SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 June 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-2020-9412	The file transfer component of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i contains a vulnerability that theoretically allows execution of arbitrary commands at the privilege level of the affected system following a failed file transfer. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i: versions 7.1.0 and below, version 8.0.0.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9411	The file transfer component of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i contains a vulnerability that theoretically allows an attacker to perform unauthorized network file transfers to and from the file system accessible to the affected component. This vulnerability is exploitable when the configuration option 'Require Node Resp' is set to 'No'. In the event of a successful exploit, the attacker could theoretically read and write any file on the file system accessible to the affected component, thus fully affecting the confidentiality, integrity, and availability of the operating system hosting the deployment of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i: versions 7.1.0 and below, version 8.0.0.	10.0	More Details
CVE-2020-8180	A too lax check in Nextcloud Talk 6.0.4, 7.0.2 and 8.0.7 allowed a code injection when a not correctly sanitized talk command was added by an administrator.	9.9	More Details
CVE-2020-13832	An issue was discovered on Samsung mobile devices with Q(10.0) (with TEEGRIS on Exynos chipsets) software. The Widevine Trustlet allows arbitrary code execution because of memory disclosure, The Samsung IDs are SVE-2020-17117, SVE-2020-17118, SVE-2020-17119, and SVE-2020-17161 (June 2020).	9.8	More Details
CVE-2020-4448	IBM WebSphere Application Server Network Deployment 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: 181228.	9.8	More Details
CVE-2020-7115	The ClearPass Policy Manager web interface is affected by a vulnerability that leads to authentication bypass. Upon successful bypass an attacker could then execute an exploit that would allow to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	9.8	More Details
CVE-2020-13835	An issue was discovered on Samsung mobile devices with O(8.x) (with TEEGRIS) software. The Gatekeeper Trustlet allows a brute-force attack on user credentials. The Samsung ID is SVE-2020-16908 (June 2020).	9.8	More Details
CVE-2020-13768	In MiniShare before 1.4.2, there is a stack-based buffer overflow via an HTTP PUT request, which allows an attacker to achieve arbitrary code execution, a similar issue to CVE-2018-19861, CVE-2018-19862, and CVE-2019-17601. NOTE: this product is discontinued.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13839	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020).	9.8	More Details
CVE-2020-13840	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020).	9.8	More Details
CVE-2020-13841	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020).	9.8	More Details
CVE-2020-11975	Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process.	9.8	More Details
CVE-2020-13909	The Ignition component before 2.0.5 for Laravel mishandles globals, _get, _post, _cookie, and _env. NOTE: in the 1.x series, versions 1.16.15 and later are unaffected as a consequence of the CVE-2021-43996 fix.	9.8	More Details
CVE-2020-4450	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181231.	9.8	More Details
CVE-2019-20830	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has an out-of-bounds write when Internet Explorer is used.	9.8	More Details
CVE-2020-6109	An exploitable path traversal vulnerability exists in the Zoom client, version 4.6.10 processes messages including animated GIFs. A specially crafted chat message can cause an arbitrary file write, which could potentially be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to exploit this vulnerability.	9.8	More Details
CVE-2020-9099	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12800	The drag-and-drop-multiple-file-upload-contact-form-7 plugin before 1.3.3.3 for WordPress allows Unrestricted File Upload and remote code execution by setting supported_type to php% and uploading a .php% file.	9.8	More Details
CVE-2020-13160	AnyDesk before 5.5.3 on Linux and FreeBSD has a format string vulnerability that can be exploited for remote code execution.	9.8	More Details
CVE-2020-9838	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5. A remote attacker may be able to cause arbitrary code execution.	9.8	More Details
CVE-2020-9850	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution.	9.8	More Details
CVE-2020-13831	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020).	9.8	More Details
CVE-2020-6265	SAP Commerce, versions - 6.7, 1808, 1811, 1905, and SAP Commerce (Data Hub), versions - 6.7, 1808, 1811, 1905, allows an attacker to bypass the authentication and/or authorization that has been configured by the system administrator due to the use of Hardcoded Credentials.	9.8	More Details
CVE-2019-20827	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It allows stack consumption because of interaction between ICC-Based color space and Alternate color space.	9.8	More Details
CVE-2020-9292	An unquoted service path vulnerability in the FortiSIEM Windows Agent component may allow an attacker to gain elevated privileges via the AoWinAgt executable service path.	9.8	More Details
CVE-2020-10546	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicies.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	9.8	More Details
CVE-2020-10547	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicyelements.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3198	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2020-10548	rConfig 3.9.4 and previous versions has unauthenticated devices.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	9.8	More Details
CVE-2019-20825	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has an out-of-bounds write when Internet Explorer is used.	9.8	More Details
