostics Agent Connection Service, this has an impact to the integrity and availability of the service.	10.0	More Details
CVE-2020-26822	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the Outside Discovery Configuration Service, this has an impact to the integrity and availability of the service.	10.0	More Details
CVE-2020-26821	SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the SVG Converter Service, this has an impact to the integrity and availability of the service.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28371	An issue was discovered in ReadyTalk Avian 1.2.0 before 2020-10-27. The FileOutputStream.write() method in FileOutputStream.java has a boundary check to prevent out-of-bounds memory read/write operations. However, an integer overflow leads to bypassing this check and achieving the out-of-bounds access. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2020-28347	tdpServer on TP-Link Archer A7 AC1750 devices before 201029 allows remote attackers to execute arbitrary code via the slave_mac parameter. NOTE: this issue exists because of an incomplete fix for CVE-2020-10882 in which shell quotes are mishandled.	9.8	More Details
CVE-2020-23138	An unrestricted file upload vulnerability was discovered in the Microweber 1.1.18 admin account page. An attacker can upload PHP code or any extension (eg- .exe) to the web server by providing image data and the image/jpeg content type with a .php extension.	9.8	More Details
CVE-2020-26542	An issue was discovered in the MongoDB Simple LDAP plugin through 2020-10-02 for Percona Server when using the SimpleLDAP authentication in conjunction with Microsoft's Active Directory, Percona has discovered a flaw that would allow authentication to complete when passing a blank value for the account password, leading to access against the service integrated with which Active Directory is deployed at the level granted to the authenticating account.	9.8	More Details
CVE-2020-14188	The preprocessArgs function in the Atlassian gajira-create GitHub Action before version 2.0.1 allows remote attackers to execute arbitrary code in the context of a GitHub runner by creating a specially crafted GitHub issue.	9.8	More Details
CVE-2020-14189	The execute function in in the Atlassian gajira-comment GitHub Action before version 2.0.2 allows remote attackers to execute arbitrary code in the context of a GitHub runner by creating a specially crafted GitHub issue comment.	9.8	More Details
CVE-2020-26168	The LDAP authentication method in LdapLoginModule in Hazelcast IMDG Enterprise 4.x before 4.0.3, and Jet Enterprise 4.x through 4.2, doesn't verify properly the password in some system-user-dn scenarios. As a result, users (clients/members) can be authenticated even if they provide invalid passwords.	9.8	More Details
CVE-2020-0446	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-168264528	9.8	More Details
CVE-2020-0445	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-168264527	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2300	Jenkins Active Directory Plugin 2.19 and earlier does not prohibit the use of an empty password in Windows/ADSI mode, which allows attackers to log in to Jenkins as any user depending on the configuration of the Active Directory server.	9.8	More Details
CVE-2020-0447	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-168251617	9.8	More Details
CVE-2020-0452	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if a third party app used this library to process remote image data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-159625731	9.8	More Details
CVE-2020-24384	A10 Networks ACOS and aGalaxy management Graphical User Interfaces (GUIs) have an unauthenticated Remote Code Execution (RCE) vulnerability that could be used to compromise affected ACOS systems. ACOS versions 3.2.x (including and after 3.2.2), 4.x, and 5.1.x are affected. aGalaxy versions 3.0.x, 3.2.x, and 5.0.x are affected.	9.8	More Details
CVE-2020-13927	The previous default setting for Airflow's Experimental API was to allow all API requests without authentication, but this poses security risks to users who miss this fact. From Airflow 1.10.11 the default has been changed to deny all requests by default and is documented at https://airflow.apache.org/docs/1.10.11/security.html#api-authentication. Note this change fixes it for new installs but existing users need to change their config to default `[api]auth_backend = airflow.api.auth.backend.deny_all` as mentioned in the Updating Guide: https://github.com/apache/airflow/blob/1.10.11/UPDATING.md#experimental-api-will-deny-all-request-by-default	9.8	More Details
CVE-2020-25074	The cache action in action/cache.py in MoinMoin through 1.9.10 allows directory traversal through a crafted HTTP request. An attacker who can upload attachments to the wiki can use this to achieve remote code execution.	9.8	More Details
CVE-2020-28340	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. Attackers can bypass Factory Reset Protection (FRP) via Secure Folder. The Samsung ID is SVE-2020-18546 (November 2020).	9.8	More Details
CVE-2020-2299	Jenkins Active Directory Plugin 2.19 and earlier allows attackers to log in as any user if a magic constant is used as the password.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3284	A vulnerability in the enhanced Preboot eXecution Environment (PXE) boot loader for Cisco IOS XR 64-bit Software could allow an unauthenticated, remote attacker to execute unsigned code during the PXE boot process on an affected device. The PXE boot loader is part of the BIOS and runs over the management interface of hardware platforms that are running Cisco IOS XR Software only. The vulnerability exists because internal commands that are issued when the PXE network boot process is loading a software image are not properly verified. An attacker could exploit this vulnerability by compromising the PXE boot server and replacing a valid software image with a malicious one. Alternatively, the attacker could impersonate the PXE boot server and send a PXE boot reply with a malicious file. A successful exploit could allow the attacker to execute unsigned code on the affected device. Note: To fix this vulnerability, both the Cisco IOS XR Software and the BIOS must be upgraded. The BIOS code is included in Cisco IOS XR Software but might require additional installation steps. For further information, see the Fixed Software section of this advisory.	9.8	More Details
CVE-2020-5644	Buffer overflow vulnerability in TCP/IP function included in the firmware of GT14 Model of GOT 1000 series (GT1455-QTBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QMBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QLBDE CoreOS version "05.65.00.BD" and earlier, GT1455HS-QTBDE CoreOS version "05.65.00.BD" and earlier, and GT1450HS-QMBDE CoreOS version "05.65.00.BD" and earlier) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	9.8	More Details
CVE-2020-27689	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains undocumented default admin credentials for the web management interface. A remote attacker could exploit this vulnerability to login and execute commands on the device, as well as upgrade the firmware image to a malicious version.	9.8	More Details
CVE-2020-7128	A remote unauthenticated arbitrary code execution vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	9.8	More Details
CVE-2020-22276	WeForms Wordpress Plugin 1.4.7 allows CSV injection via a form's entry.	9.8	More Details
CVE-2020-27955	Git LFS 2.12.0 allows Remote Code Execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17510	Apache Shiro before 1.7.0, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.	9.8	More Details
CVE-2020-25172	A relative path traversal attack in the B. Braun OnlineSuite Version AP 3.0 and earlier allows unauthenticated attackers to upload or download arbitrary files.	9.8	More Details
CVE-2020-5647	Improper access control vulnerability in TCP/IP function included in the firmware of GT14 Model of GOT 1000 series (GT1455-QTBDE CoreOS version ’05.65.00.BD’ and earlier, GT1450-QMBDE CoreOS version ’05.65.00.BD’ and earlier, GT1450-QLBDE CoreOS version ’05.65.00.BD’ and earlier, GT1455HS-QTBDE CoreOS version ’05.65.00.BD’ and earlier, and GT1450HS-QMBDE CoreOS version ’05.65.00.BD’ and earlier) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	9.8	More Details
CVE-2020-26167	In FUEL CMS 11.4.12 and before, the page preview feature allows an anonymous user to take complete ownership of any account including an administrator one.	9.8	More Details
CVE-2020-5648	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of GT14 Model of GOT 1000 series (GT1455-QTBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QMBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QLBDE CoreOS version "05.65.00.BD" and earlier, GT1455HS-QTBDE CoreOS version "05.65.00.BD" and earlier, and GT1450HS-QMBDE CoreOS version "05.65.00.BD" and earlier) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet.	9.8	More Details
CVE-2020-28250	Cellinx NVT Web Server 5.0.0.014b.test 2019-09-05 allows a remote user to run commands as root via SetFileContent.cgi because authentication is on the client side.	9.8	More Details
CVE-2020-16846	An issue was discovered in SaltStack Salt through 3002. Sending crafted web requests to the Salt API, with the SSH client enabled, can result in shell injection.	9.8	More Details
CVE-2020-25592	In SaltStack Salt through 3002, salt-netapi improperly validates eauth credentials and tokens. A user can bypass authentication and invoke Salt SSH.	9.8	More Details
CVE-2020-2301	Jenkins Active Directory Plugin 2.19 and earlier allows attackers to log in as any user with any password while a successful authentication of that user is still in the optional cache when using Windows/ADSI mode.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26892	The JWT library in NATS nats-server before 2.1.9 has Incorrect Access Control because of how expired credentials are handled.	9.8	More Details
CVE-2020-22274	JomSocial (Joomla Social Network Extention) 4.7.6 allows CSV injection via a customer's profile.	9.8	More Details
CVE-2020-15708	Ubuntu's packaging of libvirt in 20.04 LTS created a control socket with world read and write permissions. An attacker could use this to overwrite arbitrary files or execute arbitrary code.	9.3	More Details
CVE-2020-24407	Magento versions 2.4.0 and 2.3.5p1 (and earlier) are affected by an unsafe file upload vulnerability that could result in arbitrary code execution. This vulnerability could be abused by authenticated users with administrative permissions to the System/Data and Transfer/Import components.	9.1	More Details
CVE-2020-26214	In Alerta before version 8.1.0, users may be able to bypass LDAP authentication if they provide an empty password when Alerta server is configure to use LDAP as the authorization provider. Only deployments where LDAP servers are configured to allow unauthenticated authentication mechanism for anonymous authorization are affected. A fix has been implemented in version 8.1.0 that returns HTTP 401 Unauthorized response for any authentication attempts where the password field is empty. As a workaround LDAP administrators can disallow unauthenticated bind requests by clients.	9.1	More Details
CVE-2020-15952	Immuta v2.8.2 is affected by stored XSS that allows a low-privileged user to escalate privileges to administrative permissions. Additionally, unauthenticated attackers can phish unauthenticated Immuta users to steal credentials or force actions on authenticated users through reflected, DOM-based XSS.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-25268	Remote Code Execution can occur via the external news feed in ILIAS 6.4 because of incorrect parameter sanitization for Magpie RSS data.	8.8	More Details
CVE-2020-22278	phpMyAdmin through 5.0.2 allows CSV injection via Export Section. NOTE: the vendor disputes this because "the CSV file is accurately generated based on the database contents.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27387	An unrestricted file upload issue in HorizontCMS through 1.0.0-beta allows an authenticated remote attacker (with access to the FileManager) to upload and execute arbitrary PHP code by uploading a PHP payload, and then using the FileManager's rename function to provide the payload (which will receive a random name on the server) with the PHP extension, and finally executing the PHP file via an HTTP GET request to /storage/<php_file_name>. NOTE: the vendor has patched this while leaving the version number at 1.0.0-beta.	8.8	More Details
