SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 May 2020

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-12389	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76.	10.0	More Details
CVE-2020-12388	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76.	10.0	More Details
CVE-2020-1112	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9045	During installation or upgrade to Software House C•CURE 9000 v2.70 and American Dynamics victor Video Management System v5.2, the credentials of the user used to perform the installation or upgrade are logged in a file. The install log file persists after the installation.	9.9	More Details
CVE-2020-13417	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters.	9.8	More Details
CVE-2020-13389	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	9.8	More Details
CVE-2020-13390	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	9.8	More Details
CVE-2020-13391	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13392	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	9.8	More Details
CVE-2020-13393	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	9.8	More Details
CVE-2020-13394	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	9.8	More Details
CVE-2020-3280	A vulnerability in the Java Remote Management Interface of Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary code as the root user on an affected device.	9.8	More Details
CVE-2020-13388	An exploitable vulnerability exists in the configuration-loading functionality of the jw.util package before 2.3 for Python. When loading a configuration with FromString or FromStream with YAML, one can execute arbitrary Python code, resulting in OS command execution, because safe_load is not used.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5537	Cybozu Desktop for Windows 2.0.23 to 2.2.40 allows remote code execution via unspecified vectors.	9.8	More Details
CVE-2020-13442	A Remote code execution vulnerability exists in DEXT5Upload in DEXT5 through 2.7.1402870. An attacker can upload a PHP file via dext5handler.jsp handler because the uploaded file is stored under dext5uploadeddata/.	9.8	More Details
CVE-2020-8171	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	9.8	More Details
CVE-2020-12395	Mozilla developers and community members reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.	9.8	More Details
CVE-2020-12396	Mozilla developers and community members reported memory safety bugs present in Firefox 75. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 76.	9.8	More Details
CVE-2020-12390	Incorrect origin serialization of URLs with IPv6 addresses could lead to incorrect security checks. This vulnerability affects Firefox < 76.	9.8	More Details
CVE-2020-13433	Jason2605 AdminPanel 4.0 allows SQL Injection via the editPlayer.php hidden parameter.	9.8	More Details
CVE-2020-6831	A buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9409	The administrative UI component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server for AWS Marketplace, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that theoretically allows an unauthenticated attacker to obtain the permissions of a JasperReports Server "superuser" for the affected systems. The attacker can theoretically exploit the vulnerability consistently, remotely, and without authenticating. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 7.1.1 and below, TIBCO JasperReports Server for AWS Marketplace: versions 7.1.1 and below, and TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.1.1 and below.	9.8	More Details
CVE-2020-0901	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	9.8	More Details
CVE-2018-21234	Jodd before 5.0.4 performs Deserialization of Untrusted JSON Data when setClassMetadataName is set.	9.8	More Details
CVE-2020-12828	An issue was discovered in AnchorFree VPN SDK before 1.3.3.218. The VPN SDK service takes certain executable locations over a socket bound to localhost. Binding to the socket and providing a path where a malicious executable file resides leads to executing the malicious executable file with SYSTEM privileges.	9.8	More Details
CVE-2020-13226	WSO2 API Manager 3.0.0 does not properly restrict outbound network access from a Publisher node, opening up the possibility of SSRF to this node's entire intranet.	9.8	More Details
CVE-2019-5997	Video Insight VMS versions prior to 7.6.1 allow remote attackers to conduct code injection attacks via unspecified vectors.	9.8	More Details
CVE-2020-12835	An issue was discovered in SmartBear ReadyAPI SoapUI Pro 3.2.5. Due to unsafe use of an Java RMI based protocol in an unsafe configuration, an attacker can inject malicious serialized objects into the communication, resulting in remote code execution in the context of a client-side Network Licensing Protocol component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1955	CouchDB version 3.0.0 shipped with a new configuration setting that governs access control to the entire database server called `require_valid_user_except_for_up`. It was meant as an extension to the long standing setting `require_valid_user`, which in turn requires that any and all requests to CouchDB will have to be made with valid credentials, effectively forbidding any anonymous requests. The new `require_valid_user_except_for_up` is an off-by-default setting that was meant to allow requiring valid credentials for all endpoints except for the `/_up` endpoint. However, the implementation of this made an error that lead to not enforcing credentials on any endpoint, when enabled. CouchDB versions 3.0.1[1] and 3.1.0[2] fix this issue.	9.8	More Details
