SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 August 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-2020-5415	Concourse, versions prior to 6.3.1 and 6.4.1, in installations which use the GitLab auth connector, is vulnerable to identity spoofing by way of configuring a GitLab account with the same full name as another user who is granted access to a Concourse team. GitLab groups do not have this vulnerability, so GitLab users may be moved into groups which are then configured in the Concourse team.	10.0	More Details
CVE-2020-1467	An elevation of privilege vulnerability exists when Windows improperly handles hard links. An attacker who successfully exploited this vulnerability could overwrite a targeted file leading to an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows handles hard links.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6932	An information disclosure and remote code execution vulnerability in the slinger web server of the BlackBerry QNX Software Development Platform versions 6.4.0 to 6.6.0 could allow an attacker to potentially read arbitrary files and run arbitrary executables in the context of the web server.	9.8	More Details
CVE-2020-7706	The package connie-lang before 0.1.1 are vulnerable to Prototype Pollution in the configuration language library used by connie.	9.8	More Details
CVE-2020-7702	All versions of package templ8 are vulnerable to Prototype Pollution via the parse function.	9.8	More Details
CVE-2020-7703	All versions of package nis-utils are vulnerable to Prototype Pollution via the setValue function.	9.8	More Details
CVE-2020-8211	Improper input validation in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 allows SQL Injection.	9.8	More Details
CVE-2020-8212	Improper access control in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 allows access to privileged functionality.	9.8	More Details
CVE-2020-24208	A SQL injection vulnerability in SourceCodester Online Shopping Alphaware 1.0 allows remote unauthenticated attackers to bypass the authentication process via email and password parameters.	9.8	More Details
CVE-2020-7704	The package linux-cmdline before 1.0.1 are vulnerable to Prototype Pollution via the constructor.	9.8	More Details
CVE-2020-7707	The package property-expr before 2.0.3 are vulnerable to Prototype Pollution via the setter function.	9.8	More Details
CVE-2020-24361	SNMPTT before 1.4.2 allows attackers to execute shell code via EXEC, PREXEC, or unknown_trap_exec.	9.8	More Details
CVE-2020-7708	The package irrelon-path before 4.7.0; the package @irrelon/path before 4.7.0 are vulnerable to Prototype Pollution via the set, unSet, pushVal and pullVal functions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-6258	D-Link DIR-822 Rev.Bx devices with firmware v.202KRb06 and older allow a buffer overflow via long MacAddress data in a /HNAP1/SetClientInfo HNAP protocol message, which is mishandled in /usr/sbin/udhcpd during reading of the /var/servd/LAN-1-udhcpd.conf file.	9.8	More Details
CVE-2020-14934	Buffer overflows were discovered in Contiki-NG 4.4 through 4.5, in the SNMP agent. The function parsing the received SNMP request does not verify the input message's requested variables against the capacity of the internal SNMP engine buffer. If the number of variables in the request exceeds the allocated buffer, a memory write out of the buffer boundaries occurs. This write operation provides a possibility to overwrite other variables allocated in the .bss section by the application. Because the sender of the frame is in control of the content that will be written beyond the buffer limits, and there is no strict process memory separation, this issue may allow overwriting of sensitive memory areas of an IoT device.	9.8	More Details
CVE-2020-14935	Buffer overflows were discovered in Contiki-NG 4.4 through 4.5, in the SNMP bulk get request response encoding function. The function parsing the received SNMP request does not verify the input message's requested variables against the capacity of the internal SNMP engine buffer. When a bulk get request response is assembled, a stack buffer dedicated for OIDs (with a limited capacity) is allocated in snmp_engine_get_bulk(). When snmp_engine_get_bulk() is populating the stack buffer, an overflow condition may occur due to lack of input length validation. This makes it possible to overwrite stack regions beyond the allocated buffer, including the return address from the function. As a result, the code execution path may be redirected to an address provided in the SNMP bulk get payload. If the target architecture uses common addressing space for program and data memory, it may also be possible to supply code in the SNMP request payload, and redirect the execution path to the remotely injected code, by modifying the function's return address.	9.8	More Details
CVE-2020-14936	Buffer overflows were discovered in Contiki-NG 4.4 through 4.5, in the SNMP agent. Functions parsing the OIDs in SNMP requests lack sufficient allocated target-buffer capacity verification when writing parsed OID values. The function snmp_oid_decode_oid() may overwrite memory areas beyond the provided target buffer, when called from snmp_message_decode() upon an SNMP request reception. Because the content of the write operations is externally provided in the SNMP requests, it enables a remote overwrite of an IoT device's memory regions beyond the allocated buffer. This overflow may allow remote overwrite of stack and statically allocated variables memory regions by sending a crafted SNMP request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15865	A Remote Code Execution vulnerability in Stimulsoft (aka Stimulsoft Reports) 2013.1.1600.0 allows an attacker to encode C# scripts as base-64 in the report XML file so that they will be compiled and executed on the server that processes this file. This can be used to fully compromise the server.	9.8	More Details
CVE-2020-17496	vBulletin 5.5.4 through 5.6.2 allows remote command execution via crafted subWidgets data in an ajax/render/widget_tabbedcontainer_tab_panel request. NOTE: this issue exists because of an incomplete fix for CVE-2019-16759.	9.8	More Details
CVE-2020-12606	An issue was discovered in DB Soft SGLAC before 20.05.001. The ProcedimientoGenerico method in the SVCManejador.svc webservice of the SGLAC web frontend allows an attacker to run arbitrary SQL commands on the SQL Server. Command execution can be easily achieved by using the xp_cmdshell stored procedure.	9.8	More Details
CVE-2020-17474	A token-reuse vulnerability in ZKTeco FaceDepot 7B 1.0.213 and ZKBiosecurity Server 1.0.0_20190723 allows an attacker to create arbitrary new users, elevate users to administrators, delete users, and download user faces from the database.	9.8	More Details
CVE-2019-16374	Pega Platform 8.2.1 allows LDAP injection because a username can contain a * character and can be of unlimited length. An attacker can specify four characters of a username, followed by the * character, to bypass access control.	9.8	More Details
CVE-2020-17446	asyncpg before 0.21.0 allows a malicious PostgreSQL server to trigger a crash or execute arbitrary code (on a database client) via a crafted server response, because of access to an uninitialized pointer in the array data decoder.	9.8	More Details
CVE-2020-17506	Artica Web Proxy 4.30.00000000 allows remote attacker to bypass privilege detection and gain web backend administrator privileges through SQL injection of the apikey parameter in fw.login.php.	9.8	More Details
CVE-2020-12106	The Web portal of the WiFi module of VPNCrypt M10 2.6.5 allows unauthenticated users to send HTTP POST request to several critical Administrative functions such as, changing credentials of the Administrator account or connect the product to a rogue access point.	9.8	More Details
CVE-2020-12107	The Web portal of the WiFi module of VPNCrypt M10 2.6.5 allows command injection via a text field, which allow full control over this module's Operating System.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16137	A privilege escalation issue in Cisco Unified IP Conference Station 7937G 1-4-4-0 through 1-4-5-7 allows attackers to reset the credentials for the SSH administrative console to arbitrary values. Note: We cannot prove this vulnerability exists. Out of an abundance of caution, this CVE is being assigned to better serve our customers and ensure all who are still running this product understand that the product is end of life and should be removed or upgraded. For more information on this, and how to upgrade, refer to the CVE's reference information	9.8	More Details
CVE-2020-15692	In Nim 1.2.4, the standard library browsers mishandles the URL argument to browsers.openDefaultBrowser. This argument can be a local file path that will be opened in the default explorer. An attacker can pass one argument to the underlying open command to execute arbitrary registered system commands.	9.8	More Details
CVE-2020-4589	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 184585.	9.8	More Details
CVE-2020-17463	FUEL CMS 1.4.7 allows SQL Injection via the col parameter to /pages/items, /permissions/items, or /navigation/items.	9.8	More Details
CVE-2020-7700	All versions of phpjs are vulnerable to Prototype Pollution via parse_str.	9.8	More Details
CVE-2020-7701	madlib-object-utils before 0.1.7 is vulnerable to Prototype Pollution via setValue.	9.8	More Details
CVE-2020-10055	A vulnerability has been identified in Desigo CC (V4.x), Desigo CC (V3.x), Desigo CC Compact (V4.x), Desigo CC Compact (V3.x). Affected applications are delivered with a 3rd party component (BIRT) that contains a remote code execution vulnerability if the Advanced Reporting Engine is enabled. The vulnerability could allow a remote unauthenticated attacker to execute arbitrary commands on the server with SYSTEM privileges.	9.8	More Details
CVE-2020-24032	tz.pl on XoruX LPAR2RRD and STOR2RRD 2.70 virtual appliances allows cmd=set&tz=OS command injection via shell metacharacters in a timezone.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15781	A vulnerability has been identified in SICAM WEB firmware for SICAM A8000 RTUs (All versions < V05.30). The login screen does not sufficiently sanitize input, which enables an attacker to generate specially crafted log messages. If an unsuspecting victim views the log messages via the web browser, these log messages might be interpreted and executed as code by the web application. This Cross-Site-Scripting (XSS) vulnerability might compromize the confidentiality, integrity and availability of the web application.	9.6	More Details
CVE-2020-15152	ftp-srv is an npm package which is a modern and extensible FTP server designed to be simple yet configurable. In ftp-srv before versions 2.19.6, 3.1.2, and 4.3.4 are vulnerable to Server-Side Request Forgery. The PORT command allows arbitrary IPs which can be used to cause the server to make a connection elsewhere. A possible workaround is blocking the PORT through the configuration. This issue is fixed in version2 2.19.6, 3.1.2, and 4.3.4. More information can be found on the linked advisory.	9.1	More Details
CVE-2020-9233	FusionCompute 8.0.0 have an insufficient authentication vulnerability. An attacker may exploit the vulnerability to delete some files and cause some services abnormal.	9.1	More Details