CVE-2020-15950	Immuta v2.8.2 is affected by improper session management: user sessions are not revoked upon logout.	8.8	More Details
CVE-2020-24849	A remote code execution vulnerability is identified in FruityWifi through 2.4. Due to improperly escaped shell metacharacters obtained from the POST request at the page_config_adv.php page, it is possible to perform remote code execution by an authenticated attacker. This is similar to CVE-2018-17317.	8.8	More Details
CVE-2020-28115	SQL Injection vulnerability in "Documents component" found in AudimexEE version 14.1.0 allows an attacker to execute arbitrary SQL commands via the object_path parameter.	8.8	More Details
CVE-2020-25398	CSV Injection exists in InterMind iMind Server through 3.13.65 via the csv export functionality.	8.8	More Details
CVE-2020-13661	Telerik Fiddler through 5.0.20202.18177 allows attackers to execute arbitrary programs via a hostname with a trailing space character, followed by --utility-and-browser --utility-cmd-prefix= and the pathname of a locally installed program. The victim must interactively choose the Open On Browser option. Fixed in version 5.0.20204.	8.8	More Details
CVE-2019-7357	Subrion CMS 4.2.1 has CSRF in panel/modules/plugins/. The attacker can remotely activate/deactivate the plugins.	8.8	More Details
CVE-2020-26819	SAP NetWeaver AS ABAP (Web Dynpro), versions - 731, 740, 750, 751, 752, 753, 754, 755, 782, allows an authenticated user to access Web Dynpro components, that allows them to read and delete database logfiles because of Improper Access Control.	8.8	More Details
CVE-2020-26818	SAP NetWeaver AS ABAP (Web Dynpro), versions - 731, 740, 750, 751, 752, 753, 754, 755, 782, allows an authenticated user to access Web Dynpro components, which reveals sensitive system information that would otherwise be restricted to highly privileged users because of missing authorization, resulting in Information Disclosure.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0451	In sbrDecoder_AssignQmfChannels2SbrChannels of sbrdecoder.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9 Android-8.0 Android-8.1Android ID: A-158762825	8.8	More Details
CVE-2020-0449	In btm_sec_disconnected of btm_sec.cc, there is a possible memory corruption due to a use after free. This could lead to remote code execution in the Bluetooth server with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.0 Android-8.1Android ID: A-162497143	8.8	More Details
CVE-2020-6877	A ZTE product is impacted by an information leak vulnerability. An attacker could use this vulnerability to obtain the authentication password of the handheld terminal and access the device illegally for operation. This affects: ZXA10 eODN V2.3P2T1	8.8	More Details
CVE-2020-27016	Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to a cross-site request forgery (CSRF) vulnerability which could allow an attacker to modify policy rules by tricking an authenticated administrator into accessing an attacker-controlled web page. An attacker must already have obtained product administrator/root privileges to exploit this vulnerability.	8.8	More Details
CVE-2020-28373	upnpd on certain NETGEAR devices allows remote (LAN) attackers to execute arbitrary code via a stack-based buffer overflow. This affects R6400v2 V1.0.4.102_10.0.75, R6400 V1.0.1.62_1.0.41, R7000P V1.3.2.126_10.1.66, XR300 V1.0.3.50_10.3.36, R8000 V1.0.4.62, R8300 V1.0.2.136, R8500 V1.0.2.136, R7300DST V1.0.0.74, R7850 V1.0.5.64, R7900 V1.0.4.30, RAX20 V1.0.2.64, RAX80 V1.0.3.102, and R6250 V1.0.4.44.	8.8	More Details
CVE-2020-28328	SuiteCRM before 7.11.17 is vulnerable to remote code execution via the system settings Log File Name setting. In certain circumstances involving admin account takeover, logger_file_name can refer to an attacker-controlled .php file under the web root.	8.8	More Details
CVE-2020-7198	There is a remote escalation of privilege possible for a malicious user that has a OneView account in OneView and Synergy Composer. HPE has provided updates to Oneview and Synergy Composer: Update to version 5.5 of OneView, Composer, or Composer2.	8.8	More Details
CVE-2020-27347	In tmux before version 3.1c the function input_csi_dispatch_sgr_colon() in file input.c contained a stack-based buffer-overflow that can be exploited by terminal output.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27692	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains multiple CSRF vulnerabilities within its web management portal. Attackers can, for example, use this to update the TR-069 configuration server settings (responsible for managing devices remotely). This makes it possible to remotely reboot the device or upload malicious firmware.	8.8	More Details
CVE-2020-27694	Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 has updated a specific critical library that may vulnerable to attack.	8.8	More Details
CVE-2020-22275	Easy Registration Forms (ER Forms) Wordpress Plugin 2.0.6 allows an attacker to submit an entry with malicious CSV commands. After that, when the system administrator generates CSV output from the forms information, there is no check on this inputs and the codes are executable.	8.8	More Details
CVE-2020-26815	SAP Fiori Launchpad (News tile Application), versions - 750,751,752,753,754,755, allows an unauthorized attacker to send a crafted request to a vulnerable web application. It is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network to retrieve sensitive / confidential resources which are otherwise restricted for internal usage only, resulting in a Server-Side Request Forgery vulnerability.	8.6	More Details
CVE-2020-5945	In BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, undisclosed TMUI page contains a stored cross site scripting vulnerability (XSS). The issue allows a minor privilege escalation for resource admin to escalate to full admin.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10292	Visual Components (owned by KUKA) is a robotic simulator that allows simulating factories and robots in order toimprove planning and decision-making processes. Visual Components software requires a special license which can beobtained from a network license server. The network license server binds to all interfaces (0.0.0.0) and listensfor packets over UDP port 5093. No authentication/authorization is required in order to communicate with theserver. The protocol being used is a property protocol by RMS Sentinel which provides the licensing infrastructurefor the network license server. RMS Sentinel license manager service exposes UDP port 5093 which provides sensitivesystem information that could be leveraged for further exploitation without any kind of authentication. Thisinformation includes detailed hardware and OS characteristics.After a decryption process, a textual protocol is found which contains a simple header with the requested command,application-identifier, and some arguments. The protocol is vulnerable to DoS through an arbitrary pointerderreference. This flaw allows an attacker to to pass a specially crafted package that, when processed by theservice, causes an arbitrary pointer from the stack to be dereferenced, causing an uncaught exception thatterminates the service. This can be further contructed in combination with RVDP#710 which exploits an informationdisclosure leak, or with RVDP#711 for an stack-overflow and potential code execution.Beyond denying simulations, Visual Components provides capabilities to interface with industrial machinery andautomate certain processes (e.g. testing, benchmarking, etc.) which depending on the DevOps setup might beintegrated into the industrial flow. Accordingly, a DoS in the simulation might have higher repercusions, dependingon the Industrial Control System (ICS) ICS infrastructure.	8.2	More Details
CVE-2020-16122	PackageKit's apt backend mistakenly treated all local debs as trusted. The apt security model is based on repository trust and not on the contents of individual files. On sites with configured PolicyKit rules this may allow users to install malicious packages.	8.2	More Details
CVE-2020-23140	Microweber 1.1.18 is affected by insufficient session expiration. When changing passwords, both sessions for when a user changes email and old sessions in any other browser or device, the session does not expire and remains active.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15259	ad-ldap-connector's admin panel before version 5.0.13 does not provide csrf protection, which when exploited may result in remote code execution or confidential data loss. CSRF exploits may occur if the user visits a malicious page containing CSRF payload on the same machine that has access to the ad-ldap-connector admin console via a browser. You may be affected if you use the admin console included with ad-ldap-connector versions <=5.0.12. If you do not have ad-ldap-connector admin console enabled or do not visit any other public URL while on the machine it is installed on, you are not affected. The issue is fixed in version 5.0.13.	8.1	More Details
CVE-2020-26207	DatabaseSchemaViewer before version 2.7.4.3 is vulnerable to arbitrary code execution if a user is tricked into opening a specially crafted `.dbschema` file. The patch was released in v2.7.4.3. As a workaround, ensure `.dbschema` files from untrusted sources are not opened.	8.0	More Details
CVE-2020-22277	Import and export users and customers WordPress Plugin through 1.15.5.11 allows CSV injection via a customer's profile.	8.0	More Details
CVE-2020-24437	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2020-28055	A vulnerability in the TCL Android Smart TV series V8-R851T02-LF1 V295 and below and V8-T658T01-LF1 V373 and below by TCL Technology Group Corporation allows a local unprivileged attacker, such as a malicious App, to read & write to the /data/vendor/tcl, /data/vendor/upgrade, and /var/TerminalManager directories within the TV file system. An attacker, such as a malicious APK or local unprivileged user could perform fake system upgrades by writing to the /data/vendor/upgrage folder.	7.8	More Details
CVE-2020-13536	An exploitable local privilege elevation vulnerability exists in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary. By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.Js scripts to start additional application functionality.	7.8	More Details
CVE-2020-25170	An Excel Macro Injection vulnerability exists in the export feature in the B. Braun OnlineSuite Version AP 3.0 and earlier via multiple input fields that are mishandled in an Excel export.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25174	A DLL hijacking vulnerability in the B. Braun OnlineSuite Version AP 3.0 and earlier allows local attackers to execute code on the system as a high privileged user.	7.8	More Details
CVE-2020-5794	A vulnerability in Nessus Network Monitor versions 5.11.0, 5.11.1, and 5.12.0 for Windows could allow an authenticated local attacker to execute arbitrary code by copying user-supplied files to a specially constructed path in a specifically named user directory. The attacker needs valid credentials on the Windows system to exploit this vulnerability.	7.8	More Details
CVE-2020-26817	SAP 3D Visual Enterprise Viewer, version - 9, allows an user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	7.8	More Details
CVE-2020-23968	Ilex International Sign&go Workstation Security Suite 7.1 allows elevation of privileges via a symlink attack on ProgramData\Ilex\S&G\Logs\000-sngWSService1.log.	7.8	More Details
CVE-2020-13537	An exploitable local privilege elevation vulnerability exists in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary.By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.Js scripts to start additional application functionality and among them the mosquitto executable is also run.	7.8	More Details
CVE-2020-3603	Multiple vulnerabilities in Cisco Webex Network Recording Player for Windows and Cisco Webex Player for Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements of a Webex recording that is stored in the Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details