CVE-2020-11716	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support."	9.8	More Details
CVE-2020-6462	Use after free in task scheduling in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-6471	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2020-6469	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2020-6466	Use after free in media in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-6465	Use after free in reader mode in Google Chrome on Android prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-6461	Use after free in storage in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-6457	Use after free in speech recognizer in Google Chrome prior to 81.0.4044.113 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6091	An exploitable authentication bypass vulnerability exists in the ESPON Web Control functionality of Epson EB-1470Ui MAIN: 98009273ESWWV107 MAIN2: 8X7325WWV303. A specially crafted series of HTTP requests can cause authentication bypass resulting in information disclosure. An attacker can send an HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2020-13485	The Knock Knock plugin before 1.2.8 for Craft CMS allows IP Whitelist bypass via an X-Forwarded-For HTTP header.	9.1	More Details
CVE-2020-13112	An issue was discovered in libexif before 0.6.22. Several buffer over-reads in EXIF MakerNote handling could lead to information disclosure and crashes. This is different from CVE-2020-0093.	9.1	More Details
CVE-2020-9753	Whale Browser Installer before 1.2.0.5 versions don't support signature verification for Flash installer.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13412	An issue was discovered in Aviatrix Controller before 5.4.1204. An API call on the web interface lacked a session token check to control access, leading to CSRF.	8.8	More Details
CVE-2020-6468	Type confusion in V8 in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6464	Type confusion in Blink in Google Chrome prior to 81.0.4044.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6463	Use after free in ANGLE in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6474	Use after free in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6459	Use after free in payments in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6458	Out of bounds read and write in PDFium in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	8.8	More Details
CVE-2020-13252	Centreon before 19.04.15 allows remote attackers to execute arbitrary OS commands by placing shell metacharacters in RRDdatabase_status_path (via a main.get.php request) and then visiting the include/views/graphs/graphStatus/displayServiceStatus.php page.	8.8	More Details
CVE-2020-12647	Unisys ALGOL Compiler 58.1 before 58.1a.15, 59.1 before 59.1a.9, and 60.0 before 60.0a.5 can emit invalid code sequences under rare circumstances related to syntax. The resulting code could, for example, trigger a system fault or adversely affect confidentiality, integrity, and availability.	8.8	More Details
CVE-2020-1126	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1136, CVE-2020-1150.	8.8	More Details
CVE-2020-13458	An issue was discovered in the Image Resizer plugin before 2.0.9 for Craft CMS. There are CSRF issues with the log-clear controller action.	8.8	More Details
CVE-2020-1117	A remote code execution vulnerability exists in the way that the Color Management Module (ICM32.dll) handles objects in memory, aka 'Microsoft Color Management Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-13249	libmariadb/mariadb_lib.c in MariaDB Connector/C before 3.1.8 does not properly validate the content of an OK packet received from a server. NOTE: although mariadb_lib.c was originally based on code shipped for MySQL, this issue does not affect any MySQL components supported by Oracle.	8.8	More Details
CVE-2020-1956	Apache Kylin 2.3.0, and releases up to 2.6.5 and 3.0.1 has some restful apis which will concatenate os command with the user input string, a user is likely to be able to execute any os command without any protection or validation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13384	Monstra CMS 3.0.4 allows remote authenticated users to upload and execute arbitrary PHP code via admin/index.php?id=filesmanager because, for example, .php filenames are blocked but .php7 filenames are not, a related issue to CVE-2017-18048.	8.8	More Details
CVE-2020-1102	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1024.	8.8	More Details
CVE-2020-1171	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads configuration files after opening a project, aka 'Visual Studio Code Python Extension Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1192.	8.8	More Details
CVE-2020-3956	VMware Cloud Director 10.0.x before 10.0.0.2, 9.7.0.x before 9.7.0.5, 9.5.0.x before 9.5.0.6, and 9.1.0.x before 9.1.0.4 do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface and API access.	8.8	More Details
CVE-2020-8168	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	8.8	More Details
CVE-2019-20804	Gila CMS before 1.11.6 allows CSRF with resultant XSS via the admin/themes URI, leading to compromise of the admin account.	8.8	More Details
CVE-2020-1069	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1023	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1024, CVE-2020-1102.	8.8	More Details
CVE-2020-1024	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1102.	8.8	More Details
CVE-2020-1067	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1061	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-9046	A vulnerability in all versions of Kantech EntraPass Editions could potentially allow an authorized low-privileged user to gain full system-level privileges by replacing critical files with specifically crafted files.	8.8	More Details