CVE-2020-14937	Memory access out of buffer boundaries issues was discovered in Contiki-NG 4.4 through 4.5, in the SNMP BER encoder/decoder. The length of provided input/output buffers is insufficiently verified during the encoding and decoding of data. This may lead to out-of-bounds buffer read or write access in BER decoding and encoding functions.	9.1	More Details
CVE-2020-6294	Xvfb of SAP Business Objects Business Intelligence Platform, versions - 4.2, 4.3, platform on Unix does not perform any authentication checks for functionalities that require user identity.	9.1	More Details
CVE-2020-6284	SAP NetWeaver (Knowledge Management), versions - 7.30, 7.31, 7.40, 7.50, allows the automatic execution of script content in a stored file due to inadequate filtering with the accessing user's privileges. If the accessing user has administrative privileges, then the execution of the script content could result in complete compromise of system confidentiality, integrity and availability, leading to Stored Cross Site Scripting.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2020-8913	A local, arbitrary code execution vulnerability exists in the SplitCompat.install endpoint in Android's Play Core Library versions prior to 1.7.2. A malicious attacker could create an apk which targets a specific application, and if a victim were to install this apk, the attacker could perform a directory traversal, execute code as the targeted application and access the targeted application's data on the Android device. We recommend all users update Play Core to version 1.7.2 or later.	8.8	More Details
CVE-2020-6296	SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 753, 755, allows an attacker to inject code that can be executed by the application, leading to Code Injection. An attacker could thereby control the behavior of the application.	8.8	More Details
CVE-2020-1495	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1496	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1498	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	8.8	More Details
CVE-2020-8732	Heap-based buffer overflow in the firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-8731	Incorrect execution-assigned permissions in the file system for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2020-8730	Heap-based overflow for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1504	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	8.8	More Details
CVE-2020-8718	Buffer overflow in a subsystem for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2020-9242	FusionCompute 8.0.0 have a command injection vulnerability. The software does not sufficiently validate certain parameters post from user, successful exploit could allow an authenticated attacker to launch a command injection attack.	8.8	More Details
CVE-2020-8713	Improper authentication for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-8709	Improper authentication in socket services for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.45 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-17505	Artica Web Proxy 4.30.000000 allows an authenticated remote attacker to inject commands via the service-cmds parameter in cyrus.php. These commands are executed with root privileges via service_cmds_peform.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1561	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory.	8.8	More Details
CVE-2020-8708	Improper authentication for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-8707	Buffer overflow in daemon for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-1555	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1494	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	8.8	More Details
CVE-2020-8706	Buffer overflow in a daemon for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-8233	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges.	8.8	More Details
CVE-2020-23934	An issue was discovered in RiteCMS 2.2.1. An authenticated user can directly execute system commands by uploading a php web shell in the "Filemanager" section.	8.8	More Details
CVE-2020-15925	A SQL injection vulnerability at a tpf URI in Loway QueueMetrics before 19.10.21 allows remote authenticated attackers to execute arbitrary SQL commands via the TPF_XPAR1 parameter.	8.8	More Details
CVE-2020-15947	A SQL injection vulnerability in the qm_adm/qm_export_stats_run.do endpoint of Loway QueueMetrics before 19.10.21 allows remote authenticated users to execute arbitrary SQL commands via the exportId parameter.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4662	IBM Event Streams 10.0.0 could allow an authenticated user to perform tasks to a schema due to improper authentication validation. IBM X-Force ID: 186233.	8.8	More Details
CVE-2020-1583	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the user's computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Word functions handle objects in memory.	8.8	More Details
CVE-2020-7018	Elastic Enterprise Search before 7.9.0 contain a credential exposure flaw in the App Search interface. If a user is given the ï¿½developerï¿½ role, they will be able to view the administrator API credentials. These credentials could allow the developer user to conduct operations with the same permissions of the App Search administrator.	8.8	More Details
CVE-2020-13941	Reported in SOLR-14515 (private) and fixed in SOLR-14561 (public), released in Solr version 8.6.0. The Replication handler (https://lucene.apache.org/solr/guide/8_6/index-replication.html#http-api-commands-for-the-replicationhandler) allows commands backup, restore and deleteBackup. Each of these take a location parameter, which was not validated, i.e you could read/write to any location the solr user can access.	8.8	More Details
CVE-2020-13122	The novish command-line interface, included in NoviFlow NoviWare before NW500.2.12 and deployed on NoviSwitch devices, is vulnerable to command injection in the "show status destination ipaddr" command. This could be used by a read-only user (monitoring group) or admin to execute commands on the operating system.	8.8	More Details
CVE-2020-24220	ShopXO v1.8.1 has a command execution vulnerability. Attackers can use this vulnerability to execute arbitrary commands and gain control of the server.	8.8	More Details
CVE-2020-1585	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16087	An issue was discovered in Zalo.exe in VNG Zalo Desktop 19.8.1.0. An attacker can run arbitrary commands on a remote Windows machine running the Zalo client by sending the user of the device a crafted file.	8.6	More Details
CVE-2020-3363	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	8.6	More Details
CVE-2020-12299	Improper input validation in BIOS firmware for Intel(R) Server Board Families S2600ST, S2600BP and S2600WF may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2020-12300	Uninitialized pointer in BIOS firmware for Intel(R) Server Board Families S2600CW, S2600KP, S2600TP, and S2600WT may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2020-8721	Improper input validation for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2020-8722	Buffer overflow in a subsystem for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2020-12301	Improper initialization in BIOS firmware for Intel(R) Server Board Families S2600ST, S2600BP and S2600WF may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2020-8719	Buffer overflow in subsystem for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2020-4686	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13291	In GitLab before 13.2.3, project sharing could temporarily allow too permissive access.	8.1	More Details
CVE-2020-6301	SAP ERP (HCM Travel Management), versions - 600, 602, 603, 604, 605, 606, 607, 608, allows an authenticated but unauthorized attacker to read, modify and settle trips, resulting in escalation of privileges, due to Missing Authorization Check.	8.1	More Details
CVE-2020-17497	eapol.c in iNet wireless daemon (IWD) through 1.8 allows attackers to trigger a PTK reinstallation by retransmitting EAPOL Msg4/4.	8.1	More Details
CVE-2020-6298	SAP Banking Services (Generic Market Data), versions - 400, 450, 500, allows an unauthorized user to display protected Business Partner Generic Market Data (GMD) and change related GMD key figure values, due to Missing Authorization Check.	8.1	More Details
CVE-2020-15142	In openapi-python-client before version 0.5.3, clients generated with a maliciously crafted OpenAPI Document can generate arbitrary Python code. Subsequent execution of this malicious client is arbitrary code execution.	8.0	More Details
CVE-2020-1552	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Work Folder Service handles file operations.	8.0	More Details
CVE-2020-1475	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the srmsvc.dll properly handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1478	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	7.8	More Details
CVE-2020-1479	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how DirectX handles objects in memory.	7.8	More Details
CVE-2020-6295	Under certain conditions the SAP Adaptive Server Enterprise, version 16.0, allows an attacker to access encrypted sensitive and confidential information through publicly readable installation log files leading to a compromise of the installed Cockpit. This compromise could enable the attacker to view, modify and/or make unavailable any data associated with the Cockpit, leading to Information Disclosure.	7.8	More Details
CVE-2020-1474	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, an authenticated attacker could connect an imaging device (camera, scanner, cellular phone) to an affected system and run a specially crafted application to disclose information. The security update addresses the vulnerability by correcting how the WIA Service handles objects in memory.	7.8	More Details
CVE-2020-8687	Uncontrolled search path in the installer for Intel(R) RSTe Software RAID Driver for the Intel(R) Server Board M10JNP2SB before version 4.7.0.1119 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1480	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation.	7.8	More Details
CVE-2020-1484	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Work Folders Service handles memory.	7.8	More Details
CVE-2020-1486	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	7.8	More Details
CVE-2020-1487	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log onto an affected system and open a specially crafted file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The update addresses the vulnerability by correcting how Media Foundation handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8681	Out of bounds write in system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1489	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows CSC Service handles memory.	7.8	More Details
CVE-2020-0513	Out of bounds write for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-0559	Insecure inherited permissions in some Intel(R) PROSet/Wireless WiFi products on Windows* 7 and 8.1 before version 21.40.5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-0555	Improper input validation for some Intel(R) Wireless Bluetooth(R) products may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1470	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Work Folders Service handles memory.	7.8	More Details
CVE-2020-1492	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	7.8	More Details
CVE-2020-0510	Out of bounds read in some Intel(R) Graphics Drivers before versions 15.45.31.5127 and 15.40.45.5126 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1569	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.	7.8	More Details