CVE-2020-3604	Multiple vulnerabilities in Cisco Webex Network Recording Player for Windows and Cisco Webex Player for Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements of a Webex recording that is stored in the Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28341	An issue was discovered on Samsung mobile devices with Q(10.0) (Exynos990 chipsets) software. The S3K250AF Secure Element CC EAL 5+ chip allows attackers to execute arbitrary code and obtain sensitive information via a buffer overflow. The Samsung ID is SVE-2020-18632 (November 2020).	7.8	More Details
CVE-2020-3573	Multiple vulnerabilities in Cisco Webex Network Recording Player for Windows and Cisco Webex Player for Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements of a Webex recording that is stored in the Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details
CVE-2020-3600	A vulnerability in Cisco SD-WAN Software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient security controls on the CLI. An attacker could exploit this vulnerability by using an affected CLI utility that is running on an affected system. A successful exploit could allow the attacker to gain root privileges.	7.8	More Details
CVE-2020-0439	In generatePackageInfo of PackageManagerService.java, there is a possible permissions bypass due to an incorrect permission check. This could lead to local escalation of privilege that allows instant apps access to permissions not allowed for instant apps, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-140256621	7.8	More Details
CVE-2020-0438	In the AIBinder_Class constructor of ibinder.cpp, there is a possible arbitrary code execution due to uninitialized data. This could lead to local escalation of privilege if a process were using libbinder_ndk in a vulnerable way with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-161812320	7.8	More Details
CVE-2020-5793	A vulnerability in Nessus versions 8.9.0 through 8.12.0 for Windows & Nessus Agent 8.0.0 and 8.1.0 for Windows could allow an authenticated local attacker to copy user-supplied files to a specially constructed path in a specifically named user directory. An attacker could exploit this vulnerability by creating a malicious file and copying the file to a system directory. The attacker needs valid credentials on the Windows system to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24430	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability when handling malicious JavaScript. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2020-3595	A vulnerability in Cisco SD-WAN Software could allow an authenticated, local attacker to elevate privileges to root group on the underlying operating system. The vulnerability is due to incorrect permissions being set when the affected command is executed. An attacker could exploit this vulnerability by executing the affected command on an affected system. A successful exploit could allow the attacker to gain root privileges.	7.8	More Details
CVE-2020-3594	A vulnerability in Cisco SD-WAN Software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted options to a specific command. A successful exploit could allow the attacker to gain root privileges.	7.8	More Details
CVE-2020-24433	Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment.	7.8	More Details
CVE-2020-3593	A vulnerability in Cisco SD-WAN Software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to a utility that is running on an affected system. A successful exploit could allow the attacker to gain root privileges.	7.8	More Details
CVE-2020-24435	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader.	7.8	More Details
CVE-2020-24367	Incorrect file permissions in BlueStacks 4 through 4.230 on Windows allow a local attacker to escalate privileges by modifying a file that is later executed by a higher-privileged user.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24436	Acrobat Pro DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds write vulnerability that could result in writing past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit in that the victim must open a malicious document.	7.8	More Details
CVE-2020-0418	In getPermissionInfosForGroup of Utils.java, there is a logic error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-153879813	7.8	More Details
CVE-2020-0409	In create of FileMap.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.0 Android-8.1 Android-9Android ID: A-156997193	7.8	More Details
CVE-2020-4759	IBM FileNet Content Manager 5.5.4 and 5.5.5 is potentially vulnerable to CVS Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 188736.	7.8	More Details
CVE-2020-27402	The HK1 Box S905X3 TV Box contains a vulnerability that allows a local unprivileged user to escalate to root using the /system/xbin/su binary via a serial port (UART) connection or using adb.	7.8	More Details
CVE-2020-28343	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 980, 9820, and 9830 chipsets) software. The NPU driver allows attackers to execute arbitrary code because of unintended write and read operations on memory. The Samsung ID is SVE-2020-18610 (November 2020).	7.8	More Details
CVE-2020-25399	Stored XSS in InterMind iMind Server through 3.13.65 allows any user to hijack another user's session by sending a malicious file in the chat.	7.8	More Details
CVE-2020-27977	CapaSystems CapaInstaller before 6.0.101 does not properly assign, modify, or check privileges for an actor who attempts to edit registry values, allowing an attacker to escalate privileges.	7.8	More Details
CVE-2020-28342	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (China / India) software. The S Secure application allows attackers to bypass authentication for a locked Gallery application via the Reminder application. The Samsung ID is SVE-2020-18689 (November 2020).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26507	A CSV Injection (also known as Formula Injection) vulnerability in the Marmind web application with version 4.1.141.0 allows malicious users to gain remote control of other computers. By providing formula code in the “Notes” functionality in the main screen, an attacker can inject a payload into the “Description” field under the “Insert To-Do” option. Other users might download this data, for example a CSV file, and execute the malicious commands on their computer by opening the file using a software such as Microsoft Excel. The attacker could gain remote access to the user’s PC.	7.8	More Details
CVE-2020-24429	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a signature verification bypass that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.7	More Details
CVE-2020-24428	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a time-of-check time-of-use (TOCTOU) race condition vulnerability that could result in local privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.7	More Details
CVE-2020-3574	A vulnerability in the TCP packet processing functionality of Cisco IP Phones could allow an unauthenticated, remote attacker to cause the phone to stop responding to incoming calls, drop connected calls, or unexpectedly reload. The vulnerability is due to insufficient TCP ingress packet rate limiting. An attacker could exploit this vulnerability by sending a high and sustained rate of crafted TCP traffic to the targeted device. A successful exploit could allow the attacker to impact operations of the phone or cause the phone to reload, leading to a denial of service (DoS) condition.	7.5	More Details
CVE-2020-8036	The tok2strbuf() function in tcpdump 4.10.0-PRE-GIT was used by the SOME/IP dissector in an unsafe way.	7.5	More Details
CVE-2020-15949	Immuta v2.8.2 is affected by one instance of insecure permissions that can lead to user account takeover.	7.5	More Details
CVE-2020-3444	A vulnerability in the packet filtering features of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to bypass L3 and L4 traffic filters. The vulnerability is due to improper traffic filtering conditions on an affected device. An attacker could exploit this vulnerability by crafting a malicious TCP packet with specific characteristics and sending it to a targeted device. A successful exploit could allow the attacker to bypass the L3 and L4 traffic filters and inject an arbitrary packet into the network.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5942	In BIG-IP PEM versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, when processing Capabilities-Exchange-Answer (CEA) packets with certain attributes from the Policy and Charging Rules Function (PCRF) server, the Traffic Management Microkernel (TMM) may generate a core file and restart.	7.5	More Details
CVE-2020-8037	The ppp decapsulator in tcpdump 4.9.3 can be convinced to allocate a large amount of memory.	7.5	More Details
CVE-2020-7763	This affects the package phantom-html-to-pdf before 0.6.1.	7.5	More Details
CVE-2020-5941	On BIG-IP versions 16.0.0-16.0.0.1 and 15.1.0-15.1.0.5, using the RESOLV::lookup command within an iRule may cause the Traffic Management Microkernel (TMM) to generate a core file and restart. This issue occurs when data exceeding the maximum limit of a hostname passes to the RESOLV::lookup command.	7.5	More Details
CVE-2020-0442	In Message and toBundle of Notification.java, there is a possible UI slowdown or crash due to improper input validation. This could lead to remote denial of service if a malicious contact file is received, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.0 Android-8.1 Android-9Android ID: A-147358092	7.5	More Details
CVE-2020-5939	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.3, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, and 13.1.0-13.1.3.4, BIG-IP Virtual Edition (VE) systems on VMware, with an Intel-based 85299 Network Interface Controller (NIC) card and Single Root I/O Virtualization (SR-IOV) enabled on vSphere, may fail and leave the Traffic Management Microkernel (TMM) in a state where it cannot transmit traffic.	7.5	More Details
CVE-2020-0441	In Message and toBundle of Notification.java, there is a possible resource exhaustion due to improper input validation. This could lead to remote denial of service requiring a device reset to fix with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-158304295	7.5	More Details
CVE-2020-8268	Prototype pollution vulnerability in json8-merge-patch npm package < 1.0.3 may allow attackers to inject or modify methods and properties of the global object constructor.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5645	Session fixation vulnerability in TCP/IP function included in the firmware of GT14 Model of GOT 1000 series (GT1455-QTBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QMBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QLBDE CoreOS version "05.65.00.BD" and earlier, GT1455HS-QTBDE CoreOS version "05.65.00.BD" and earlier, and GT1450HS-QMBDE CoreOS version "05.65.00.BD" and earlier) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.	7.5	More Details
CVE-2020-28267	Prototype pollution vulnerability in '@strikeentco/set' version 1.0.0 allows attacker to cause a denial of service and may lead to remote code execution.	7.5	More Details
CVE-2020-5649	Resource management error vulnerability in TCP/IP function included in the firmware of GT14 Model of GOT 1000 series (GT1455-QTBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QMBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QLBDE CoreOS version "05.65.00.BD" and earlier, GT1455HS-QTBDE CoreOS version "05.65.00.BD" and earlier, and GT1450HS-QMBDE CoreOS version "05.65.00.BD" and earlier) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.	7.5	More Details
CVE-2020-5646	NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of GT14 Model of GOT 1000 series (GT1455-QTBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QMBDE CoreOS version "05.65.00.BD" and earlier, GT1450-QLBDE CoreOS version "05.65.00.BD" and earlier, GT1455HS-QTBDE CoreOS version "05.65.00.BD" and earlier, and GT1450HS-QMBDE CoreOS version "05.65.00.BD" and earlier) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.	7.5	More Details