CVE-2020-4177	IBM Security Guardium 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174732.	9.8	More Details
CVE-2020-13756	Sabberworm PHP CSS Parser before 8.3.1 calls eval on uncontrolled data, possibly leading to remote code execution if the function allSelectors() or getSelectorsBySpecificity() is called with input from an attacker.	9.8	More Details
CVE-2020-3227	A vulnerability in the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an unauthenticated, remote attacker to execute Cisco IOx API commands without proper authorization. The vulnerability is due to incorrect handling of requests for authorization tokens. An attacker could exploit this vulnerability by using a crafted API call to request such a token. An exploit could allow the attacker to obtain an authorization token and execute any of the IOx API commands on an affected device.	9.8	More Details
CVE-2020-10549	rConfig 3.9.4 and previous versions has unauthenticated snippets.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	9.8	More Details
CVE-2020-4193	IBM Security Guardium 11.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 174857.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13804	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows information disclosure of a hardcoded username and password in the DocuSign plugin.	9.8	More Details
CVE-2020-13805	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has brute-force attack mishandling because the CAS service lacks a limit on login failures.	9.8	More Details
CVE-2019-20822	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.7.0.29430. It has an out-of-bounds write via incorrect image data.	9.8	More Details
CVE-2020-13814	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It has a use-after-free via a document that lacks a dictionary.	9.8	More Details
CVE-2018-21242	An issue was discovered in Foxit PhantomPDF before 8.3.6. It allows Remote Code Execution via a GoToE or GoToR action.	9.8	More Details
CVE-2020-10516	An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20. This vulnerability was reported via the GitHub Bug Bounty program.	9.8	More Details
CVE-2018-21244	An issue was discovered in Foxit PhantomPDF before 8.3.6. It allows arbitrary application execution via an embedded executable file in a PDF portfolio, aka FG-VD-18-029.	9.8	More Details
CVE-2020-3258	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2020-12773	A security misconfiguration vulnerability exists in the SDK of some Realtek ADSL/PON Modem SoC firmware, which allows attackers using a default password to execute arbitrary commands remotely via the build-in network monitoring tool.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6493	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 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-2020-1963	Apache Ignite uses H2 database to build SQL distributed execution engine. H2 provides SQL functions which could be used by attacker to access to a filesystem.	9.1	More Details
CVE-2020-13910	Pengutronix Barebox through v2020.05.0 has an out-of-bounds read in nfs_read_reply in net/nfs.c because a field of an incoming network packet is directly used as a length field without any bounds check.	9.1	More Details
CVE-2020-13833	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The system area allows arbitrary file overwrites via a symlink attack. The Samsung ID is SVE-2020-17183 (June 2020).	9.1	More Details
CVE-2020-10070	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	9.0	More Details
CVE-2020-10062	An off-by-one error in the Zephyr project MQTT packet length decoder can result in memory corruption and possible remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	9.0	More Details
CVE-2020-10071	The Zephyr MQTT parsing code performs insufficient checking of the length field on publish messages, allowing a buffer overflow and potentially remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13996	The J2Store plugin before 3.3.13 for Joomla! allows a SQL injection attack by a trusted store manager.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3199	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2020-9789	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution.	8.8	More Details
CVE-2020-9790	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution.	8.8	More Details
CVE-2020-3281	A vulnerability in the audit logging component of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.	8.8	More Details
CVE-2020-3234	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device’s virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9802	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-9803	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-1239	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-2020-1238.	8.8	More Details
CVE-2020-3229	A vulnerability in Role Based Access Control (RBAC) functionality of Cisco IOS XE Web Management Software could allow a Read-Only authenticated, remote attacker to execute commands or configuration changes as an Admin user. The vulnerability is due to incorrect handling of RBAC for the administration GUI. An attacker could exploit this vulnerability by sending a modified HTTP request to the affected device. An exploit could allow the attacker as a Read-Only user to execute CLI commands or configuration changes as if they were an Admin user.	8.8	More Details
CVE-2020-3224	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with read-only privileges to inject IOS commands to an affected device. The injected commands should require a higher privilege level in order to be executed. The vulnerability is due to insufficient input validation of specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a specific web UI endpoint on an affected device. A successful exploit could allow the attacker to inject IOS commands to the affected device, which could allow the attacker to alter the configuration of the device or cause a denial of service (DoS) condition.	8.8	More Details