CVE-2020-8763	Improper permissions in the installer for the Intel(R) RealSense(TM) D400 Series UWP driver for Windows* 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-8743	Improper permissions in the installer for the Intel(R) Mailbox Interface driver, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-8736	Improper access control in subsystem for the Intel(R) Computing Improvement Program before version 2.4.5718 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1564	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8729	Buffer copy without checking size of input for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1577	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory.	7.8	More Details
CVE-2020-1556	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows WalletService properly handles objects in memory.	7.8	More Details
CVE-2020-1563	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory.	7.8	More Details
CVE-2020-1579	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Function Discovery SSDP Provider handles memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1587	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Ancillary Function Driver for WinSock handles memory.	7.8	More Details
CVE-2020-1584	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the dnsrslvr.dll properly handles objects in memory.	7.8	More Details
CVE-2020-9767	A vulnerability related to Dynamic-link Library (“DLL”) loading in the Zoom Sharing Service would allow an attacker who had local access to a machine on which the service was running with elevated privileges to elevate their system privileges as well through use of a malicious DLL. Zoom addressed this issue, which only applies to Windows users, in the 5.0.4 client release.	7.8	More Details
CVE-2020-7583	A vulnerability has been identified in Automation License Manager 5 (All versions), Automation License Manager 6 (All versions < V6.0.8). The application does not properly validate the users' privileges when executing some operations, which could allow a user with low permissions to arbitrary modify files that should be protected against writing.	7.8	More Details
CVE-2020-22722	Rapid Software LLC Rapid SCADA 5.8.0 is affected by a local privilege escalation vulnerability in the ScadaAgentSvc.exe executable file. An attacker can obtain admin privileges by placing a malicious .exe file in the application and renaming it ScadaAgentSvc.exe, which would result in executing the binary as NT AUTHORITY\SYSTEM in a Windows operating system. For example, an attacker can plant a reverse shell from a low privileged user account and by restarting the computer, the malicious service will be started as NT AUTHORITY\SYSTEM by giving the attacker full system access to the remote PC.	7.8	More Details
CVE-2020-22721	A File Upload Vulnerability in PNotes - Andrey Gruber PNotes.NET v3.8.1.2 allows a local attacker to execute arbitrary code via the Miscellaneous " External Programs by uploading the malicious .exe file to the external program.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3433	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.	7.8	More Details
CVE-2020-0604	A remote code execution vulnerability exists in Visual Studio Code when it process environment variables after opening a project. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to clone a repository and open it in Visual Studio Code. Attacker-specified code would execute when the target opened the integrated terminal. The update address the vulnerability by modifying the way Visual Studio Code handles environment variables.	7.8	More Details
CVE-2020-17462	CMS Made Simple 2.2.14 allows Authenticated Arbitrary File Upload because the File Manager does not block .ptar files, a related issue to CVE-2017-16798.	7.8	More Details
CVE-2020-1046	A remote code execution vulnerability exists when Microsoft .NET Framework processes input. An attacker who successfully exploited this vulnerability could take control of an affected system. To exploit the vulnerability, an attacker would need to be able to upload a specially crafted file to a web application. The security update addresses the vulnerability by correcting how .NET Framework processes input.	7.8	More Details
CVE-2020-1337	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows Print Spooler Component writes to the file system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1582	A remote code execution vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Access. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. The security update addresses the vulnerability by correcting how Microsoft Access handles objects in memory.	7.8	More Details
CVE-2019-20383	ABBYY network license server in ABBYY FineReader 15 before Release 4 (aka 15.0.112.2130) allows escalation of privileges by local users via manipulations involving files and using symbolic links.	7.8	More Details
CVE-2020-1339	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects. An attacker who successfully exploited the vulnerability could take control of an affected system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Audio Codec handles objects.	7.8	More Details
CVE-2020-1377	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. A locally authenticated attacker could exploit this vulnerability by running a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly handles objects in memory.	7.8	More Details
CVE-2020-24346	njs through 0.4.3, used in NGINX, has a use-after-free in njs_json_parse_iterator_call in njs_json.c.	7.8	More Details
CVE-2020-24345	JerryScript through 2.3.0 allows stack consumption via function a(){new new Proxy(a,{})}JSON.parse("[]",a). NOTE: the vendor states that the problem is the lack of the --stack-limit option	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24343	Artifex MuJS through 1.0.7 has a use-after-free in jsrun.c because of unconditional marking in jsgc.c.	7.8	More Details
CVE-2020-24342	Lua through 5.4.0 allows a stack redzone cross in luaO_pushvfstring because a protection mechanism wrongly calls luaD_callnoyield twice in a row.	7.8	More Details
CVE-2020-1380	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	7.8	More Details
CVE-2020-24331	An issue was discovered in TrouSerS through 0.3.14. If the tcsd daemon is started with root privileges, the tss user still has read and write access to the /etc/tcsd.conf file (which contains various settings related to this daemon).	7.8	More Details
CVE-2020-24330	An issue was discovered in TrouSerS through 0.3.14. If the tcsd daemon is started with root privileges instead of by the tss user, it fails to drop the root gid privilege when no longer needed.	7.8	More Details
CVE-2020-0261	In C2 flame devices, there is a possible bypass of seccomp due to a missing configuration file. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146059841	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1464	A spoofing vulnerability exists when Windows incorrectly validates file signatures. An attacker who successfully exploited this vulnerability could bypass security features and load improperly signed files. In an attack scenario, an attacker could bypass security features intended to prevent improperly signed files from being loaded. The update addresses the vulnerability by correcting how Windows validates file signatures.	7.8	More Details
CVE-2020-1581	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) components handle objects in memory. An attacker who successfully exploited the vulnerability could elevate privileges. The attacker would need to already have the ability to execute code on the system. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The security update addresses the vulnerability by correcting how Microsoft Office Click-to-Run (C2R) components handle objects in memory.	7.8	More Details
CVE-2020-1466	A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RD Gateway service on the target system to stop responding. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides RD Gateway services. The update addresses the vulnerability by correcting how RD Gateway handles connection requests.	7.8	More Details
CVE-2020-1490	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges on the victim system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application. The security update addresses the vulnerability by correcting how the Storage Services handles file operations.	7.8	More Details
CVE-2020-1534	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1540	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1526	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Network Connection Broker handles memory.	7.8	More Details
CVE-2020-1527	An elevation of privilege vulnerability exists when the Windows Custom Protocol Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Custom Protocol Engine handles memory.	7.8	More Details
CVE-2020-1528	An elevation of privilege vulnerability exists when the Windows Radio Manager API improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Radio Manager API handles memory.	7.8	More Details
CVE-2020-16303	A use-after-free vulnerability in xps_finish_image_path() in devices/vector/gdevxps.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted PDF file. This is fixed in v9.51.	7.8	More Details
CVE-2020-1529	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1530	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how Windows Remote Access handles memory.	7.8	More Details
CVE-2020-1531	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Accounts Control handles memory.	7.8	More Details
CVE-2020-1533	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows WalletService properly handles objects in memory.	7.8	More Details
CVE-2020-1535	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1536	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1537	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Remote Access properly handles file operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1538	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows UPnP Device Host handles memory.	7.8	More Details
CVE-2020-1539	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1541	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1524	An elevation of privilege vulnerability exists when the Windows Speech Shell Components improperly handle memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Speech Shell Components handle memory.	7.8	More Details
CVE-2020-1542	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1543	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1544	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1545	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-12287	Incorrect permissions in the Intel(R) Distribution of OpenVINO(TM) Toolkit before version 2020.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1546	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1547	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1548	An information disclosure vulnerability exists when the Windows WaasMedic Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to improperly disclose memory. The security update addresses the vulnerability by correcting how the Windows WaasMedic Service handles memory.	7.8	More Details
CVE-2020-1549	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows CDP User Components handle memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1550	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows CDP User Components handle memory.	7.8	More Details