CVE-2020-25201	HashiCorp Consul Enterprise version 1.7.0 up to 1.8.4 includes a namespace replication bug which can be triggered to cause denial of service via infinite Raft writes. Fixed in 1.7.9 and 1.8.5.	7.5	More Details
CVE-2020-5946	In BIG-IP Advanced WAF and FPS versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.7, under some circumstances, certain format client-side alerts sent to the BIG-IP virtual server configured with DataSafe may cause the Traffic Management Microkernel (TMM) to restart, resulting in a Denial-of-Service (DoS).	7.5	More Details
CVE-2020-25837	Sensitive information disclosure vulnerability in Micro Focus Self Service Password Reset (SSPR) product. The vulnerability affects versions 4.4.0.0 to 4.4.0.6 and 4.5.0.1 and 4.5.0.2. In certain configurations the vulnerability could disclose sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28339	The usc-e-shop (aka Collne Welcart e-Commerce) plugin before 1.9.36 for WordPress allows Object Injection because of usces_unserialize. There is not a complete POP chain.	7.5	More Details
CVE-2020-8580	SANtricity OS Controller Software versions 11.30 and higher are susceptible to a vulnerability which allows an unauthenticated attacker with access to the system to cause a Denial of Service (DoS).	7.5	More Details
CVE-2020-26882	In Play Framework 2.6.0 through 2.8.2, data amplification can occur when an application accepts multipart/form-data JSON input.	7.5	More Details
CVE-2020-26883	In Play Framework 2.6.0 through 2.8.2, stack consumption can occur because of unbounded recursion during parsing of crafted JSON documents.	7.5	More Details
CVE-2020-28345	An issue was discovered on LG mobile devices with Android OS 10 software. The Wi-Fi subsystem may crash because of the lack of a NULL parameter check. The LG ID is LVE-SMP-200025 (November 2020).	7.5	More Details
CVE-2020-26810	SAP Commerce Cloud (Accelerator Payment Mock), versions - 1808, 1811, 1905, 2005, allows an unauthenticated attacker to submit a crafted request over a network to a particular SAP Commerce module URL which will be processed without further interaction, the crafted request can render the SAP Commerce service itself unavailable leading to Denial of Service with no impact on confidentiality or integrity.	7.5	More Details
CVE-2020-27196	An issue was discovered in PlayJava in Play Framework 2.6.0 through 2.8.2. The body parsing of HTTP requests eagerly parses a payload given a Content-Type header. A deep JSON structure sent to a valid POST endpoint (that may or may not expect JSON payloads) causes a StackOverflowError and Denial of Service.	7.5	More Details
CVE-2020-27589	Synopsys hub-rest-api-python (aka blackduck on PyPI) version 0.0.25 - 0.0.52 does not validate SSL certificates in certain cases.	7.5	More Details
CVE-2020-27688	RVToolsPasswordEncryption.exe in RVTools 4.0.6 allows users to encrypt passwords to be used in the configuration files. This encryption used a static IV and key, and thus using the Decrypt() method from VISKD.cs from the RVTools.exe executable allows for decrypting the encrypted passwords. The accounts used in the configuration files have access to vSphere instances.	7.5	More Details
CVE-2020-28344	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. System services may crash because of the lack of a NULL parameter check. The LG ID is LVE-SMP-200024 (November 2020).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10291	Visual Components (owned by KUKA) is a robotic simulator that allows simulating factories and robots in order toimprove planning and decision-making processes. Visual Components software requires a special license which can beobtained from a network license server. The network license server binds to all interfaces (0.0.0.0) and listensfor packets over UDP port 5093. No authentication/authorization is required in order to communicate with theserver. The protocol being used is a property protocol by RMS Sentinel which provides the licensing infrastructurefor the network license server. RMS Sentinel license manager service exposes UDP port 5093 which provides sensitivesystem information that could be leveraged for further exploitation without any kind of authentication. Thisinformation includes detailed hardware and OS characteristics.After a decryption process, a textual protocol is found which contains a simple header with the requested command,application-identifier, and some arguments. The protocol leaks information regarding the receiving serverinformation, license information and managing licenses, among others.Through this flaw, attackers can retreive information about a KUKA simulation system, particularly, the version ofthe licensing server, which is connected to the simulator, and which will allow them to launch local simulationswith similar characteristics, further understanding the dynamics of motion virtualization and opening doors toother attacks (see RVDP#711 and RVDP#712 for subsequent vulnerabilities that compromise integrity andavailability).Beyond compromising simulations, Visual Components provides capabilities to interface with industrial machinery.Particularly, their PLC Connectivity feature 'makes it easy' to connect simulations with control systems usingeither the industry standard OPC UA or other supported vendor specific interfaces. This fills the gap of jumpingfrom simulation to real and enables attackers to pivot from the Visual Components simulator to robots or otherIndustrial Control System (ICS) devices, such as PLCs.	7.5	More Details
CVE-2020-26521	The JWT library in NATS nats-server before 2.1.9 allows a denial of service (a nil dereference in Go code).	7.5	More Details
CVE-2020-25661	A Red Hat only CVE-2020-12351 regression issue was found in the way the Linux kernel's Bluetooth implementation handled L2CAP packets with A2MP CID. This flaw allows a remote attacker in an adjacent range to crash the system, causing a denial of service or potentially executing arbitrary code on the system by sending a specially crafted L2CAP packet. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.5	More Details
CVE-2020-28196	MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoded Kerberos message because the lib/krb5/asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3588	A vulnerability in virtualization channel messaging in Cisco Webex Meetings Desktop App for Windows could allow a local attacker to execute arbitrary code on a targeted system. This vulnerability occurs when this app is deployed in a virtual desktop environment and using virtual environment optimization. This vulnerability is due to improper validation of messages processed by the Cisco Webex Meetings Desktop App. A local attacker with limited privileges could exploit this vulnerability by sending malicious messages to the affected software by using the virtualization channel interface. A successful exploit could allow the attacker to modify the underlying operating system configuration, which could allow the attacker to execute arbitrary code with the privileges of a targeted user. Note: This vulnerability can be exploited only when Cisco Webex Meetings Desktop App is in a virtual desktop environment on a hosted virtual desktop (HVD) and is configured to use the Cisco Webex Meetings virtual desktop plug-in for thin clients.	7.3	More Details
CVE-2020-7766	This affects all versions of package json-ptr. The issue occurs in the set operation (https://flitbit.github.io/json-ptr/classes/_src_pointer_.jsonpointer.htmlset) when the force flag is set to true. The function recursively set the property in the target object, however it does not properly check the key being set, leading to a prototype pollution.	7.3	More Details
CVE-2020-3556	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client Software could allow an authenticated, local attacker to cause a targeted AnyConnect user to execute a malicious script. The vulnerability is due to a lack of authentication to the IPC listener. An attacker could exploit this vulnerability by sending crafted IPC messages to the AnyConnect client IPC listener. A successful exploit could allow an attacker to cause the targeted AnyConnect user to execute a script. This script would execute with the privileges of the targeted AnyConnect user. In order to successfully exploit this vulnerability, there must be an ongoing AnyConnect session by the targeted user at the time of the attack. To exploit this vulnerability, the attacker would also need valid user credentials on the system upon which the AnyConnect client is being run. Cisco has not released software updates that address this vulnerability.	7.3	More Details
CVE-2020-16125	gdm3 versions before 3.36.2 or 3.38.2 would start gnome-initial-setup if gdm3 can't contact the accountservice service via dbus in a timely manner; on Ubuntu (and potentially derivatives) this could be be chained with an additional issue that could allow a local user to create a new privileged account.	7.2	More Details
CVE-2020-24063	The Canto plugin 1.3.0 for WordPress allows includes/lib/download.php?subdomain= SSRF.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7129	A remote execution of arbitrary commands vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	7.2	More Details
CVE-2020-26808	SAP AS ABAP(DMIS), versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 and SAP S4 HANA(DMIS), versions - 101, 102, 103, 104, 105, allows an authenticated attacker to inject arbitrary code into function module leading to code injection that can be executed in the application which affects the confidentiality, availability and integrity of the application.	7.2	More Details
CVE-2020-26820	SAP NetWeaver AS JAVA, versions - 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker who is authenticated as an administrator to use the administrator console, to expose unauthenticated access to the file system and upload a malicious file. The attacker or another user can then use a separate mechanism to execute OS commands through the uploaded file leading to Privilege Escalation and completely compromise the confidentiality, integrity and availability of the server operating system and any application running on it.	7.2	More Details
CVE-2020-15297	Insufficient validation in the Bitdefender Update Server and BEST Relay components of Bitdefender Endpoint Security Tools versions prior to 6.6.20.294 allows an unprivileged attacker to bypass the in-place mitigations and interact with hosts on the network. This issue affects: Bitdefender Update Server versions prior to 6.6.20.294.	7.1	More Details
CVE-2017-18926	raptor_xml_writer_start_element_common in raptor_xml_writer.c in Raptor RDF Syntax Library 2.0.15 miscalculates the maximum nspace declarations for the XML writer, leading to heap-based buffer overflows (sometimes seen in raptor_qname_format_as_xml).	7.1	More Details
CVE-2020-24400	Magento versions 2.4.0 and 2.3.5 (and earlier) are affected by an SQL Injection vulnerability that could lead to sensitive information disclosure. This vulnerability could be exploited by an authenticated user with permissions to the product listing page to read data from the database.	7.1	More Details
CVE-2020-5388	Dell Inspiron 15 7579 2-in-1 BIOS versions prior to 1.31.0 contain an Improper SMM communication buffer verification vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7207	A local elevation of privilege using physical access security vulnerability was found in HPE Proliant Gen10 Servers using Intel Innovation Engine (IE). This attack requires a physical attack to the server motherboard. To mitigate this issue, ensure your server is always physically secured. HPE will not address this issue in the impacted Gen 10 servers listed. HPE recommends using appropriate physical security methods as a compensating control to disallow an attacker from having physical access to the server main circuit board.	6.8	More Details
CVE-2020-14366	A vulnerability was found in keycloak, where path traversal using URL-encoded path segments in the request is possible because the resources endpoint applies a transformation of the url path to the file path. Only few specific folder hierarchies can be exposed by this flaw	6.8	More Details