CVE-2020-9806	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-1317	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9807	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-3219	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with administrative privileges on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input to the web UI. A successful exploit could allow an attacker to execute arbitrary commands with administrative privileges on an affected device.	8.8	More Details
CVE-2020-1238	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-2020-1239.	8.8	More Details
CVE-2020-3217	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition.	8.8	More Details
CVE-2020-9818	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination.	8.8	More Details
CVE-2020-1321	A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7012	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	8.8	More Details
CVE-2020-7014	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an authentication token being generated with elevated privileges.	8.8	More Details
CVE-2020-1248	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-6496	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-1286	A remote code execution vulnerability exists when the Windows Shell does not properly validate file paths.An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the current user, aka 'Windows Shell Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1281	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-11679	Castel NextGen DVR v1.0.0 is vulnerable to privilege escalation through the Adminstrator/Users/Edit/:UserId functionality. Adminstrator/Users/Edit/:UserId fails to check that the request was submitted by an Administrator. This allows a normal user to escalate their privileges by adding additional roles to their account.	8.8	More Details
CVE-2020-1295	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'.	8.8	More Details
CVE-2020-1299	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13895	Crypt::Perl::ECDSA in the Crypt::Perl (aka p5-Crypt-Perl) module before 0.32 for Perl fails to verify correct ECDSA signatures when r and s are small and when s = 1. This happens when using the curve secp256r1 (prime256v1). This could conceivably have a security-relevant impact if an attacker wishes to use public r and s values when guessing whether signature verification will fail.	8.8	More Details
CVE-2020-6110	An exploitable partial path traversal vulnerability exists in the way Zoom Client version 4.6.10 processes messages including shared code snippets. A specially crafted chat message can cause an arbitrary binary planting which could be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to trigger this vulnerability. For the most severe effect, target user interaction is required.	8.8	More Details
CVE-2020-9042	In Couchbase Server 6.0, credentials cached by a browser can be used to perform a CSRF attack if an administrator has used their browser to check the results of a REST API request.	8.8	More Details
CVE-2020-13976	An issue was discovered in DD-WRT through 16214. The Diagnostic page allows remote attackers to execute arbitrary commands via shell metacharacters in the host field of the ping command. Exploitation through CSRF might be possible. NOTE: software maintainers consider the report invalid because it refers to an old software version, requires administrative privileges, and does not provide access beyond that already available to administrative users	8.8	More Details
CVE-2020-6453	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6419	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-1300	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1255	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'.	8.8	More Details
CVE-2011-1805	Bad cast in CSS in Google Chrome prior to 11.0.0.0 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-1301	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-5589	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product.	8.8	More Details
CVE-2020-3205	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory.	8.8	More Details
CVE-2020-9800	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-4180	IBM Security Guardium 11.1 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 174735.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13786	D-Link DIR-865L Ax 1.20B01 Beta devices allow CSRF.	8.8	More Details
CVE-2020-1181	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-2020-1178	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted authentication request to an affected SharePoint server, aka 'Microsoft SharePoint Server Elevation of Privilege Vulnerability'.	8.8	More Details
CVE-2020-13872	Royal TS before 5 has a 0.0.0.0 listener, which makes it easier for attackers to bypass tunnel authentication via a brute-force approach.	8.8	More Details
CVE-2020-2200	Jenkins Play Framework Plugin 1.0.2 and earlier lets users specify the path to the `play` command on the Jenkins master for a form validation endpoint, resulting in an OS command injection vulnerability exploitable by users able to store such a file on the Jenkins master.	8.8	More Details
CVE-2020-1223	A remote code execution vulnerability exists when Microsoft Word for Android fails to properly handle certain files.To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted URL file.The update addresses the vulnerability by correcting how Microsoft Word for Android handles specially crafted URL files., aka 'Word for Android Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1225	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'. This CVE ID is unique from CVE-2020-1226.	8.8	More Details
CVE-2020-13782	D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection.	8.8	More Details
CVE-2020-1226	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'. This CVE ID is unique from CVE-2020-1225.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3228	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2020-3226	A vulnerability in the Session Initiation Protocol (SIP) library of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on received SIP messages. An attacker could exploit this vulnerability by sending crafted SIP messages to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service condition.	8.6	More Details