CVE-2020-1551	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Engine handles memory.	7.8	More Details
CVE-2020-1553	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory.	7.8	More Details
CVE-2020-1554	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	7.8	More Details
CVE-2020-1525	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1509	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request. A remote attacker who successfully exploited this vulnerability could cause an elevation of privilege on the target system's LSASS service. The security update addresses the vulnerability by changing the way that LSASS handles specially crafted authentication requests.	7.8	More Details
CVE-2020-8712	Buffer overflow in a verification process for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.45 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1517	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows File Server Resource Management Service handles memory.	7.8	More Details
CVE-2020-1511	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The security update addresses the vulnerability by correcting how the Connected User Experiences and Telemetry Service handles file operations.	7.8	More Details
CVE-2020-8714	Improper authentication for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1522	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Speech Runtime handles memory.	7.8	More Details
CVE-2020-1513	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows CSC Service handles memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1515	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Telephony Server handles memory.	7.8	More Details
CVE-2020-1562	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory.	7.8	More Details
CVE-2020-1560	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.	7.8	More Details
CVE-2020-17360	An issue was discovered in ReadyTalk Avian 1.2.0. The vm::arrayCopy method defined in classpath-common.h contains multiple boundary checks that are performed to prevent out-of-bounds memory read/write. However, two of these boundary checks contain an integer overflow that leads to a bypass of these checks, and out-of-bounds read/write. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.8	More Details
CVE-2020-1558	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1516	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Work Folders Service handles memory.	7.8	More Details
CVE-2020-1512	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory.	7.8	More Details
CVE-2020-1521	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Speech Runtime handles memory.	7.8	More Details
CVE-2020-1520	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory. An attacker who successfully exploited the vulnerability would gain execution on a victim system. The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory.	7.8	More Details
CVE-2020-1518	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows File Server Resource Management Service handles memory.	7.8	More Details
CVE-2020-1519	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows UPnP Device Host handles memory.	7.8	More Details
CVE-2020-7304	Cross site request forgery vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote attacker to embed a CRSF script via adding a new label.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8209	Improper access control in Citrix XenMobile Server 10.12 before RP2, Citrix XenMobile Server 10.11 before RP4, Citrix XenMobile Server 10.10 before RP6 and Citrix XenMobile Server before 10.9 RP5 and leads to the ability to read arbitrary files.	7.5	More Details
CVE-2020-13933	Apache Shiro before 1.6.0, when using Apache Shiro, a specially crafted HTTP request may cause an authentication bypass.	7.5	More Details
CVE-2020-1565	An elevation of privilege vulnerability exists when the "Public Account Pictures" folder improperly handles junctions. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how Windows handles junctions.	7.5	More Details
CVE-2020-12674	In Dovecot before 2.3.11.3, sending a specially formatted RPA request will crash the auth service because a length of zero is mishandled.	7.5	More Details
CVE-2020-1597	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the ASP.NET Core application. The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests.	7.5	More Details
CVE-2020-17475	Lack of authentication in the network relays used in MEGVII Koala 2.9.1-c3s allows attackers to grant physical access to anyone by sending packet data to UDP port 5000.	7.5	More Details
CVE-2020-15868	Sonatype Nexus Repository Manager OSS/Pro before 3.26.0 has Incorrect Access Control.	7.5	More Details
CVE-2020-12673	In Dovecot before 2.3.11.3, sending a specially formatted NTLM request will crash the auth service because of an out-of-bounds read.	7.5	More Details
CVE-2020-8210	Insufficient protection of secrets in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 discloses credentials of a service account.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6309	SAP NetWeaver AS JAVA, versions - (ENGINEAPI 7.10; WSRM 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; J2EE-FRMW 7.10, 7.11), does not perform any authentication checks for a web service allowing the attacker to send several payloads and leading to complete denial of service.	7.5	More Details
CVE-2020-2232	Jenkins Email Extension Plugin 2.72 and 2.73 transmits and displays the SMTP password in plain text as part of the global Jenkins configuration form, potentially resulting in its exposure.	7.5	More Details
CVE-2020-24372	LuaJIT through 2.1.0-beta3 has an out-of-bounds read in lj_err_run in lj_err.c.	7.5	More Details
CVE-2020-1568	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that contains malicious PDF content. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted PDF content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Microsoft Edge PDF Reader handles objects in memory.	7.5	More Details
CVE-2020-16139	A denial-of-service in Cisco Unified IP Conference Station 7937G 1-4-4-0 through 1-4-5-7 allows attackers restart the device remotely through sending specially crafted packets. Note: We cannot prove this vulnerability exists. Out of an abundance of caution, this CVE is being assigned to better serve our customers and ensure all who are still running this product understand that the product is end of life and should be removed or upgraded. For more information on this, and how to upgrade, refer to the CVE’s reference information	7.5	More Details
CVE-2020-24369	ldebug.c in Lua 5.4.0 attempts to access debug information via the line hook of a stripped function, leading to a NULL pointer dereference.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16138	A denial-of-service issue in Cisco Unified IP Conference Station 7937G 1-4-4-0 through 1-4-5-7 allows attackers to remotely disable the device until it is power cycled. Note: We cannot prove this vulnerability exists. Out of an abundance of caution, this CVE is being assigned to better serve our customers and ensure all who are still running this product understand that the product is end of life and should be removed or upgraded. For more information on this, and how to upgrade, refer to the CVE's reference information	7.5	More Details
CVE-2020-15694	In Nim 1.2.4, the standard library httpClient fails to properly validate the server response. For example, httpClient.get().contentLength() does not raise any error if a malicious server provides a negative Content-Length.	7.5	More Details
CVE-2020-3411	A vulnerability in Cisco DNA Center software could allow an unauthenticated remote attacker access to sensitive information on an affected system. The vulnerability is due to improper handling of authentication tokens by the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker access to sensitive device information, which includes configuration files.	7.5	More Details
CVE-2020-8688	Improper input validation in the Intel(R) RAID Web Console 3 for Windows* may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2020-9228	FusionCompute 8.0.0 has an information disclosure vulnerability. Due to the properly protection of certain information, attackers may exploit this vulnerability to obtain certain information.	7.5	More Details
CVE-2020-1378	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. A locally authenticated attacker could exploit this vulnerability by running a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly handles objects in memory.	7.5	More Details
CVE-2020-12100	In Dovecot before 2.3.11.3, uncontrolled recursion in submission, lmtp, and lda allows remote attackers to cause a denial of service (resource consumption) via a crafted e-mail message with deeply nested MIME parts.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1459	An information disclosure vulnerability exists on ARM implementations that use speculative execution in control flow via a side-channel analysis, aka "straight-line speculation." To exploit this vulnerability, an attacker with local privileges would need to run a specially crafted application. The security update addresses the vulnerability by bypassing the speculative execution.	7.5	More Details
CVE-2020-1570	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	7.5	More Details
CVE-2020-13290	In GitLab before 13.0.12, 13.1.6, and 13.2.3, improper access control was used on the Applications page	7.5	More Details
CVE-2019-19643	ise smart connect KNX Vaillant 1.2.839 contain a Denial of Service.	7.5	More Details
CVE-2020-7360	An Uncontrolled Search Path Element (CWE-427) vulnerability in SmartControl version 4.3.15 and versions released before April 15, 2020 may allow an authenticated user to escalate privileges by placing a specially crafted DLL file in the search path. This issue was fixed in version 1.0.7, which was released after April 15, 2020. (Note, the version numbering system changed significantly between version 4.3.15 and version 1.0.7.)	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1182	A remote code execution vulnerability exists in Microsoft Dynamics 365 for Finance and Operations (on-premises) version 10.0.11. An attacker who successfully exploited this vulnerability could gain remote code execution via server-side script execution on the victim server. An authenticated attacker with privileges to import and export data could exploit this vulnerability by sending a specially crafted file to a vulnerable Dynamics server. The security update addresses the vulnerability by correcting how Microsoft Dynamics 365 for Finance and Operations (on-premises) version 10.0.11 handles user input.	7.3	More Details
CVE-2020-1557	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.3	More Details
CVE-2020-13285	For GitLab before 13.0.12, 13.1.6, 13.2.3 a cross-site scripting (XSS) vulnerability exists in the issue reference number tooltip.	7.3	More Details
CVE-2020-13283	For GitLab before 13.0.12, 13.1.6, 13.2.3 a cross-site scripting vulnerability exists in the issues list via milestone title.	7.3	More Details
CVE-2020-1571	An elevation of privilege vulnerability exists in Windows Setup in the way it handles permissions. A locally authenticated attacker could run arbitrary code with elevated system privileges. After successfully exploiting the vulnerability, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by ensuring Windows Setup properly handles permissions.	7.3	More Details