CVE-2020-4097	In HCL Notes version 9 previous to release 9.0.1 FixPack 10 Interim Fix 8, version 10 previous to release 10.0.1 FixPack 6 and version 11 previous to 11.0.1 FixPack 1, a vulnerability in the input parameter handling of the Notes Client could potentially be exploited by an attacker resulting in a buffer overflow. This could enable an attacker to crash HCL Notes or execute attacker-controlled code on the client.	6.8	More Details
CVE-2020-24432	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document.	6.7	More Details
CVE-2020-27129	A vulnerability in the remote management feature of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands and potentially gain elevated privileges. The vulnerability is due to improper validation of commands to the remote management CLI of the affected application. An attacker could exploit this vulnerability by sending malicious requests to the affected application. A successful exploit could allow the attacker to inject arbitrary commands and potentially gain elevated privileges.	6.7	More Details
CVE-2020-27122	A vulnerability in the Microsoft Active Directory integration of Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to elevate privileges on an affected device. To exploit this vulnerability, an attacker would need to have a valid administrator account on an affected device. The vulnerability is due to incorrect privilege assignment. An attacker could exploit this vulnerability by logging in to the system with a crafted Active Directory account. A successful exploit could allow the attacker to obtain root privileges on an affected device.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12145	Silver Peak Unity Orchestrator versions prior to 8.9.11+, 8.10.11+, or 9.0.1+ uses HTTP headers to authenticate REST API calls from localhost. This makes it possible to log in to Orchestrator by introducing an HTTP HOST header set to 127.0.0.1 or localhost. Orchestrator instances that are hosted by customers –on-premise or in a public cloud provider –are affected by this vulnerability.	6.6	More Details
CVE-2020-12147	In Silver Peak Unity Orchestrator versions prior to 8.9.11+, 8.10.11+, or 9.0.1+, an authenticated user can make unauthorized MySQL queries against the Orchestrator database using the /sqlExecution REST API, which had been used for internal testing.	6.6	More Details
CVE-2020-12146	In Silver Peak Unity Orchestrator versions prior to 8.9.11+, 8.10.11+, or 9.0.1+, an authenticated user can access, modify, and delete restricted files on the Orchestrator server using the/debugFiles REST API.	6.6	More Details
CVE-2020-5943	In versions 14.1.0-14.1.0.1 and 14.1.2.5-14.1.2.7, when a BIG-IP object is created or listed through the REST interface, the protected fields are obfuscated in the REST response, not protected via a SecureVault cryptogram as TMSH does. One example of protected fields is the GTM monitor password.	6.5	More Details
CVE-2020-3592	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system. The vulnerability is due to insufficient authorization checking on an affected system. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to gain privileges beyond what would normally be authorized for their configured user authorization level. This could allow the attacker to modify the configuration of an affected system.	6.5	More Details
CVE-2020-5643	Improper input validation vulnerability in Cybozu Garoon 5.0.0 to 5.0.2 allows a remote authenticated attacker to delete some data of the bulletin board via unspecified vector.	6.5	More Details
CVE-2020-2319	Jenkins VMware Lab Manager Slaves Plugin 0.2.8 and earlier stores a password unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2020-22273	Neoflex Video Subscription System Version 2.0 is affected by CSRF which allows the Website's Settings to be changed (such as Payment Settings)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7762	This affects the package jsreport-chrome-pdf before 1.10.0.	6.5	More Details
CVE-2020-2318	Jenkins Mail Commander Plugin for Jenkins-ci Plugin 1.0.0 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details
CVE-2020-28349	An inaccurate frame deduplication process in ChirpStack Network Server 3.9.0 allows a malicious gateway to perform uplink Denial of Service via malformed frequency attributes in CollectAndCallOnceCollect in internal/uplink/collect.go. NOTE: the vendor's position is that there are no "guarantees that allowing untrusted LoRa gateways to the network should still result in a secure network.	6.5	More Details
CVE-2020-24401	Magento versions 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect authorization vulnerability. A user can still access resources provisioned under their old role after an administrator removes the role or disables the user's account.	6.5	More Details
CVE-2020-28241	libmaxminddb before 1.4.3 has a heap-based buffer over-read in dump_entry_data_list in maxminddb.c.	6.5	More Details
CVE-2020-28242	An issue was discovered in Asterisk Open Source 13.x before 13.37.1, 16.x before 16.14.1, 17.x before 17.8.1, and 18.x before 18.0.1 and Certified Asterisk before 16.8-cert5. If Asterisk is challenged on an outbound INVITE and the nonce is changed in each response, Asterisk will continually send INVITEs in a loop. This causes Asterisk to consume more and more memory since the transaction will never terminate (even if the call is hung up), ultimately leading to a restart or shutdown of Asterisk. Outbound authentication must be configured on the endpoint for this to occur.	6.5	More Details
CVE-2020-2315	Jenkins Visualworks Store Plugin 1.1.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details
CVE-2020-27616	ati_2d_blt in hw/display/ati_2d.c in QEMU 4.2.1 can encounter an outside-limits situation in a calculation. A guest can crash the QEMU process.	6.5	More Details
CVE-2020-27617	eth_get_gso_type in net/eth.c in QEMU 4.2.1 allows guest OS users to trigger an assertion failure. A guest can crash the QEMU process via packet data that lacks a valid Layer 3 protocol.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2312	Jenkins SQLPlus Script Runner Plugin 2.0.12 and earlier does not mask a password provided as command line argument in build logs.	6.5	More Details
CVE-2020-2304	Jenkins Subversion Plugin 2.13.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details
CVE-2020-9300	The Access Control issues include allowing a regular user to view a restricted incident, user role escalation to admin, users adding themselves as a participant in a restricted incident, and users able to view restricted incidents via the search feature. If your install has followed the secure deployment guidelines the risk of this is lowered, as this may only be exploited by an authenticated user.	6.5	More Details
CVE-2020-27128	A vulnerability in the application data endpoints of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to write arbitrary files to an affected system. The vulnerability is due to improper validation of requests to APIs. An attacker could exploit this vulnerability by sending malicious requests to an API within the affected application. A successful exploit could allow the attacker to conduct directory traversal attacks and write files to an arbitrary location on the targeted system.	6.5	More Details
CVE-2020-0450	In rw_i93_sm_format of rw_i93.cc, there is a possible out of bounds read due to uninitialized data. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-157650336	6.5	More Details
CVE-2020-26084	A vulnerability in the REST API of Cisco Edge Fog Fabric could allow an authenticated, remote attacker to access files outside of their authorization sphere on an affected device. The vulnerability is due to incorrect authorization enforcement on an affected system. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27403	A vulnerability in the TCL Android Smart TV series V8-R851T02-LF1 V295 and below and V8-T658T01-LF1 V373 and below by TCL Technology Group Corporation allows an attacker on the adjacent network to arbitrarily browse and download sensitive files over an insecure web server running on port 7989 that lists all files & directories. An unprivileged remote attacker on the adjacent network, can download most system files, leading to serious critical information disclosure. Also, some TV models and/or FW versions may expose the webserver with the entire filesystem accessible on another port. For example, nmap scan for all ports run directly from the TV model U43P6046 (Android 8.0) showed port 7983 not mentioned in the original CVE description, but containing the same directory listing of the entire filesystem. This webserver is bound (at least) to localhost interface and accessible freely to all unprivileged installed apps on the Android such as a regular web browser. Any app can therefore read any files of any other apps including Android system settings including sensitive data such as saved passwords, private keys etc.	6.5	More Details
CVE-2020-2305	Jenkins Mercurial Plugin 2.11 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details
CVE-2020-4482	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 could allow an authenticated user to bypass security. A user with access to a snapshot could apply unauthorized additional statuses via direct rest calls. IBM X-Force ID: 181856.	6.5	More Details
CVE-2020-3590	A vulnerability in the web-based management interface of the Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.4	More Details
CVE-2020-3587	A vulnerability in the web-based management interface of the Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3371	A vulnerability in the web UI of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject arbitrary code and execute arbitrary commands at the underlying operating system level. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary commands at the underlying operating system level.	6.3	More Details
CVE-2020-28049	An issue was discovered in SDDM before 0.19.0. It incorrectly starts the X server in a way that - for a short time period - allows local unprivileged users to create a connection to the X server without providing proper authentication. A local attacker can thus access X server display contents and, for example, intercept keystrokes or access the clipboard. This is caused by a race condition during Xauthority file creation.	6.3	More Details
CVE-2020-5795	UNIX Symbolic Link (Symlink) Following in TP-Link Archer A7(US)_V5_200721 allows an authenticated admin user, with physical access and network access, to execute arbitrary code after plugging a crafted USB drive into the router.	6.2	More Details
CVE-2020-28249	Joplin 1.2.6 for Desktop allows XSS via a LINK element in a note.	6.1	More Details
CVE-2020-28351	The conferencing component on Mitel ShoreTel 19.46.1802.0 devices could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack (via the PATH_INFO to index.php) due to insufficient validation for the time_zone object in the HOME_MEETING& page.	6.1	More Details
CVE-2020-3579	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3551	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2020-24353	Pega Platform before 8.4.0 has a XSS issue via stream rule parameters used in the request header.	6.1	More Details
CVE-2020-28364	A stored cross-site scripting (XSS) vulnerability affects the Web UI in Locust before 1.3.2, if the installation violates the usage expectations by exposing this UI to outside users.	6.1	More Details
CVE-2020-15951	Immuta v2.8.2 accepts user-supplied project names without properly sanitizing the input, allowing attackers to inject arbitrary HTML content that is rendered as part of the application. An attacker could leverage this to redirect application users to a phishing website in an attempt to steal credentials.	6.1	More Details
CVE-2020-14222	HCL Digital Experience 8.5, 9.0, 9.5 is susceptible to cross site scripting (XSS). One subcomponent is vulnerable to reflected XSS. In reflected XSS, an attacker must induce a victim to click on a crafted URL from some delivery mechanism (email, other web site).	6.1	More Details
CVE-2020-14240	HCL Notes versions previous to releases 9.0.1 FP10 IF8, 10.0.1 FP6 and 11.0.1 FP1 is susceptible to a Stored Cross-site Scripting (XSS) vulnerability. An attacker could use this vulnerability to execute script in a victim's Web browser within the security context of the hosting Web site and/or steal the victim's cookie-based authentication credentials.	6.1	More Details