CVE-2020-3225	Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to insufficient input processing of CIP traffic. An attacker could exploit these vulnerabilities by sending crafted CIP traffic to be processed by an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.	8.6	More Details
CVE-2020-9847	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to break out of its sandbox.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3221	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device.	8.6	More Details
CVE-2020-3203	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition.	8.6	More Details
CVE-2020-4040	Bolt CMS before version 3.7.1 lacked CSRF protection in the preview generating endpoint. Previews are intended to be generated by the admins, developers, chief-editors, and editors, who are authorized to create content in the application. But due to lack of proper CSRF protection, unauthorized users could generate a preview. This has been fixed in Bolt 3.7.1	8.6	More Details
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.	8.2	More Details
CVE-2020-13379	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on. Furthermore, passing invalid URL objects could be used for DOS'ing Grafana via SegFault.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3238	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, remote attacker to write or modify arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient input validation of user-supplied application packages. An attacker who can upload a malicious package within Cisco IOx could exploit the vulnerability to modify arbitrary files. The impacts of a successful exploit are limited to the scope of the virtual instance and do not affect the device that is hosting Cisco IOx.	8.1	More Details
CVE-2020-1073	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'.	8.1	More Details
CVE-2020-12851	Pydio Cells 2.0.4 allows an authenticated user to write or overwrite existing files in another user’s personal and cells folders (repositories) by uploading a custom generated ZIP file and leveraging the file extraction feature present in the web application. The extracted files will be placed in the targeted user folders.	8.1	More Details
CVE-2020-13790	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in get_rgb_row() in rdppm.c via a malformed PPM input file.	8.1	More Details
CVE-2020-11681	Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials.	8.1	More Details
CVE-2020-10061	Improper handling of the full-buffer case in the Zephyr Bluetooth implementation can result in memory corruption. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	8.1	More Details
CVE-2020-9794	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents.	8.1	More Details
CVE-2020-3257	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12846	Zimbra before 8.8.15 Patch 10 and 9.x before 9.0.0 Patch 3 allows remote code execution via an avatar file. There is potential abuse of /service/upload servlet in the webmail subsystem. A user can upload executable files (exe,sh,bat,jar) in the Contact section of the mailbox as an avatar image for a contact. A user will receive a "Corrupt File" error, but the file is still uploaded and stored locally in /opt/zimbra/data/tmp/upload/, leaving it open to possible remote execution.	8.0	More Details
CVE-2020-2196	Jenkins Selenium Plugin 3.141.59 and earlier has no CSRF protection for its HTTP endpoints, allowing attackers to perform all administrative actions provided by the plugin.	8.0	More Details
CVE-2020-1270	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-13646	In Cheetah free WiFi 5.1, the driver file (liebaonat.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x830020f8, 0x830020E0, 0x830020E4, or 0x8300210c.	7.8	More Details
CVE-2020-1271	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, aka 'Windows Backup Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1266	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1203	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1202.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1262	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1269	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1199	An elevation of privilege vulnerability exists when the Windows Feedback Hub improperly handles objects in memory, aka 'Windows Feedback Hub Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-13866	WinGate v9.4.1.5998 has insecure permissions for the installation directory, which allows local users to gain privileges by replacing an executable file with a Trojan horse.	7.8	More Details
CVE-2020-1264	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1201	An elevation of privilege vulnerability exists in the way the Windows Now Playing Session Manager handles objects in memory, aka 'Windows Now Playing Session Manager Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1207	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-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310.	7.8	More Details
CVE-2020-1265	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-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1202	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203.	7.8	More Details
CVE-2020-1234	An elevation of privilege vulnerability exists when Windows Error Reporting improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1277	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'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1302, CVE-2020-1312.	7.8	More Details
CVE-2020-1272	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312.	7.8	More Details
CVE-2020-1208	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-2020-1236.	7.8	More Details
CVE-2020-13812	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory.	7.8	More Details
CVE-2020-13813	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory when FoxitStudioPhoto366_3.6.6.916.exe is used.	7.8	More Details