CVE-2020-16205	Using a specially crafted URL command, a remote authenticated user can execute commands as root on the G-Cam and G-Code (Firmware Versions 1.12.0.25 and prior as well as the limited Versions 1.12.13.2 and 1.12.14.5).	7.2	More Details
CVE-2020-24344	JerryScript through 2.3.0 has a (function({a=arguments}){const arguments}) buffer over-read.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0554	Race condition in software installer for some Intel(R) Wireless Bluetooth(R) products on Windows* 7, 8.1 and 10 may allow an unprivileged user to potentially enable escalation of privilege via local access.	7.0	More Details
CVE-2020-9241	Huawei 5G Mobile WiFi E6878-370 with versions of 10.0.3.1(H563SP1C00),10.0.3.1(H563SP21C233) have an improper authorization vulnerability. The device does not restrict certain data received from WAN port. Successful exploit could allow an attacker at WAN side to manage certain service of the device.	7.0	More Details
CVE-2020-1488	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files. To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges.	7.0	More Details
CVE-2020-8680	Race condition in some Intel(R) Graphics Drivers before version 15.40.45.5126 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.0	More Details
CVE-2020-1473	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.0	More Details
CVE-2020-1477	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3500	A vulnerability in the IPv6 implementation of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to an affected device with the goal of reaching the vulnerable section of the input buffer. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	6.8	More Details
CVE-2020-9237	Huawei smartphone Taurus-AL00B with versions earlier than 10.1.0.126(C00E125R5P3) have a user after free vulnerability. A module is lack of lock protection. Attackers can exploit this vulnerability by launching specific request. This could compromise normal service of the affected device.	6.7	More Details
CVE-2020-5385	Dell Encryption versions prior to 10.8 and Dell Endpoint Security Suite versions prior to 2.8 contain a privilege escalation vulnerability because of an incomplete fix for CVE-2020-5358. A local malicious user with low privileges could potentially exploit this vulnerability to gain elevated privilege on the affected system with the help of a symbolic link.	6.7	More Details
CVE-2020-8759	Improper access control in the installer for Intel(R) SSD DCT versions before 3.0.23 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-7305	Privilege escalation vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows a low privileged remote attacker to create new rule sets via incorrect validation of user credentials.	6.7	More Details
CVE-2020-8710	Buffer overflow in the bootloader for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.45 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8711	Improper access control in the bootloader for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.45 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8733	Improper buffer restrictions in the firmware for Intel(R) Server Board M10JNP2SB before version 7.210 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15596	The ALPS ALPINE touchpad driver before 8.2206.1717.634, as used on various Dell, HP, and Lenovo laptops, allows attackers to conduct Path Disclosure attacks via a "fake" DLL file.	6.7	More Details
CVE-2020-15145	In Composer-Setup for Windows before version 6.0.0, if the developer's computer is shared with other users, a local attacker may be able to exploit the following scenarios. 1. A local regular user may modify the existing `C:\ProgramData\ComposerSetup\bin\composer.bat` in order to get elevated command execution when composer is run by an administrator. 2. A local regular user may create a specially crafted dll in the `C:\ProgramData\ComposerSetup\bin` folder in order to get Local System privileges. See: https://itm4n.github.io/windows-server-netman-dll-hijacking. 3. If the directory of the php.exe selected by the user is not in the system path, it is added without checking that it is admin secured, as per Microsoft guidelines. See: https://msrc-blog.microsoft.com/2018/04/04/triaging-a-dll-planting-vulnerability.	6.7	More Details
CVE-2020-8684	Improper access control in firmware for Intel(R) PAC with Arria(R) 10 GX FPGA before Intel Acceleration Stack version 1.2.1 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-11733	An issue was discovered on Spirent TestCenter and Avalanche appliance admin interface firmware. An attacker, who already has access to an SSH restricted shell, can achieve root access via shell metacharacters. The attacker can then, for example, read sensitive files such as appliance admin configuration source code. This affects Spirent TestCenter and Avalanche products which chassis version <= 5.08. The SSH restricted shell is available with default credentials.	6.7	More Details
CVE-2020-8742	Improper input validation in the firmware for Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2019-14620	Insufficient control flow management for some Intel(R) Wireless Bluetooth(R) products may allow an unprivileged user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-2235	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline Maven Integration Plugin 3.8.2 and earlier allows attackers to connect to an attacker-specified JDBC URL using attacker-specified credentials IDs obtained through another method, potentially capturing credentials stored in Jenkins.	6.5	More Details
CVE-2020-17498	In Wireshark 3.2.0 to 3.2.5, the Kafka protocol dissector could crash. This was addressed in epan/dissectors/packet-kafka.c by avoiding a double free during LZ4 decompression.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13281	For GitLab before 13.0.12, 13.1.6, 13.2.3 a denial of service exists in the project import feature	6.5	More Details
CVE-2020-6293	SAP NetWeaver (Knowledge Management), versions - 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to upload a malicious file and also to access, modify or make unavailable existing files but the impact is limited to the files themselves and is restricted by other policies such as access control lists and other upload file size restrictions, leading to Unrestricted File Upload.	6.5	More Details
CVE-2016-11085	php/qmn_options_questions_tab.php in the quiz-master-next plugin before 4.7.9 for WordPress allows CSRF, with resultant stored XSS, via the question_name parameter because js/admin_question.js mishandles parsing inside of a SCRIPT element.	6.5	More Details
CVE-2020-8689	Improper buffer restrictions in the Intel(R) Wireless for Open Source before version 1.5 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2019-5591	A Default Configuration vulnerability in FortiOS may allow an unauthenticated attacker on the same subnet to intercept sensitive information by impersonating the LDAP server.	6.5	More Details
CVE-2020-13280	For GitLab before 13.0.12, 13.1.6, 13.2.3 a memory exhaustion flaw exists due to excessive logging of an invite email error message.	6.5	More Details
CVE-2020-2234	A missing permission check in Jenkins Pipeline Maven Integration Plugin 3.8.2 and earlier allows users with Overall/Read access to connect to an attacker-specified JDBC URL using attacker-specified credentials IDs obtained through another method, potentially capturing credentials stored in Jenkins.	6.5	More Details
CVE-2020-2233	A missing permission check in Jenkins Pipeline Maven Integration Plugin 3.8.2 and earlier allows users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	6.5	More Details
CVE-2020-7019	In Elasticsearch before 7.9.0 and 6.8.12 a field disclosure flaw was found when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden. This could result in an attacker gaining additional permissions against a restricted index.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12480	In Play Framework 2.6.0 through 2.8.1, the CSRF filter can be bypassed by making CORS simple requests with content types that contain parameters that can't be parsed.	6.5	More Details
CVE-2020-8232	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages.	6.5	More Details
CVE-2020-15693	In Nim 1.2.4, the standard library httpClient is vulnerable to a CR-LF injection in the target URL. An injection is possible if the attacker controls any part of the URL provided in a call (such as httpClient.get or httpClient.post), the User-Agent header value, or custom HTTP header names or values.	6.5	More Details
CVE-2020-13286	For GitLab before 13.0.12, 13.1.6, 13.2.3 user controlled git configuration settings can be modified to result in Server Side Request Forgery.	6.4	More Details
CVE-2020-8904	An arbitrary memory overwrite vulnerability in the trusted memory of Asylo exists in versions prior to 0.6.0. As the ecall_restore function fails to validate the range of the output_len pointer, an attacker can manipulate the tmp_output_len value and write to an arbitrary location in the trusted (enclave) memory. We recommend updating Asylo to version 0.6.0 or later.	6.4	More Details
CVE-2020-8723	Cross-site scripting for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	6.3	More Details
CVE-2020-14333	A flaw was found in Ovirt Engine's web interface in ovirt 4.4 and earlier, where it did not filter user-controllable parameters completely, resulting in a reflected cross-site scripting attack. This flaw allows an attacker to leverage a phishing attack, steal an unsuspecting user's cookies or other confidential information, or impersonate them within the application's context.	6.3	More Details
CVE-2020-17362	search.php in the Nova Lite theme before 1.3.9 for WordPress allows Reflected XSS.	6.1	More Details
CVE-2019-7410	There is stored cross site scripting (XSS) in Galileo CMS v0.042. Remote authenticated users could inject arbitrary web script or HTML via $page_title in /lib/Galileo/files/templates/page/show.html.ep (aka the PAGE TITLE Field).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15926	Rocket.Chat through 3.4.2 allows XSS where an attacker can send a specially crafted message to a channel or in a direct message to the client which results in remote code execution on the client side.	6.1	More Details
CVE-2020-3463	A vulnerability in the web-based management interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected service. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected service. An attacker could exploit this vulnerability by persuading a user to click a malicious 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-2020-3346	A vulnerability in the web UI of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) 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 UI does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2020-8208	Improper input validation in Citrix XenMobile Server 10.12 before RP1, Citrix XenMobile Server 10.11 before RP4, Citrix XenMobile Server 10.11 before RP6 and Citrix XenMobile Server before 10.9 RP5 allows Cross-Site Scripting (XSS).	6.1	More Details
CVE-2020-17450	PHP-Fusion 9.03 allows XSS on the preview page.	6.1	More Details
CVE-2020-13183	Reflected Cross Site Scripting in Teradici PCoIP Management Console prior to 20.07 could allow an attacker to take over the user's active session if the user is exposed to a malicious payload.	6.1	More Details