CVE-2020-6467	Use after free in WebRTC in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-7808	In RAONWIZ K Upload v2018.0.2.51 and prior, automatic update processing without integrity check on update module(web.js) allows an attacker to modify arguments which causes downloading a random DLL and injection on it.	8.7	More Details
CVE-2020-13398	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) write vulnerability has been detected in crypto_rsa_common in libfreerdp/crypto/crypto.c.	8.3	More Details
CVE-2020-13113	An issue was discovered in libexif before 0.6.22. Use of uninitialized memory in EXIF Makernote handling could lead to crashes and potential use-after-free conditions.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12034	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable.The EDS subsystem does not provide adequate input sanitation, which may allow an attacker to craft specialized EDS files to inject SQL queries and manipulate the database storing the EDS files. This can lead to denial-of-service conditions.	8.2	More Details
CVE-2020-1056	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain.In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'.	8.1	More Details
CVE-2020-12387	A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.	8.1	More Details
CVE-2020-12693	Slurm 19.05.x before 19.05.7 and 20.02.x before 20.02.3, in the rare case where Message Aggregation is enabled, allows Authentication Bypass via an Alternate Path or Channel. A race condition allows a user to launch a process as an arbitrary user.	8.1	More Details
CVE-2020-1174	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176.	7.8	More Details
CVE-2020-1137	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1082	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1021, CVE-2020-1088.	7.8	More Details
CVE-2020-1081	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1138	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1079	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068.	7.8	More Details
CVE-2020-1139	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1078	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1077	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1175	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176.	7.8	More Details
CVE-2020-1153	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1070	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048.	7.8	More Details
CVE-2020-1140	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1151	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1142	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1068	An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1079.	7.8	More Details
CVE-2020-1143	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054.	7.8	More Details
CVE-2020-1066	An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level.To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.The update addresses the vulnerability by correcting how .NET Framework activates COM objects., aka '.NET Framework Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1176	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175.	7.8	More Details
CVE-2020-1144	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1086	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1124	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-1088	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1021, CVE-2020-1082.	7.8	More Details
CVE-2020-1109	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1110.	7.8	More Details
CVE-2020-1121	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1165, CVE-2020-1166.	7.8	More Details
CVE-2020-1125	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1131	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1154	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1114	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1087.	7.8	More Details
CVE-2020-1111	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1121, CVE-2020-1165, CVE-2020-1166.	7.8	More Details
CVE-2020-1184	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-1132	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles file and folder links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1110	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1109.	7.8	More Details
CVE-2020-1155	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1090	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1156	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1134	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-1157	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1158	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1164.	7.8	More Details
CVE-2020-1135	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1136	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150.	7.8	More Details
CVE-2020-1164	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1165	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1121, CVE-2020-1166.	7.8	More Details
CVE-2020-1166	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1121, CVE-2020-1165.	7.8	More Details
CVE-2020-1087	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1114.	7.8	More Details
CVE-2020-1150	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1136.	7.8	More Details
CVE-2020-1054	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143.	7.8	More Details
CVE-2020-1185	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-12393	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.	7.8	More Details