CVE-2020-27691	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 allows XSS via URLBlocking Settings, SNMP Settings, and System Log Settings.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26505	A Stored Cross-Site Scripting (XSS) vulnerability in the “Marmind” web application with version 4.1.141.0 allows an attacker to inject code that will later be executed by legitimate users when they open the assets containing the JavaScript code. This would allow an attacker to perform unauthorized actions in the application on behalf of legitimate users or spread malware via the application. By using the “Assets Upload” function, an attacker can abuse the upload function to upload a malicious PDF file containing a stored XSS.	6.1	More Details
CVE-2020-8577	SANtricity OS Controller Software versions 11.50.1 and higher are susceptible to a vulnerability which could allow an attacker to discover sensitive information by intercepting its transmission within an https session.	5.9	More Details
CVE-2020-26213	In teler before version 0.0.1, if you run teler inside a Docker container and encounter `errors.Exit` function, it will cause denial-of-service (`SIGSEGV`) because it doesn't get process ID and process group ID of teler properly to kills. The issue is patched in teler 0.0.1 and 0.0.1-dev5.1.	5.9	More Details
CVE-2020-28168	Axios NPM package 0.21.0 contains a Server-Side Request Forgery (SSRF) vulnerability where an attacker is able to bypass a proxy by providing a URL that responds with a redirect to a restricted host or IP address.	5.9	More Details
CVE-2020-7764	This affects the package find-my-way before 2.2.5, from 3.0.0 and before 3.0.5. It accepts the Accept-Version' header by default, and if versioned routes are not being used, this could lead to a denial of service. Accept-Version can be used as an unkeyed header in a cache poisoning attack.	5.9	More Details
CVE-2020-25655	An issue was discovered in ManagedClusterView API, that could allow secrets to be disclosed to users without the correct permissions. Views created for an admin user would be made available for a short time to users with only view permission. In this short time window the user with view permission could read cluster secrets that should only be disclosed to admin users.	5.7	More Details
CVE-2020-6015	Check Point Endpoint Security for Windows before E84.10 can reach denial of service during clean install of the client which will prevent the storage of service log files in non-standard locations.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8276	The implementation of Brave Desktop's privacy-preserving analytics system (P3A) between 1.1 and 1.18.35 logged the timestamp of when the user last opened an incognito window, including Tor windows. The intended behavior was to log the timestamp for incognito windows excluding Tor windows. Note that if a user has P3A enabled, the timestamp is not sent to Brave's server, but rather a value from:Used in last 24hUsed in last week but not 24hUsed in last 28 days but not weekEver used but not in last 28 daysNever usedThe privacy risk is low because a local attacker with disk access cannot tell if the timestamp corresponds to a Tor window or a non-Tor incognito window.	5.5	More Details
CVE-2020-0443	In LocaleList of LocaleList.java, there is a possible forced reboot due to an uncaught exception. This could lead to local denial of service requiring factory reset to restore with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-152410253	5.5	More Details
CVE-2020-2314	Jenkins AppSpider Plugin 1.0.12 and earlier stores a password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	5.5	More Details
CVE-2020-0437	In CellBroadcastReceiver's intent handlers, there is a possible denial of service due to a missing permission check. This could lead to local denial of service of emergency alerts with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-162741784	5.5	More Details
CVE-2020-0448	In getPhoneAccountsForPackage of TelecomServiceImpl.java, there is a possible way to access a tracking identifier due to a missing permission check. This could lead to local information disclosure of the identifier, which could be used to track an account across devices, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-153995334	5.5	More Details
CVE-2020-0453	In updateNotification of BeamTransferManager.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-8.0 Android-8.1Android ID: A-159060474	5.5	More Details
CVE-2020-0454	In callCallbackForRequest of ConnectivityService.java, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure of the current SSID with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-161370134	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4568	IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, and 4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 184157.	5.5	More Details
CVE-2020-12485	The frame touch module does not make validity judgments on parameter lengths when processing specific parameters,which caused out of the boundary when memory access.The vulnerability eventually leads to a local DOS on the device.	5.5	More Details
CVE-2020-27123	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to read arbitrary files on the underlying operating system of an affected device. The vulnerability is due to an exposed IPC function. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process on an affected device. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system of the affected device.	5.5	More Details
CVE-2020-17490	The TLS module within SaltStack Salt through 3002 creates certificates with weak file permissions.	5.5	More Details
CVE-2020-27152	An issue was discovered in ioapic_lazy_update_eoi in arch/x86/kvm/ioapic.c in the Linux kernel before 5.9.2. It has an infinite loop related to improper interaction between a resampler and edge triggering, aka CID-77377064c3a9.	5.5	More Details
CVE-2020-0424	In send_vc of res_send.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-161362564	5.5	More Details
CVE-2020-5667	Studyplus App for Android v6.3.7 and earlier and Studyplus App for iOS v8.29.0 and earlier use a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	5.5	More Details
CVE-2020-23136	Microweber v1.1.18 is affected by no session expiry after log-out.	5.5	More Details
CVE-2020-27019	Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to an information disclosure vulnerability which could allow an attacker to access a specific database and key.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23139	Microweber 1.1.18 is affected by broken authentication and session management. Local session hijacking may occur, which could result in unauthorized access to system data or functionality, or a complete system compromise.	5.5	More Details
CVE-2020-27018	Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to a server side request forgery vulnerability which could allow an authenticated attacker to abuse the product's web server and grant access to web resources or parts of local files. An attacker must already have obtained authenticated privileges on the product to exploit this vulnerability.	5.5	More Details
CVE-2020-27690	The Relish (Verve Connect) VH510 device with firmware before 1.0.1.6L0516 contains a buffer overflow within its web management portal. When a POST request is sent to /boaform/admin/formDOMAINBLK with a large blkDomain value, the Boa server crashes.	5.5	More Details
CVE-2020-28408	The server in Dundas BI through 8.0.0.1001 allows XSS via an HTML label when creating or editing a dashboard.	5.4	More Details
CVE-2020-28409	The server in Dundas BI through 8.0.0.1001 allows XSS via addition of a Component (e.g., a button) when events such as click, hover, etc. occur.	5.4	More Details
CVE-2020-4760	IBM Content Navigator 3.0CD 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: 188737.	5.4	More Details
CVE-2020-4704	IBM Content Navigator 3.0CD is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 187189.	5.4	More Details
CVE-2019-7356	Subrion CMS v4.2.1 allows XSS via the panel/phrases/ VALUE parameter.	5.4	More Details
CVE-2020-25267	An XSS issue exists in the question-pool file-upload preview feature in ILIAS 6.4.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28047	AudimexEE before 14.1.1 is vulnerable to Reflected XSS (Cross-Site-Scripting). If the recommended security configuration parameter "unique_error_numbers" is not set, remote attackers can inject arbitrary web script or HTML via 'action, cargo, panel' parameters that can lead to data leakage.	5.4	More Details
CVE-2020-9299	There were XSS vulnerabilities discovered and reported in the Dispatch application, affecting name and description parameters of Incident Priority, Incident Type, Tag Type, and Incident Filter. This vulnerability can be exploited by an authenticated user.	5.4	More Details
CVE-2020-2317	Jenkins FindBugs Plugin 5.0.0 and earlier does not escape the annotation message in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide report files to Jenkins FindBugs Plugin's post build step.	5.4	More Details
CVE-2020-2316	Jenkins Static Analysis Utilities Plugin 1.96 and earlier does not escape the annotation message in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-5940	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.2.3, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility.	5.4	More Details
CVE-2020-7761	This affects the package @absolunet/kafe before 3.2.10. It allows cause a denial of service when validating crafted invalid emails.	5.3	More Details
CVE-2020-28327	A res_pjsip_session crash was discovered in Asterisk Open Source 13.x before 13.37.1, 16.x before 16.14.1, 17.x before 17.8.1, and 18.x before 18.0.1. and Certified Asterisk before 16.8-cert5. Upon receiving a new SIP Invite, Asterisk did not return the created dialog locked or referenced. This caused a gap between the creation of the dialog object, and its next use by the thread that created it. Depending on some off-nominal circumstances and timing, it was possible for another thread to free said dialog in this gap. Asterisk could then crash when the dialog object, or any of its dependent objects, were dereferenced or accessed next by the initial-creation thread. Note, however, that this crash can only occur when using a connection-oriented protocol (e.g., TCP or TLS, but not UDP) for SIP transport. Also, the remote client must be authenticated, or Asterisk must be configured for anonymous calling.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26811	SAP Commerce Cloud (Accelerator Payment Mock), versions - 1808, 1811, 1905, 2005, allows an unauthenticated attacker to submit a crafted request over a network to a particular SAP Commerce module URL which will be processed without further interaction, the crafted request leads to Server Side Request Forgery attack which could lead to retrieval of limited pieces of information about the service with no impact on integrity or availability.	5.3	More Details
CVE-2020-26809	SAP Commerce Cloud, versions- 1808,1811,1905,2005, allows an attacker to bypass existing authentication and permission checks via the '/medias' endpoint hence gaining access to Secure Media folders. This folder could contain sensitive files that results in disclosure of sensitive information and impact system configuration confidentiality.	5.3	More Details
CVE-2020-25662	A Red Hat only CVE-2020-12352 regression issue was found in the way the Linux kernel's Bluetooth stack implementation handled the initialization of stack memory when handling certain AMP packets. This flaw allows a remote attacker in an adjacent range to leak small portions of stack memory on the system by sending specially crafted AMP packets. The highest threat from this vulnerability is to data confidentiality.	5.3	More Details
CVE-2020-8133	A wrong generation of the passphrase for the encrypted block in Nextcloud Server 19.0.1 allowed an attacker to overwrite blocks in a file.	5.3	More Details