CVE-2020-13278	Reflected Cross-Site Scripting vulnerability in Modules.php in RosarioSIS Student Information System < 6.5.1 allows remote attackers to execute arbitrary web script via embedding javascript or HTML tags in a GET request.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-6112	A Cross-site scripting (XSS) vulnerability in /inc/class-search.php in the Sell Media plugin v2.4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the keyword parameter (aka $search_term or the Search field).	6.1	More Details
CVE-2020-16145	Roundcube Webmail before 1.3.15 and 1.4.8 allows stored XSS in HTML messages during message display via a crafted SVG document. This issue has been fixed in 1.4.8 and 1.3.15.	6.1	More Details
CVE-2020-12648	A cross-site scripting (XSS) vulnerability in TinyMCE 5.2.1 and earlier allows remote attackers to inject arbitrary web script when configured in classic editing mode.	6.1	More Details
CVE-2020-9708	The resolveRepositoryPath function doesn't properly validate user input and a malicious user may traverse to any valid Git repository outside the repoRoot. This issue may lead to unauthorized access of private Git repositories as long as the malicious user knows or brute-forces the location of the repository.	5.9	More Details
CVE-2020-17473	Lack of mutual authentication in ZKTeco FaceDepot 7B 1.0.213 and ZKBiosecurity Server 1.0.0_20190723 allows an attacker to obtain a long-lasting token by impersonating the server.	5.9	More Details
CVE-2020-3448	A vulnerability in an access control mechanism of Cisco Cyber Vision Center Software could allow an unauthenticated, remote attacker to bypass authentication and access internal services that are running on an affected device. The vulnerability is due to insufficient enforcement of access control in the software. An attacker could exploit this vulnerability by directly accessing the internal services of an affected device. A successful exploit could allow an attacker to impact monitoring of sensors that are managed by the software.	5.8	More Details
CVE-2020-8226	A vulnerability exists in phpBB <v3.2.10 and <v3.3.1 which allowed remote image dimensions check to be used to SSRF.	5.8	More Details
CVE-2020-3447	A vulnerability in the CLI of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to excessive verbosity in certain log subscriptions. An attacker could exploit this vulnerability by accessing specific log files on an affected device. A successful exploit could allow the attacker to obtain sensitive log data, which may include user credentials. To exploit this vulnerability, the attacker would need to have valid credentials at the operator level or higher on the affected device.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3435	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to overwrite VPN profiles on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of user-supplied input. 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 modify VPN profile files. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.	5.5	More Details
CVE-2020-24347	njs through 0.4.3, used in NGINX, has an out-of-bounds read in njs_lvlhsh_level_find in njs_lvlhsh.c.	5.5	More Details
CVE-2020-3434	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of user-supplied input. 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 stop the AnyConnect process, causing a DoS condition on the device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.	5.5	More Details
CVE-2020-16299	A Division by Zero vulnerability in bj10v_print_page() in contrib/japanese/gdev10v.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16301	A buffer overflow vulnerability in okiibm_print_page1() in devices/gdevokii.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-24349	njs through 0.4.3, used in NGINX, allows control-flow hijack in njs_value_property in njs_value.c. NOTE: the vendor considers the issue to be "fluff" in the NGINX use case because there is no remote attack surface.	5.5	More Details
CVE-2020-24348	njs through 0.4.3, used in NGINX, has an out-of-bounds read in njs_json_stringify_iterator in njs_json.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16302	A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-1379	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	5.5	More Details
CVE-2020-0512	Uncaught exception in the system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-8715	Invalid pointer for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an unauthenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-8716	Improper access control for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-1510	An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how win32k handles objects in memory.	5.5	More Details
CVE-2020-8717	Improper input validation in a subsystem for some Intel Server Boards, Server Systems and Compute Modules before version 1.59 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-1505	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles objects in memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1503	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the user's computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Word functions handle objects in memory.	5.5	More Details
CVE-2020-1502	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the user's computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Word functions handle objects in memory.	5.5	More Details
CVE-2020-1497	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the user's computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Excel functions handle objects in memory.	5.5	More Details
CVE-2020-1493	An information disclosure vulnerability exists when attaching files to Outlook messages. This vulnerability could potentially allow users to share attached files such that they are accessible by anonymous users where they should be restricted to specific users. To exploit this vulnerability, an attacker would have to attach a file as a link to an email. The email could then be shared with individuals that should not have access to the files, ignoring the default organizational setting. The security update addresses the vulnerability by correcting how Outlook handles file attachment links.	5.5	More Details
CVE-2020-8679	Out-of-bounds write in Kernel Mode Driver for some Intel(R) Graphics Drivers before version 26.20.100.7755 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-24332	An issue was discovered in TrouSerS through 0.3.14. If the tcsd daemon is started with root privileges, the creation of the system.data file is prone to symlink attacks. The tss user can be used to create or corrupt existing files, which could possibly lead to a DoS attack.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8682	Out of bounds read in system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-8683	Improper buffer restrictions in system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-1485	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, an authenticated attacker could connect an imaging device (camera, scanner, cellular phone) to an affected system and run a specially crafted application to disclose information. The security update addresses the vulnerability by correcting how the WIA Service handles objects in memory.	5.5	More Details
CVE-2020-8720	Buffer overflow in a subsystem for some Intel(R) Server Boards, Server Systems and Compute Modules before version 1.59 may allow a privileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-16310	A division by zero vulnerability in dot24_print_page() in devices/gdevdm24.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16300	A buffer overflow vulnerability in tiff12_print_page() in devices/gdevtfnx.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1472	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access. Microsoft is addressing the vulnerability in a phased two-part rollout. These updates address the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels. For guidelines on how to manage the changes required for this vulnerability and more information on the phased rollout, see How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 (updated September 28, 2020). When the second phase of Windows updates become available in Q1 2021, customers will be notified via a revision to this security vulnerability. If you wish to be notified when these updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this advisory. See Microsoft Technical Security Notifications.	5.5	More Details
CVE-2020-1417	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	5.5	More Details
CVE-2020-1383	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system To exploit this vulnerability, an attacker would need to run a specially crafted application against an RPC server which has Routing and Remote Access enabled. Routing and Remote Access is a non-default configuration; systems without it enabled are not vulnerable. The security update addresses the vulnerability by correcting how the Routing and Remote Access service handles requests.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1476	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files. An attacker who successfully exploited this vulnerability could gain access to restricted files. To exploit this vulnerability, an attacker would need to send a specially crafted request to an affected server. The update addresses the vulnerability by changing how ASP.NET and .NET handle requests.	5.5	More Details
CVE-2020-17538	A buffer overflow vulnerability in GetNumSameData() in contrib/lips4/gdevlips.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-15137	All versions of HoRNDIS are affected by an integer overflow in the RNDIS packet parsing routines. A malicious USB device can trigger disclosure of unrelated kernel memory to userspace applications on the host, or can cause the kernel to crash. Kernel memory disclosure is especially likely on 32-bit kernels; 64-bit kernels are more likely to crash on attempted exploitation. It is not believed that kernel memory corruption is possible, or that unattended kernel memory disclosure without the collaboration of a userspace program running on the host is possible. The vulnerability is in `HoRNDIS::receivePacket`. `msg_len`, `data_ofs`, and `data_len` can be controlled by an attached USB device, and a negative value of `data_ofs` can bypass the check for `(data_ofs + data_len + 8) > msg_len`, and subsequently can cause a wild pointer copy in the `mbuf_copyback` call. The software is not maintained and no patches are planned. Users of multi-tenant systems with HoRNDIS installed should only connect trusted USB devices to their system.	5.5	More Details
CVE-2020-16306	A null pointer dereference vulnerability in devices/gdevtsep.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted postscript file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16307	A null pointer dereference vulnerability in devices/vector/gdevtxtw.c and psi/zbfont.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted postscript file. This is fixed in v9.51.	5.5	More Details
CVE-2020-1574	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17361	An issue was discovered in ReadyTalk Avian 1.2.0. The vm::arrayCopy method defined in classpath-common.h returns silently when a negative length is provided (instead of throwing an exception). This could result in data being lost during the copy, with varying consequences depending on the subsequent use of the destination buffer. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.5	More Details