CVE-2020-1291	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1287	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21241	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has an untrusted search path that allows a DLL to execute remote code.	7.8	More Details
CVE-2020-1211	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1282	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-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334.	7.8	More Details
CVE-2020-1209	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-13842	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020).	7.8	More Details
CVE-2020-1273	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1280	An elevation of privilege vulnerability exists in the way that the Windows Bluetooth Service handles objects in memory, aka 'Windows Bluetooth Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1279	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly load spotlight images from a secure location, aka 'Windows Lockscreen Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1278	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11492	An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.	7.8	More Details
CVE-2020-1276	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-9859	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-1275	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1274	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1197	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1163	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170.	7.8	More Details
CVE-2020-1196	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9816	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-9858	A dynamic library loading issue was addressed with improved path searching. This issue is fixed in Windows Migration Assistant 2.2.0.0 (v. 1A11). Running the installer in an untrusted directory may result in arbitrary code execution.	7.8	More Details
CVE-2020-9855	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Catalina 10.15.5. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2020-9852	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-1237	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-2020-0986, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-1236	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-2020-1208.	7.8	More Details
CVE-2020-9813	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9814	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9815	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9817	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2020-1222	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1309.	7.8	More Details
CVE-2020-9841	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-1235	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-2020-1231, CVE-2020-1233, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334.	7.8	More Details
CVE-2020-9821	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-1231	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-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334.	7.8	More Details
CVE-2020-9834	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9822	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9825	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A malicious application may be able to bypass Privacy preferences.	7.8	More Details
CVE-2020-9830	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-1241	A security feature bypass vulnerability exists when Windows Kernel fails to properly sanitize certain parameters.To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system.The update addresses the vulnerability by correcting how Windows Kernel handles parameter sanitization., aka 'Windows Kernel Security Feature Bypass Vulnerability'.	7.8	More Details
CVE-2020-1292	An elevation of privilege vulnerability exists in OpenSSH for Windows when it does not properly restrict access to configuration settings, aka 'OpenSSH for Windows Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1257	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293.	7.8	More Details
CVE-2020-1162	An elevation of privilege (user to user) vulnerability exists in Windows Security Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1324.	7.8	More Details
CVE-2020-1170	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163.	7.8	More Details
CVE-2020-13428	A heap-based buffer overflow in the hxxx_AnnexB_to_xVC function in modules/packetizer/hxxx_nal.c in VideoLAN VLC media player before 3.0.11 for macOS/iOS allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted H.264 Annex-B video (.avi for example) file.	7.8	More Details
CVE-2020-13884	Citrix Workspace App before 1912 on Windows has Insecure Permissions and an Unquoted Path vulnerability which allows local users to gain privileges during the uninstallation of the application.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13885	Citrix Workspace App before 1912 on Windows has Insecure Permissions which allows local users to gain privileges during the uninstallation of the application.	7.8	More Details
CVE-2020-1254	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-13974	An issue was discovered in the Linux kernel 4.4 through 5.7.1. drivers/tty/vt/keyboard.c has an integer overflow if k_ascii is called several times in a row, aka CID-b86dab054059. NOTE: Members in the community argue that the integer overflow does not lead to a security issue in this case.	7.8	More Details
CVE-2020-1233	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-2020-1231, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334.	7.8	More Details
CVE-2020-10757	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system.	7.8	More Details
CVE-2020-1217	An information disclosure vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Information Disclosure Vulnerability'.	7.8	More Details
CVE-2020-9795	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-1247	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-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1246	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-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-9788	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.5. A file may be incorrectly rendered to execute JavaScript.	7.8	More Details