CVE-2020-8267	A security issue was found in UniFi Protect controller v1.14.10 and earlier.The authentication in the UniFi Protect controller API was using “x-token” improperly, allowing attackers to use the API to send authenticated messages without a valid token.This vulnerability was fixed in UniFi Protect v1.14.11 and newer.This issue does not impact UniFi Cloud Key Gen 2 plus.This issue does not impact UDM-Pro customers with UniFi Protect stopped.Affected Products:UDM-Pro firmware 1.7.2 and earlier.UNVR firmware 1.3.12 and earlier.Mitigation:Update UniFi Protect to v1.14.11 or newer version; the UniFi Protect controller can be updated through your UniFi OS settings.Alternatively, you can update UNVR and UDM-Pro to:- UNVR firmware to 1.3.15 or newer.- UDM-Pro firmware to 1.8.0 or newer.	5.3	More Details
CVE-2020-27146	The Core component of TIBCO Software Inc.'s TIBCO iProcess Workspace (Browser) contains a vulnerability that theoretically allows an unauthenticated attacker with network access to execute a Cross Site Request Forgery (CSRF) attack on the affected system. A successful attack using this vulnerability requires human interaction from an authenticated user other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO iProcess Workspace (Browser): versions 11.6.0 and below.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24402	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect permissions vulnerability in the Integrations component. This vulnerability could be abused by authenticated users with permissions to the Resource Access API to delete customer details via the REST API without authorization.	4.9	More Details
CVE-2020-27017	Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to an XML External Entity Processing (XXE) vulnerability which could allow an authenticated administrator to read arbitrary local files. An attacker must already have obtained product administrator/root privileges to exploit this vulnerability.	4.9	More Details
CVE-2020-26814	SAP Process Integration (PGP Module - Business-to-Business Add On), version - 1.0, allows an attacker to read PGP Keys under certain conditions in the PGP Module of Business-to-Business Add-On, these keys can then be used to read messages processed by the module leading to Information Disclosure.	4.9	More Details
CVE-2020-4651	IBM Maximo Spatial Asset Management 7.6.0.3, 7.6.0.4, 7.6.0.5, and 7.6.1.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 186024.	4.8	More Details
CVE-2020-26083	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need to have valid administrative credentials.	4.8	More Details
CVE-2020-28368	Xen through 4.14.x allows guest OS administrators to obtain sensitive information (such as AES keys from outside the guest) via a side-channel attack on a power/energy monitoring interface, aka a "Platypus" attack. NOTE: there is only one logically independent fix: to change the access control for each such interface in Xen.	4.4	More Details
CVE-2020-27693	Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 stores administrative passwords using a hash that is considered outdated.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24431	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.4	More Details
CVE-2020-4484	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 could disclose sensitive information to an authenticated user that could be used in further attacks against the system. IBM X-Force ID: 181858.	4.3	More Details
CVE-2020-26506	An Authorization Bypass vulnerability in the Marmind web application with version 4.1.141.0 allows users with lower privileges to gain control to files uploaded by administrative users. The accessed files were not visible by the low privileged users in the web GUI.	4.3	More Details
CVE-2020-4483	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 181857.	4.3	More Details
CVE-2020-2302	A missing permission check in Jenkins Active Directory Plugin 2.19 and earlier allows attackers with Overall/Read permission to access the domain health check diagnostic page.	4.3	More Details
CVE-2020-2303	A cross-site request forgery (CSRF) vulnerability in Jenkins Active Directory Plugin 2.19 and earlier allows attackers to perform connection tests, connecting to attacker-specified or previously configured Active Directory servers using attacker-specified credentials.	4.3	More Details
CVE-2020-2313	A missing permission check in Jenkins Azure Key Vault Plugin 2.0 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2020-6316	SAP ERP and SAP S/4 HANA allows an authenticated user to see cost records to objects to which he has no authorization in PS reporting, leading to Missing Authorization check.	4.3	More Details
CVE-2020-5944	In BIG-IQ 7.1.0, accessing the DoS Summary events and DNS Overview pages in the BIG-IQ system interface returns an error message due to disabled Grafana reverse proxy in web service configuration. F5 has done further review of this vulnerability and has re-classified it as a defect. CVE-2020-5944 will continue to be referenced in F5 Security Advisory K57274211 and will not be assigned to other F5 vulnerabilities.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26086	A vulnerability in the video endpoint API (xAPI) of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, remote attacker to gain access to sensitive information on an affected device. The vulnerability is due to improper storage of sensitive information on an affected device. An attacker could exploit this vulnerability by accessing information that should not be accessible to users with low privileges. A successful exploit could allow the attacker to gain access to sensitive information.	4.3	More Details
CVE-2020-27121	A vulnerability in Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) Software could allow an authenticated, remote attacker to cause the Cisco XCP Authentication Service on an affected device to restart, resulting in a denial of service (DoS) condition. The vulnerability is due to improper handling of login requests. An attacker could exploit this vulnerability by sending a crafted client login request to an affected device. A successful exploit could allow the attacker to cause a process to crash, resulting in a DoS condition for new login attempts. Users who are authenticated at the time of the attack would not be affected. There are workarounds that address this vulnerability.	4.3	More Details
CVE-2020-2306	A missing permission check in Jenkins Mercurial Plugin 2.11 and earlier allows attackers with Overall/Read permission to obtain a list of names of configured Mercurial installations.	4.3	More Details
CVE-2020-2310	Missing permission checks in Jenkins Ansible Plugin 1.0 and earlier allow attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2020-2309	A missing/An incorrect permission check in Jenkins Kubernetes Plugin 1.27.3 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2020-2307	Jenkins Kubernetes Plugin 1.27.3 and earlier allows low-privilege users to access possibly sensitive Jenkins controller environment variables.	4.3	More Details
CVE-2020-3591	A vulnerability in the web-based management interface of the Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24405	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect permissions issue vulnerability in the Inventory module. This vulnerability could be abused by authenticated users to modify inventory stock data without authorization.	4.3	More Details
CVE-2020-2308	A missing permission check in Jenkins Kubernetes Plugin 1.27.3 and earlier allows attackers with Overall/Read permission to list global pod template names.	4.3	More Details
CVE-2020-2311	A missing permission check in Jenkins AWS Global Configuration Plugin 1.5 and earlier allows attackers with Overall/Read permission to replace the global AWS configuration.	4.3	More Details
CVE-2020-8150	A cryptographic issue in Nextcloud Server 19.0.1 allowed an attacker to downgrade the encryption scheme and break the integrity of encrypted files.	4.1	More Details
CVE-2020-24406	When in maintenance mode, Magento version 2.4.0 and 2.3.4 (and earlier) are affected by an information disclosure vulnerability that could expose the installation path during build deployments. This information could be helpful to attackers if they are able to identify other exploitable vulnerabilities in the environment.	3.7	More Details
CVE-2020-4650	IBM Maximo Spatial Asset Management 7.6.0.3, 7.6.0.4, 7.6.0.5, and 7.6.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 186023.	3.3	More Details
CVE-2020-16121	PackageKit provided detailed error messages to unprivileged callers that exposed information about file presence and mimetype of files that the user would be unable to determine on its own.	3.3	More Details
CVE-2020-24438	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a use-after-free vulnerability that could result in a memory address leak. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2020-24427	Acrobat Reader versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an input validation vulnerability when decoding a crafted codec that could result in the disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24426	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2020-26807	SAP ERP Client for E-Bilanz, version - 1.0, installation sets Incorrect default filesystem permissions are set in its installation folder which allows anyone to modify the files in the folder.	3.3	More Details
CVE-2020-24434	Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2020-24439	Acrobat Reader DC for macOS versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a security feature bypass. While the practical security impact is minimal, a defense-in-depth fix has been implemented to further harden the Adobe Reader update process.	2.8	More Details
CVE-2020-24404	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect permissions vulnerability within the Integrations component. This vulnerability could be abused by users with permissions to the Pages resource to delete cms pages via the REST API without authorization.	2.7	More Details
CVE-2020-24403	Magento version 2.4.0 and 2.3.5p1 (and earlier) are affected by an incorrect user permissions vulnerability within the Inventory component. This vulnerability could be abused by authenticated users with Inventory and Source permissions to make unauthorized changes to inventory source data via the REST API.	2.7	More Details
CVE-2018-1725	IBM QRadar SIEM 7.3 and 7.4 n a multi tenant configuration could be vulnerable to information disclosure. IBM X-Force ID: 147440.	2.3	More Details
CVE-2018-16919	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-2018-16920	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-2018-16914	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-2018-16918	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-2018-16917	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-2018-16916	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-2018-16915	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-2020-27165	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-28050. Reason: This candidate is a reservation duplicate of CVE-2020-28050. Notes: All CVE users should reference CVE-2020-28050 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2018-16913	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-2018-16912	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-2018-16911	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-2018-16910	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-2018-16909	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-2018-16922	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-2018-16908	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-2018-16921	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-2018-16934	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-2018-16923	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-2018-16924	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-2018-16925	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-2018-16926	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-2018-16927	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-2018-16928	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-2018-16929	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-2018-16930	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-2018-16931	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-2018-16932	