CVE-2020-16308	A buffer overflow vulnerability in p_print_image() in devices/gdevcdj.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16309	A buffer overflow vulnerability in lxm5700m_print_page() in devices/gdevlxm.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted eps file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16287	A buffer overflow vulnerability in lprn_is_black() in contrib/lips4/gdevlprn.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16288	A buffer overflow vulnerability in pj_common_print_page() in devices/gdevpjet.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16289	A buffer overflow vulnerability in cif_print_page() in devices/gdevcif.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16290	A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16291	A buffer overflow vulnerability in contrib/gdevdj9.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-13288	In GitLab before 13.0.12, 13.1.6, and 13.2.3, a stored XSS vulnerability exists in the CI/CD Jobs page	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16293	A null pointer dereference vulnerability in compose_group_nonknockout_nonblend_isolated_allmask_common() in base/gxblend.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16292	A buffer overflow vulnerability in mj_raster_cmd() in contrib/japanese/gdevmjc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16305	A buffer overflow vulnerability in pcx_write_rle() in contrib/japanese/gdev10v.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16295	A null pointer dereference vulnerability in clj_media_size() in devices/gdevclj.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16298	A buffer overflow vulnerability in mj_color_correct() in contrib/japanese/gdevmjc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16297	A buffer overflow vulnerability in FloydSteinbergDitheringC() in contrib/gdevbjca.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-8230	A memory corruption vulnerability exists in NextCloud Desktop Client v2.6.4 where missing ASLR and DEP protections in for windows allowed to corrupt memory.	5.5	More Details
CVE-2020-16296	A buffer overflow vulnerability in GetNumWrongData() in contrib/lips4/gdevlips.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1573	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.5	More Details
CVE-2020-16304	A buffer overflow vulnerability in image_render_color_thresh() in base/gxicolor.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted eps file. This is fixed in v9.51.	5.5	More Details
CVE-2020-16294	A buffer overflow vulnerability in epsc_print_page() in devices/gdevepsc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.	5.5	More Details
CVE-2020-1499	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details
CVE-2020-7302	Unrestricted Upload of File with Dangerous Type in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated attackers to upload malicious files to the DLP case management section via lack of sanity checking.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1591	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-16266	An XSS issue was discovered in MantisBT before 2.24.2. Improper escaping on view_all_bug_page.php allows a remote attacker to inject arbitrary HTML into the page by saving it into a text Custom Field, leading to possible code execution in the browser of any user subsequently viewing the issue (if CSP settings allow it).	5.4	More Details
CVE-2020-2236	Jenkins Yet Another Build Visualizer Plugin 1.11 and earlier does not escape tooltip content, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Run/Update permission.	5.4	More Details
CVE-2020-1580	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details
CVE-2020-2229	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the tooltip content of help icons, resulting in a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-17372	SugarCRM before 10.1.0 (Q3 2020) allows XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1500	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details
CVE-2020-17449	PHP-Fusion 9.03 allows XSS via the error_log file.	5.4	More Details
CVE-2020-2231	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the remote address of the host starting a build via 'Trigger builds remotely', resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Job/Configure permission or knowledge of the Authentication Token.	5.4	More Details
CVE-2020-2230	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the project naming strategy description, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Overall/Manage permission.	5.4	More Details
CVE-2020-1501	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9415	The TIBCO Data Virtualization Server component of TIBCO Software Inc.'s TIBCO Data Virtualization and TIBCO Data Virtualization for AWS Marketplace contains a vulnerability that theoretically allows a malicious authenticated user to download any arbitrary file from the affected system. The user must be authenticated and have privileges required to monitor the server in an operational capacity. Affected releases are TIBCO Software Inc.'s TIBCO Data Virtualization: versions 7.0.8 and below, versions 8.0.0, 8.1.0, 8.1.1, and 8.2.0 and TIBCO Data Virtualization for AWS Marketplace: versions 8.2.0 and below.	5.3	More Details
CVE-2020-17373	SugarCRM before 10.1.0 (Q3 2020) allows SQL Injection.	5.3	More Details
CVE-2020-24370	ldebug.c in Lua 5.4.0 allows a negation overflow and segmentation fault in getlocal and setlocal, as demonstrated by getlocal(3,2^31).	5.3	More Details
CVE-2020-24371	lgc.c in Lua 5.4.0 mishandles the interaction between barriers and the sweep phase, leading to a memory access violation involving collectgarbage.	5.3	More Details
CVE-2015-8033	In Textpattern 4.5.7, the password-reset feature does not securely tether a hash to a user account.	5.3	More Details
CVE-2020-1455	A denial of service vulnerability exists when Microsoft SQL Server Management Studio (SSMS) improperly handles files. An attacker could exploit the vulnerability to trigger a denial of service. To exploit the vulnerability, an attacker would first require execution on the victim system. The security update addresses the vulnerability by ensuring Microsoft SQL Server Management Studio properly handles files.	5.3	More Details
CVE-2020-7374	Documalis Free PDF Editor version 5.7.2.26 and Documalis Free PDF Scanner version 5.7.2.122 do not appropriately validate the contents of JPEG images contained within a PDF. Attackers can exploit this vulnerability to trigger a buffer overflow on the stack and gain remote code execution as the user running the Documalis Free PDF Editor or Documalis Free PDF Scanner software.	5.3	More Details
CVE-2015-8032	In Textpattern 4.5.7, an unprivileged author can change an article's markup setting.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17507	An issue was discovered in Qt through 5.12.9, and 5.13.x through 5.15.x before 5.15.1. read_xbm_body in gui/image/qxbmhandler.cpp has a buffer over-read.	5.3	More Details
CVE-2020-7306	Unprotected Storage of Credentials vulnerability in McAfee Data Loss Prevention (DLP) for Mac prior to 11.5.2 allows local users to gain access to the ADRMS username and password via unprotected log files containing plain text	5.2	More Details
CVE-2020-7307	Unprotected Storage of Credentials vulnerability in McAfee Data Loss Prevention (DLP) for Mac prior to 11.5.2 allows local users to gain access to the RiskDB username and password via unprotected log files containing plain text credentials.	5.2	More Details
CVE-2020-3472	A vulnerability in the contacts feature of Cisco Webex Meetings could allow an authenticated, remote attacker with a legitimate user account to access sensitive information. The vulnerability is due to improper access restrictions on users who are added within user contacts. An attacker on one Webex Meetings site could exploit this vulnerability by sending specially crafted requests to the Webex Meetings site. A successful exploit could allow the attacker to view the details of users on another Webex site, including user names and email addresses.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1483	A remote code execution vulnerability exists in Microsoft Outlook when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Outlook software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that where severity is indicated as Critical in the Affected Products table, the Preview Pane is an attack vector. The security update addresses the vulnerability by correcting how Outlook handles objects in memory.	5.0	More Details
CVE-2020-6300	SAP Business Objects Business Intelligence Platform (Central Management Console), versions- 4.2, 4.3, allows an attacker with administrator rights can use the web application to send malicious code to a different end user (victim), as it does not sufficiently encode user-controlled inputs for RecycleBin, resulting in Stored Cross-Site Scripting (XSS) vulnerability.	4.8	More Details
CVE-2020-3464	A vulnerability in the web-based management interface of Cisco UCS Director 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 input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. 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. To exploit this vulnerability, an attacker would need administrative credentials on the affected device.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1578	An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.	4.7	More Details
CVE-2020-7300	Improper Authorization vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote attackers to change the configuration when logged in with view only privileges via carefully constructed HTTP post messages.	4.6	More Details
CVE-2019-14630	Reliance on untrusted inputs in a security decision in some Intel(R) Thunderbolt(TM) controllers may allow unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2020-9103	HUAWEI Mate 20 smartphones with 9.0.0.205(C00E205R2P1) have a logic error vulnerability. In a special scenario, the system does not properly process. As a result, attackers can perform a series of operations to successfully establish P2P connections that are rejected by the peer end. As a result, the availability of the device is affected.	4.6	More Details
CVE-2020-9229	FusionCompute 8.0.0 has an information disclosure vulnerability. Due to the properly protection of certain information, attackers may exploit this vulnerability to obtain certain information.	4.4	More Details
CVE-2020-0553	Out-of-bounds read in kernel mode driver for some Intel(R) Wireless Bluetooth(R) products on Windows* 10, may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2020-6297	Under certain conditions the upgrade of SAP Data Hub 2.7 to SAP Data Intelligence, version - 3.0, allows an attacker to access confidential system configuration information, that should otherwise be restricted, leading to Information Disclosure.	4.4	More Details