CVE-2020-13241	Microweber 1.1.18 allows Unrestricted File Upload because admin/view:modules/load_module:users#edit-user=1 does not verify that the file extension (used with the Add Image option on the Edit User screen) corresponds to an image file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6477	Inappropriate implementation in installer in Google Chrome on OS X prior to 83.0.4103.61 allowed a local attacker to perform privilege escalation via a crafted file.	7.8	More Details
CVE-2020-7813	Ezhttptrans.ocx ActiveX Control in Kaoni ezHTTPTrans 1.0.0.70 and prior versions contain a vulnerability that could allow remote attacker to download and execute arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution.	7.8	More Details
CVE-2020-1191	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190.	7.8	More Details
CVE-2020-1190	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1191.	7.8	More Details
CVE-2020-5752	Relative path traversal in Druva inSync Windows Client 6.6.3 allows a local, unauthenticated attacker to execute arbitrary operating system commands with SYSTEM privileges.	7.8	More Details
CVE-2020-1189	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-1188	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1187	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-1186	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	7.8	More Details
CVE-2020-1192	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads workspace settings from a notebook file, aka 'Visual Studio Code Python Extension Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1171.	7.8	More Details
CVE-2020-1149	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	7.8	More Details
CVE-2020-1028	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1126, CVE-2020-1136, CVE-2020-1150.	7.8	More Details
CVE-2020-1010	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079.	7.8	More Details
CVE-2020-1051	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176.	7.8	More Details
CVE-2020-1048	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1021	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1082, CVE-2020-1088.	7.8	More Details
CVE-2017-18868	Digi XBee 2 devices do not have an effective protection mechanism against remote AT commands, because of issues related to the network stack upon which the ZigBee protocol is built.	7.7	More Details
CVE-2020-10725	A flaw was found in DPDK version 19.11 and above that allows a malicious guest to cause a segmentation fault of the vhost-user backend application running on the host, which could result in a loss of connectivity for the other guests running on that host. This is caused by a missing validity check of the descriptor address in the function `virtio_dev_rx_batch_packed()`.	7.7	More Details
CVE-2020-1118	A denial of service vulnerability exists in the Windows implementation of Transport Layer Security (TLS) when it improperly handles certain key exchanges, aka 'Microsoft Windows Transport Layer Security Denial of Service Vulnerability'.	7.5	More Details
CVE-2020-12391	Documents formed using data: URLs in an OBJECT element failed to inherit the CSP of the creating context. This allowed the execution of scripts that should have been blocked, albeit with a unique opaque origin. This vulnerability affects Firefox < 76.	7.5	More Details
CVE-2020-3272	A vulnerability in the DHCP server of Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation of incoming DHCP traffic. An attacker could exploit this vulnerability by sending a crafted DHCP request to an affected device. A successful exploit could allow the attacker to cause a restart of the DHCP server process, causing a DoS condition.	7.5	More Details
CVE-2020-13415	An issue was discovered in Aviatrix Controller through 5.1. An attacker with any signed SAML assertion from the Identity Provider can establish a connection (even if that SAML assertion has expired or is from a user who is not authorized to access Aviatrix), aka XML Signature Wrapping.	7.5	More Details
CVE-2020-3811	qmail-verify as used in netqmail 1.06 is prone to a mail-address verification bypass vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1113	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'.	7.5	More Details
CVE-2020-13414	An issue was discovered in Aviatrix Controller before 5.4.1204. It contains credentials unused by the software.	7.5	More Details
CVE-2020-1060	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093.	7.5	More Details
CVE-2020-1108	A denial of service vulnerability exists when .NET Core or .NET Framework improperly handles web requests, aka '.NET Core & .NET Framework Denial of Service Vulnerability'.	7.5	More Details
CVE-2020-11076	In Puma (RubyGem) before 4.3.4 and 3.12.5, an attacker could smuggle an HTTP response, by using an invalid transfer-encoding header. The problem has been fixed in Puma 3.12.5 and Puma 4.3.4.	7.5	More Details
CVE-2020-1062	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092.	7.5	More Details
CVE-2020-1035	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093.	7.5	More Details
CVE-2020-1161	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'.	7.5	More Details
CVE-2020-8572	Element OS prior to version 12.0 and Element HealthTools prior to version 2020.04.01.04 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information.	7.5	More Details
CVE-2020-1092	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0909	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'.	7.5	More Details
CVE-2020-6830	For native-to-JS bridging, the app requires a unique token to be passed that ensures non-app code can't call the bridging functions. That token was being used for JS-to-native also, but it isn't needed in this case, and its usage was also leaking this token. This vulnerability affects Firefox for iOS < 25.	7.5	More Details