CVE-2020-0986	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-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	7.8	More Details
CVE-2020-0916	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'. This CVE ID is unique from CVE-2020-0915.	7.8	More Details
CVE-2020-9791	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9793	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause arbitrary code execution.	7.8	More Details
CVE-2020-0915	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'. This CVE ID is unique from CVE-2020-0916.	7.8	More Details
CVE-2020-13811	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It has an out-of-bounds write via a crafted TIFF file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1212	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1316	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307.	7.8	More Details
CVE-2020-1311	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1309	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1222.	7.8	More Details
CVE-2020-1307	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-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1316.	7.8	More Details
CVE-2020-1306	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-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1334.	7.8	More Details
CVE-2020-1305	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'.	7.8	More Details
CVE-2020-1313	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1314	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1304	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-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1306, CVE-2020-1334.	7.8	More Details
CVE-2020-1302	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'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312.	7.8	More Details
CVE-2020-1293	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278.	7.8	More Details
CVE-2020-1294	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1287.	7.8	More Details
CVE-2020-1334	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-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306.	7.8	More Details
CVE-2020-1324	An elevation of privilege (user to user) vulnerability exists in Windows Security Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1162.	7.8	More Details
CVE-2020-1312	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'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1302.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3232	A vulnerability in the Simple Network Management Protocol (SNMP) implementation in Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM could allow an authenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect handling of data that is returned for Cisco Discovery Protocol queries to SNMP. An attacker could exploit this vulnerability by sending a request for Cisco Discovery Protocol information by using SNMP. An exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.	7.7	More Details
CVE-2020-3235	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system.	7.7	More Details
CVE-2020-3200	A vulnerability in the Secure Shell (SSH) server code of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. The vulnerability is due to an internal state not being represented correctly in the SSH state machine, which leads to an unexpected behavior. An attacker could exploit this vulnerability by creating an SSH connection to an affected device and using a specific traffic pattern that causes an error condition within that connection. A successful exploit could allow an attacker to cause the device to reload, resulting in a denial of service (DoS) condition.	7.7	More Details
CVE-2020-13822	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading '\0' bytes, or integer overflows. This could conceivably have a security-relevant impact if an application relied on a single canonical signature.	7.7	More Details
CVE-2020-13692	PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4509	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364.	7.6	More Details
CVE-2020-9827	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause a denial of service.	7.5	More Details
CVE-2020-1230	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-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260.	7.5	More Details
CVE-2020-4449	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230.	7.5	More Details
CVE-2020-13784	D-Link DIR-865L Ax 1.20B01 Beta devices have a predictable seed in a Pseudo-Random Number Generator.	7.5	More Details
CVE-2020-9844	A double free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	7.5	More Details
CVE-2020-13787	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Transmission of Sensitive Information.	7.5	More Details
CVE-2020-13818	In Zoho ManageEngine OpManager before 125144, when <cachestart> is used, directory traversal validation can be bypassed.	7.5	More Details
CVE-2020-13803	An issue was discovered in Foxit PhantomPDF Mac and Foxit Reader for Mac before 4.0. It allows signature validation bypass via a modified file or a file with non-standard signatures.	7.5	More Details
CVE-2020-5591	XACK DNS 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0 allow remote attackers to cause a denial of service condition resulting in degradation of the recursive resolver's performance or compromising the recursive resolver as a reflector in a reflection attack.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9837	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. A remote attacker may be able to leak memory.	7.5	More Details
CVE-2020-13785	D-Link DIR-865L Ax 1.20B01 Beta devices have Inadequate Encryption Strength.	7.5	More Details
CVE-2020-7661	all versions of url-regex are vulnerable to Regular Expression Denial of Service. An attacker providing a very long string in String.test can cause a Denial of Service.	7.5	More Details
CVE-2020-9826	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause a denial of service.	7.5	More Details