CVE-2020-8685	Improper authentication in subsystem for Intel (R) LED Manager for NUC before version 1.2.3 may allow privileged user to potentially enable denial of service via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3449	A vulnerability in the Border Gateway Protocol (BGP) additional paths feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to prevent authorized users from monitoring the BGP status and cause the BGP process to stop processing new updates, resulting in a denial of service (DOS) condition. The vulnerability is due to an incorrect calculation of lexicographical order when displaying additional path information within Cisco IOS XR Software, which causes an infinite loop. An attacker could exploit this vulnerability by sending a specific BGP update from a BGP neighbor peer session of an affected device; an authorized user must then issue a show bgp command for the vulnerability to be exploited. A successful exploit could allow the attacker to prevent authorized users from properly monitoring the BGP status and prevent BGP from processing new updates, resulting in outdated information in the routing and forwarding tables.	4.3	More Details
CVE-2020-3412	A vulnerability in the scheduled meeting template feature of Cisco Webex Meetings could allow an authenticated, remote attacker to create a scheduled meeting template that would belong to another user in their organization. The vulnerability is due to insufficient authorization enforcement for the creation of scheduled meeting templates. An attacker could exploit this vulnerability by sending a crafted request to the Webex Meetings interface to create a scheduled meeting template. A successful exploit could allow the attacker to create a scheduled meeting template that would belong to a user other than themselves.	4.3	More Details
CVE-2020-3413	A vulnerability in the scheduled meeting template feature of Cisco Webex Meetings could allow an authenticated, remote attacker to delete a scheduled meeting template that belongs to another user in their organization. The vulnerability is due to insufficient authorization enforcement for requests to delete scheduled meeting templates. An attacker could exploit this vulnerability by sending a crafted request to the Webex Meetings interface to delete a scheduled meeting template. A successful exploit could allow the attacker to delete a scheduled meeting template that belongs to a user other than themselves.	4.3	More Details
CVE-2019-4582	IBM Maximo Asset Management 7.6.0 and 7.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 167288.	4.3	More Details
CVE-2020-6310	Improper access control in SOA Configuration Trace component in SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 702, 730, 731, 740, 750, allows any authenticated user to enumerate all SAP users, leading to Information Disclosure.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2237	A cross-site request forgery (CSRF) vulnerability in Jenkins Flaky Test Handler Plugin 1.0.4 and earlier allows attackers to rebuild a project at a previous git revision.	4.3	More Details
CVE-2020-6273	SAP S/4 HANA (Fiori UI for General Ledger Accounting), versions 103, 104, does not perform necessary authorization checks for an authenticated user working with attachment service, allowing the attacker to delete attachments due to Missing Authorization Check.	4.3	More Details
CVE-2020-6299	SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 740, 750, 751, 752, 753, 754, 755, allows a business user to access the list of users in the given system using value help, leading to Information Disclosure.	4.3	More Details
CVE-2020-14483	A timeout during a TLS handshake can result in the connection failing to terminate. This can result in a Niagara thread hanging and requires a manual restart of Niagara (Versions 4.6.96.28, 4.7.109.20, 4.7.110.32, 4.8.0.110) and Niagara Enterprise Security (Versions 2.4.31, 2.4.45, 4.8.0.35) to correct.	4.3	More Details
CVE-2020-1567	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input. An attacker could execute arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a HTML editing attack scenario, an attacker could trick a user into editing a specially crafted file that is designed to exploit the vulnerability. The security update addresses the vulnerability by modifying how MSHTML engine validates input.	4.2	More Details
CVE-2020-1566	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3502	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users.	4.1	More Details
CVE-2020-3501	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users.	4.1	More Details
CVE-2020-7301	Cross Site scripting vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated attackers to trigger alerts via the file upload tab in the DLP case management section.	4.1	More Details
CVE-2020-7303	Cross Site scripting vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote user to trigger scripts to run in a user's browser via adding a new label.	4.1	More Details
CVE-2020-6653	Eaton's Secure connect mobile app v1.7.3 & prior stores the user login credentials in logcat file when user create or register the account on the Mobile app. A malicious app or unauthorized user can harvest the information and later on can use the information to monitor and control the user's account and associated devices.	3.8	More Details
CVE-2020-13282	For GitLab before 13.0.12, 13.1.6, 13.2.3 after a group transfer occurs, members from a parent group keep their access level on the subgroup leading to improper access.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2035	When SSL/TLS Forward Proxy Decryption mode has been configured to decrypt the web transactions, the PAN-OS URL filtering feature inspects the HTTP Host and URL path headers for policy enforcement on the decrypted HTTPS web transactions but does not consider Server Name Indication (SNI) field within the TLS Client Hello handshake. This allows a compromised host in a protected network to evade any security policy that uses URL filtering on a firewall configured with SSL Decryption in the Forward Proxy mode. A malicious actor can then use this technique to evade detection of communication on the TLS handshake phase between a compromised host and a remote malicious server. This technique does not increase the risk of a host being compromised in the network. It does not impact the confidentiality or availability of a firewall. This is considered to have a low impact on the integrity of the firewall because the firewall fails to enforce a policy on certain traffic that should have been blocked. This issue does not impact the URL filtering policy enforcement on clear text or encrypted web transactions. This technique can be used only after a malicious actor has compromised a host in the protected network and the TLS/SSL Decryption feature is enabled for the traffic that the attacker controls. Palo Alto Networks is not aware of any malware that uses this technique to exfiltrate data. This issue is applicable to all current versions of PAN-OS. This issue does not impact Panorama or WF-500 appliances.	3.0	More Details
CVE-2020-15141	In openapi-python-client before version 0.5.3, there is a path traversal vulnerability. If a user generated a client using a maliciously crafted OpenAPI document, it is possible for generated files to be placed in arbitrary locations on disk.	3.0	More Details
CVE-2020-8905	A buffer length validation vulnerability in Asylo versions prior to 0.6.0 allows an attacker to read data they should not have access to. The 'enc_untrusted_recvfrom' function generates a return value which is deserialized by 'MessageReader', and copied into three different 'extents'. The length of the third 'extents' is controlled by the outside world, and not verified on copy, allowing the attacker to force Asylo to copy trusted memory data into an untrusted buffer of significantly small length.. We recommend updating Asylo to version 0.6.0 or later.	2.8	More Details
CVE-2020-16186	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-2020-23938	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. This candidate was erroneously published without a public reference containing the required information	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24212	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. This candidate was erroneously published without a public reference containing the required information	N/A	More Details
CVE-2020-23933	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2016-6499	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2016. Notes: none	N/A	More Details
CVE-2016-6502	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2016. Notes: none	N/A	More Details
CVE-2017-9014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2018-7128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7127	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7126	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7089	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-7085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7062	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7061	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2017-9018	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9017	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9016	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9012	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2020-22720	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2017-9011	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9010	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-9009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9007	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9006	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-9004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8999	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8998	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8997	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8996	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8995	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details
CVE-2017-8986	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-7129	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7130	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7131	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7132	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2020-0255	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-10751. Reason: This candidate is a duplicate of CVE-2020-10751. Notes: All CVE users should reference CVE-2020-10751 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-14353	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2017-18270. Reason: This candidate is a duplicate of CVE-2017-18270. Notes: All CVE users should reference CVE-2017-18270 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-17464	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2016-6498	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2016. Notes: none	N/A	More Details
CVE-2018-7157	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-7155	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7154	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7153	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7152	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7150	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7147	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7146	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-7143	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7140	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7139	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7136	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7135	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7134	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details
CVE-2018-7133	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-9013	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none	N/A	More Details