CVE-2020-13114	An issue was discovered in libexif before 0.6.22. An unrestricted size in handling Canon EXIF MakerNote data could lead to consumption of large amounts of compute time for decoding EXIF data.	7.5	More Details
CVE-2020-10738	A flaw was found in Moodle versions 3.8 before 3.8.3, 3.7 before 3.7.6, 3.6 before 3.6.10, 3.5 before 3.5.12 and earlier unsupported versions. It was possible to create a SCORM package in such a way that when added to a course, it could be interacted with via web services in order to achieve remote code execution.	7.5	More Details
CVE-2020-1037	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'.	7.5	More Details
CVE-2020-1065	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'.	7.5	More Details
CVE-2020-13246	An issue was discovered in Gitea through 1.11.5. An attacker can trigger a deadlock by initiating a transfer of a repository's ownership from one organization to another.	7.5	More Details
CVE-2020-1093	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060.	7.5	More Details
CVE-2020-1096	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1799	E6878-370 with versions of 10.0.3.1(H557SP27C233), 10.0.3.1(H563SP1C00), 10.0.3.1(H563SP1C233) has a use after free vulnerability. The software references memory after it has been freed in certain scenario, the attacker does a series of crafted operations through web portal, successful exploit could cause a use after free condition which may lead to malicious code execution.	7.5	More Details
CVE-2020-1064	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, aka 'MSHTML Engine Remote Code Execution Vulnerability'.	7.5	More Details
CVE-2020-1058	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093.	7.5	More Details
CVE-2020-13482	EM-HTTP-Request 1.1.5 uses the library eventmachine in an insecure way that allows an attacker to perform a man-in-the-middle attack against users of the library. The hostname in a TLS server certificate is not verified.	7.4	More Details
CVE-2020-9410	The report generator component of TIBCO Software Inc.'s TIBCO JasperReports Library, TIBCO JasperReports Library for ActiveMatrix BPM, TIBCO JasperReports Server, TIBCO JasperReports Server for AWS Marketplace, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that theoretically allows an attacker to exploit HTML injection to gain full control of a web interface containing the output of the report generator component with the privileges of any user that views the affected report(s). The attacker can theoretically exploit this vulnerability when other users view a maliciously generated report, where those reports use Fusion Charts and a data source with contents controlled by the attacker. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Library: versions 7.1.1 and below, versions 7.2.0 and 7.2.1, version 7.3.0, version 7.5.0, TIBCO JasperReports Library for ActiveMatrix BPM: versions 7.1.1 and below, TIBCO JasperReports Server: versions 7.1.1 and below, version 7.2.0, version 7.5.0, TIBCO JasperReports Server for AWS Marketplace: versions 7.5.0 and below, and TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.1.1 and below.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3184	A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates user input for specific SQL queries. An attacker could exploit this vulnerability by authenticating to the application with valid administrative credentials and sending malicious requests to an affected system. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, or delete information from the database that they are not authorized to delete.	7.2	More Details
CVE-2020-5579	SQL injection vulnerability in the Paid Memberships versions prior to 2.3.3 allows attacker with administrator rights to execute arbitrary SQL commands via unspecified vectors.	7.2	More Details
CVE-2020-13396	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in ntlm_read_ChallengeMessage in winpr/libwinpr/sspi/NTLM/ntlm_message.c.	7.1	More Details
CVE-2020-13425	TrackR devices through 2020-05-06 allow attackers to trigger the Beep (aka alarm) feature, which will eventually cause a denial of service when battery capacity is exhausted.	7.1	More Details
CVE-2020-9484	When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.	7.0	More Details
CVE-2020-11078	In httplib2 before version 0.18.0, an attacker controlling unescaped part of uri for `httplib2.Http.request()` could change request headers and body, send additional hidden requests to same server. This vulnerability impacts software that uses httplib2 with uri constructed by string concatenation, as opposed to proper urllib building with escaping. This has been fixed in 0.18.0.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1071	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'.	6.8	More Details
CVE-2020-1173	A spoofing vulnerability exists in Microsoft Power BI Report Server in the way it validates the content-type of uploaded attachments, aka 'Microsoft Power BI Report Server Spoofing Vulnerability'.	6.8	More Details
CVE-2020-11077	In Puma (RubyGem) before 4.3.5 and 3.12.6, a client could smuggle a request through a proxy, causing the proxy to send a response back to another unknown client. If the proxy uses persistent connections and the client adds another request in via HTTP pipelining, the proxy may mistake it as the first request's body. Puma, however, would see it as two requests, and when processing the second request, send back a response that the proxy does not expect. If the proxy has reused the persistent connection to Puma to send another request for a different client, the second response from the first client will be sent to the second client. This is a similar but different vulnerability from CVE-2020-11076. The problem has been fixed in Puma 3.12.6 and Puma 4.3.5.	6.8	More Details