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-2018-16933	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-2018-16935	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-2018-16936	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-2018-16906	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-2018-16907	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-2020-27346	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-2018-16905	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-2012-6156	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-2014-7856	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-2014-7855	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-2014-7820	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-2013-6506	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-2013-6505	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-2013-6504	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-2013-6503	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-2013-6502	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-2012-6157	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-2012-6155	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-2018-16904	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-2012-6154	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-2012-5555	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-2012-5528	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-2011-4978	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-2011-4977	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-2011-4976	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-2011-4975	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-2011-4974	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-2010-5116	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-2015-0300	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-2015-1823	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-2015-1824	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-2015-1825	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-2017-15154	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-2017-15153	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-2017-15152	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-2017-15151	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-2017-15150	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-2017-15149	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-2017-15148	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-2017-15147	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-2017-15146	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-2017-15145	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-2017-15144	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-2017-15143	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-2017-15142	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-2017-15141	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-2017-15140	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-2016-0745	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-2016-0744	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-2016-0743	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-2015-1826	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-2010-5115	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-2010-5114	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-2010-5113	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-2003-1602	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-2003-1600	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-2002-2442	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-2002-2441	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-2002-2440	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-2001-1592	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-2001-1591	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-2001-1590	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-2001-1589	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-2001-1588	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-2000-1252	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-2000-1251	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-2000-1250	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-2000-1249	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-2000-1248	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-1999-1598	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-1999-1597	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-1999-1596	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-1999-1595	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-1999-1594	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-2003-1601	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-2004-2772	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-2010-5112	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-2004-2773	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-2009-5106	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-2009-5105	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-2009-5104	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-2009-5070	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-2009-5069	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-2008-7308	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-2008-7307	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-2008-7306	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-2008-7305	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-2008-7304	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-2007-6749	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-2007-6748	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-2007-6747	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-2006-7251	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-2005-4894	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-2005-4893	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-2005-4892	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-2004-2775	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-2004-2774	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-2017-15155	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-2017-15156	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-2017-15157	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-2017-17372	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-2017-17370	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-2017-17369	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-2017-17368	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-2017-17367	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-2017-17366	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-2017-17365	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-2017-17364	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-2017-17363	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-2017-17362	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-2017-17361	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-2017-17360	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-2017-17359	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-2017-17358	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-2017-17357	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-2017-17356	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-2017-17355	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-2017-17354	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-2017-17353	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-2017-17352	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-2017-17371	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-2017-17373	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-2017-17349	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-2017-17374	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-2018-16903	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-2018-16902	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-2018-16901	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-2018-16900	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-2018-16899	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-2018-16898	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-2018-16897	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-2018-16896	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-2018-16895	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-2018-16894	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-2018-16893	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-2018-16892	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-2018-16891	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-2017-17380	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-2017-17379	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-2017-17378	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-2017-17377	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-2017-17376	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-2017-17375	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-2017-17350	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-2017-17348	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-2017-15158	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-2017-15179	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-2017-15177	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-2017-15176	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-2017-15175	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-2017-15174	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-2017-15173	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-2017-15172	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-2017-15171	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-2017-15170	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-2017-15169	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-2017-15168	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-2017-15167	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-2017-15166	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-2017-15165	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-2017-15164	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-2017-15163	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-2017-15162	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-2017-15161	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-2017-15160	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-2017-15159	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-2017-15178	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-2017-15180	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-2017-17347	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-2017-15181	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-2017-17346	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-2017-17345	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-2017-17344	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-2017-17343	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-2017-17342	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-2017-17341	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-2017-17340	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-2017-17339	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-2017-17338	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-2017-17337	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-2017-17336	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-2017-17335	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-2017-17334	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-2017-17333	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-2017-17332	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-2017-17331	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-2017-15184	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-2017-15183	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-2017-15182	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-2017-17351	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details