CVE-2020-12431	A Windows privilege change issue was discovered in Splashtop Software Updater before 1.5.6.16. Insecure permissions on the configuration file and named pipe allow for local privilege escalation to NT AUTHORITY/SYSTEM, by forcing a permission change to any Splashtop files and directories, with resultant DLL hijacking. This product is bundled with Splashtop Streamer (before 3.3.8.0) and Splashtop Business (before 3.3.8.0).	6.6	More Details
CVE-2020-13440	ffjpeg through 2020-02-24 has an invalid write in bmp_load in bmp.c.	6.5	More Details
CVE-2020-13439	ffjpeg through 2020-02-24 has a heap-based buffer over-read in jfif_decode in jfif.c.	6.5	More Details
CVE-2020-10719	A flaw was found in Undertow in versions before 2.1.1.Final, regarding the processing of invalid HTTP requests with large chunk sizes. This flaw allows an attacker to take advantage of HTTP request smuggling.	6.5	More Details
CVE-2020-1179	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13438	ffjpeg through 2020-02-24 has an invalid read in jfif_encode in jfif.c.	6.5	More Details
CVE-2020-13424	The XCloner component before 3.5.4 for Joomla! allows Authenticated Local File Disclosure.	6.5	More Details
CVE-2020-13416	An issue was discovered in Aviatrix Controller before 5.4.1066. A Controller Web Interface session token parameter is not required on an API call, which opens the application up to a Cross Site Request Forgery (CSRF) vulnerability for password resets.	6.5	More Details
CVE-2020-1103	An information disclosure vulnerability exists where certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF).When users are simultaneously logged in to Microsoft SharePoint Server and visit a malicious web page, the attacker can, through standard browser functionality, induce the browser to invoke search queries as the logged in user, aka 'Microsoft SharePoint Information Disclosure Vulnerability'.	6.5	More Details
CVE-2020-6484	Insufficient data validation in ChromeDriver in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted request.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9069	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8	6.5	More Details
CVE-2020-6491	Insufficient data validation in site information in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted domain name.	6.5	More Details
CVE-2020-0963	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179.	6.5	More Details
CVE-2020-6478	Inappropriate implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6476	Insufficient policy enforcement in tab strip in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	6.5	More Details
CVE-2020-6475	Incorrect implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details
CVE-2020-6473	Insufficient policy enforcement in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2020-6472	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory or disk via a crafted Chrome Extension.	6.5	More Details
CVE-2020-6479	Inappropriate implementation in sharing in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details
CVE-2020-6480	Insufficient policy enforcement in enterprise in Google Chrome prior to 83.0.4103.61 allowed a local attacker to bypass navigation restrictions via UI actions.	6.5	More Details
CVE-2020-6460	Insufficient data validation in URL formatting in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to perform domain spoofing via a crafted domain name.	6.5	More Details
CVE-2020-6481	Insufficient policy enforcement in URL formatting in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to perform domain spoofing via a crafted domain name.	6.5	More Details
CVE-2020-6487	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-13231	In Cacti before 1.2.11, auth_profile.php?action=edit allows CSRF for an admin email change.	6.5	More Details
CVE-2020-6486	Insufficient policy enforcement in navigations in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6482	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	6.5	More Details
CVE-2020-4461	IBM Security Access Manager Appliance 9.0.7.1 could allow an authenticated user to bypass security by allowing id_token claims manipulation without verification. IBM X-Force ID: 181481.	6.5	More Details
CVE-2020-6483	Insufficient policy enforcement in payments in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-6485	Insufficient data validation in media router in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-3314	A vulnerability in the file scan process of Cisco AMP for Endpoints Mac Connector Software could cause the scan engine to crash during the scan of local files, resulting in a restart of the AMP Connector and a denial of service (DoS) condition of the Cisco AMP for Endpoints service. The vulnerability is due to insufficient input validation of specific file attributes. An attacker could exploit this vulnerability by providing a crafted file to a user of an affected system. A successful exploit could allow the attacker to cause the Cisco AMP for Endpoints service to crash, resulting in missed detection and logging of the potentially malicious file. Continued attempts to scan the file could result in a DoS condition of the Cisco AMP for Endpoints service.	6.1	More Details
CVE-2020-7655	netius prior to 1.17.58 is vulnerable to HTTP Request Smuggling. HTTP pipelining issues and request smuggling attacks might be possible due to incorrect Transfer encoding header parsing which could allow for CL:TE or TE:TE attacks.	6.1	More Details
CVE-2020-7658	meinheld prior to 1.0.2 is vulnerable to HTTP Request Smuggling. HTTP pipelining issues and request smuggling attacks might be possible due to incorrect Content-Length and Transfer encoding header parsing.	6.1	More Details
CVE-2020-13258	Contentful through 2020-05-21 for Python allows reflected XSS, as demonstrated by the api parameter to the-example-app.py.	6.1	More Details
CVE-2019-20803	Gila CMS before 1.11.6 has reflected XSS via the admin/content/postcategory id parameter, which is mishandled for g_preview_theme.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13430	Grafana before 7.0.0 allows tag value XSS via the OpenTSDB datasource.	6.1	More Details
CVE-2020-6470	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 83.0.4103.61 allowed a local attacker to inject arbitrary scripts or HTML (UXSS) via crafted clipboard contents.	6.1	More Details
CVE-2020-13486	The Knock Knock plugin before 1.2.8 for Craft CMS allows malicious redirection.	6.1	More Details
CVE-2020-10751	A flaw was found in the Linux kernels SELinux LSM hook implementation before version 5.7, where it incorrectly assumed that an skb would only contain a single netlink message. The hook would incorrectly only validate the first netlink message in the skb and allow or deny the rest of the messages within the skb with the granted permission without further processing.	6.1	More Details
CVE-2020-8170	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	6.1	More Details
CVE-2020-1106	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, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1099, CVE-2020-1100, CVE-2020-1101.	6.1	More Details
CVE-2020-1055	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs, aka 'Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability'.	6.1	More Details
CVE-2020-10726	A vulnerability was found in DPDK versions 19.11 and above. A malicious container that has direct access to the vhost-user socket can keep sending VHOST_USER_GET_INFLIGHT_FD messages, causing a resource leak (file descriptors and virtual memory), which may result in a denial of service.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10711	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service.	5.9	More Details
CVE-2020-13614	An issue was discovered in ssl.c in Axel before 2.17.8. The TLS implementation lacks hostname verification.	5.9	More Details
CVE-2020-13615	lib/QoreSocket.cpp in Qore before 0.9.4.2 lacks hostname verification for X.509 certificates.	5.9	More Details
CVE-2020-13616	The boost ASIO wrapper in net/asio.cpp in Pichi before 1.3.0 lacks TLS hostname verification.	5.9	More Details
CVE-2020-1195	An elevation of privilege vulnerability exists in Microsoft Edge (Chromium-based) when the Feedback extension improperly validates input, aka 'Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability'.	5.9	More Details
CVE-2020-1145	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1179.	5.5	More Details
CVE-2020-13435	SQLite through 3.32.0 has a segmentation fault in sqlite3ExprCodeTarget in expr.c.	5.5	More Details
CVE-2020-1076	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1084	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values.An attacker who successfully exploited this vulnerability could deny dependent security feature functionality.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 the Connected User Experiences and Telemetry Service validates certain function values., aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1123.	5.5	More Details
CVE-2020-1075	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka 'Windows Subsystem for Linux Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1072	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-3812	qmail-verify as used in netqmail 1.06 is prone to an information disclosure vulnerability. A local attacker can test for the existence of files and directories anywhere in the filesystem because qmail-verify runs as root and tests for the existence of files in the attacker's home directory, without dropping its privileges first.	5.5	More Details
CVE-2020-3344	A vulnerability in Cisco AMP for Endpoints Linux Connector Software and Cisco AMP for Endpoints Mac Connector Software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted packet to an affected device. A successful exploit could allow the attacker to cause the Cisco AMP for Endpoints service to crash and restart.	5.5	More Details
CVE-2020-12392	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.	5.5	More Details
CVE-2020-13152	A remote user can create a specially crafted M3U file, media playlist file that when loaded by the target user, will trigger a memory leak, whereby Amarok 2.8.0 continue to waste resources over time, eventually allows attackers to cause a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1116	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-13397	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in security_fips_decrypt in libfreerdp/core/security.c due to an uninitialized value.	5.5	More Details
CVE-2020-1123	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1084.	5.5	More Details
CVE-2020-1141	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179.	5.5	More Details
CVE-2020-3343	A vulnerability in Cisco AMP for Endpoints Linux Connector Software and Cisco AMP for Endpoints Mac Connector Software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted packet to an affected device. A successful exploit could allow the attacker to cause the Cisco AMP for Endpoints service to crash and restart.	5.5	More Details
CVE-2020-13434	SQLite through 3.32.0 has an integer overflow in sqlite3_str_vappendf in printf.c.	5.5	More Details
CVE-2020-13239	The DMS/ECM module in Dolibarr 11.0.4 renders user-uploaded .html files in the browser when the attachment parameter is removed from the direct download link. This causes XSS.	5.4	More Details
CVE-2020-1104	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1105, CVE-2020-1107.	5.4	More Details
CVE-2020-1101	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, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1099, CVE-2020-1100, CVE-2020-1106.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13240	The DMS/ECM module in Dolibarr 11.0.4 allows users with the 'Setup documents directories' permission to rename uploaded files to have insecure file extensions. This bypasses the .noexe protection mechanism against XSS.	5.4	More Details
CVE-2020-1105	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1107.	5.4	More Details
CVE-2020-1107	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1105.	5.4	More Details
CVE-2020-1100	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, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1099, CVE-2020-1101, CVE-2020-1106.	5.4	More Details
CVE-2020-8789	Composr 10.0.30 allows Persistent XSS via a Usergroup name under the Security configuration.	5.4	More Details
CVE-2020-13459	An issue was discovered in the Image Resizer plugin before 2.0.9 for Craft CMS. There is stored XSS in the Bulk Resize action.	5.4	More Details
CVE-2020-1063	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, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'.	5.4	More Details
CVE-2020-1099	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, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1100, CVE-2020-1101, CVE-2020-1106.	5.4	More Details
CVE-2020-13429	legend.ts in the piechart-panel (aka Pie Chart Panel) plugin before 1.5.0 for Grafana allows XSS via the Values Header (aka legend header) option.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11048	In PHP versions 7.2.x below 7.2.31, 7.3.x below 7.3.18 and 7.4.x below 7.4.6, when HTTP file uploads are allowed, supplying overly long filenames or field names could lead PHP engine to try to allocate oversized memory storage, hit the memory limit and stop processing the request, without cleaning up temporary files created by upload request. This potentially could lead to accumulation of uncleaned temporary files exhausting the disk space on the target server.	5.3	More Details
CVE-2020-13413	An issue was discovered in Aviatrix Controller before 5.4.1204. There is a Observable Response Discrepancy from the API, which makes it easier to perform user enumeration via brute force.	5.3	More Details
CVE-2020-5365	Dell EMC Isilon versions 8.2.2 and earlier contain a remotesupport vulnerability. The pre-configured support account, remotesupport, is bundled in the Dell EMC Isilon OneFS installation. This account is used for diagnostics and other support functions. Although the default password is different for every cluster, it is predictable.	5.3	More Details
CVE-2020-5364	Dell EMC Isilon OneFS versions 8.2.2 and earlier contain an SNMPv2 vulnerability. The SNMPv2 services is enabled, by default, with a pre-configured community string. This community string allows read-only access to many aspects of the Isilon cluster, some of which are considered sensitive and can foster additional access.	5.3	More Details
CVE-2020-5753	Signal Private Messenger Android v4.59.0 and up and iOS v3.8.1.5 and up allows a remote non-contact to ring a victim's Signal phone and disclose currently used DNS server due to ICE Candidate handling before call is answered or declined.	5.3	More Details
CVE-2020-13225	phpIPAM 1.4 contains a stored cross site scripting (XSS) vulnerability within the Edit User Instructions field of the User Instructions widget.	4.8	More Details
CVE-2020-13487	The bbPress plugin through 2.6.4 for WordPress has stored XSS in the Forum creation section, resulting in JavaScript execution at wp-admin/edit.php?post_type=forum (aka the Forum listing page) for all users. An administrator can exploit this at the wp-admin/post.php?action=edit URI.	4.8	More Details
CVE-2020-1059	A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content, aka 'Microsoft Edge Spoofing Vulnerability'.	4.3	More Details
CVE-2020-6490	Insufficient data validation in loader in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had been able to write to disk to leak cross-origin data via a crafted HTML page.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6489	Inappropriate implementation in developer tools in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had convinced the user to take certain actions in developer tools to obtain potentially sensitive information from disk via a crafted HTML page.	4.3	More Details
CVE-2020-12397	By encoding Unicode whitespace characters within the From email header, an attacker can spoof the sender email address that Thunderbird displays. This vulnerability affects Thunderbird < 68.8.0.	4.3	More Details
CVE-2020-6488	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	4.3	More Details
CVE-2020-13230	In Cacti before 1.2.11, disabling a user account does not immediately invalidate any permissions granted to that account (e.g., permission to view logs).	4.3	More Details
CVE-2020-12394	A logic flaw in our location bar implementation could have allowed a local attacker to spoof the current location by selecting a different origin and removing focus from the input element. This vulnerability affects Firefox < 76.	3.3	More Details
CVE-2020-11970	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