CVE-2020-9824	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.5. A non-privileged user may be able to modify restricted network settings.	7.5	More Details
CVE-2020-1260	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-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230.	7.5	More Details
CVE-2020-13625	PHPMailer before 6.1.6 contains an output escaping bug when the name of a file attachment contains a double quote character. This can result in the file type being misinterpreted by the receiver or any mail relay processing the message.	7.5	More Details
CVE-2020-12695	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	7.5	More Details
CVE-2020-9041	In Couchbase Server 6.0.3 and Couchbase Sync Gateway through 2.7.0, the Cluster management, views, query, and full-text search endpoints are vulnerable to the Slowloris denial-of-service attack because they don't more aggressively terminate slow connections.	7.5	More Details
CVE-2020-9040	Couchbase Server Java SDK before 2.7.1.1 allows a potential attacker to forge an SSL certificate and pose as the intended peer. An attacker can leverage this flaw by crafting a cryptographically valid certificate that will be accepted by Java SDK's Netty component due to missing hostname verification.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13960	D-Link DSL 2730-U IN_1.10 and IN_1.11 and DIR-600M 3.04 devices have the domain.name string in the DNS resolver search path by default, which allows remote attackers to provide valid DNS responses (and also offer Internet services such as HTTP) for names that otherwise would have had an NXDOMAIN error, by registering a subdomain of the domain.name domain name.	7.5	More Details
CVE-2020-13962	Qt 5.12.2 through 5.14.2, as used in unofficial builds of Mumble 1.3.0 and other products, mishandles OpenSSL's error queue, which can cause a denial of service to QSslSocket users. Because errors leak in unrelated TLS sessions, an unrelated session may be disconnected when any handshake fails. (Mumble 1.3.1 is not affected, regardless of the Qt version.)	7.5	More Details
CVE-2020-7010	Elastic Cloud on Kubernetes (ECK) versions prior to 1.1.0 generate passwords using a weak random number generator. If an attacker is able to determine when the current Elastic Stack cluster was deployed they may be able to more easily brute force the Elasticsearch credentials generated by ECK.	7.5	More Details
CVE-2020-13894	handler/upload_handler.jsp in DEXT5 Editor through 3.5.1402961 allows an attacker to download arbitrary files via the savefilepath field.	7.5	More Details
CVE-2020-3230	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent IKEv2 from establishing new security associations. The vulnerability is due to incorrect handling of crafted IKEv2 SA-Init packets. An attacker could exploit this vulnerability by sending crafted IKEv2 SA-Init packets to the affected device. An exploit could allow the attacker to cause the affected device to reach the maximum incoming negotiation limits and prevent further IKEv2 security associations from being formed.	7.5	More Details
CVE-2020-12723	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.	7.5	More Details
CVE-2020-13881	In support.c in pam_tacplus 1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used.	7.5	More Details
CVE-2020-13871	SQLite 3.32.2 has a use-after-free in resetAccumulator in select.c because the parse tree rewrite for window functions is too late.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9820	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5. A remote attacker may be able to modify the file system.	7.5	More Details
CVE-2020-9823	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5. Users removed from an iMessage conversation may still be able to alter state.	7.5	More Details
CVE-2020-13806	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a use-after-free because of JavaScript execution after a deletion or close operation.	7.5	More Details
CVE-2020-13807	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has circular reference mishandling that causes a loop.	7.5	More Details
CVE-2020-13432	rejetto HFS (aka HTTP File Server) v2.3m Build #300, when virtual files or folders are used, allows remote attackers to trigger an invalid-pointer write access violation via concurrent HTTP requests with a long URI or long HTTP headers.	7.5	More Details
CVE-2020-1214	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-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260.	7.5	More Details
CVE-2019-20834	An issue was discovered in Foxit PhantomPDF before 8.3.10. It allows signature validation bypass via a modified file or a file with non-standard signatures.	7.5	More Details
CVE-2019-20833	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has mishandling of cloud credentials, as demonstrated by Google Drive.	7.5	More Details
CVE-2019-20817	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	7.5	More Details
CVE-2019-20831	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.5.0.20733. It has void data mishandling, causing a crash.	7.5	More Details
CVE-2019-20829	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20828	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	7.5	More Details
CVE-2019-20826	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It has a NULL pointer dereference.	7.5	More Details
CVE-2019-20824	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	7.5	More Details
CVE-2019-20823	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	7.5	More Details
CVE-2019-20818	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows memory consumption because data is created for each page of an application level.	7.5	More Details
CVE-2020-13808	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via crafted cross-reference stream data.	7.5	More Details
CVE-2018-21240	An issue was discovered in Foxit Reader and PhantomPDF before 9.2. It allows memory consumption via an ArrayBuffer(0xfffffffe) call.	7.5	More Details
CVE-2019-20819	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows stack consumption via nested function calls for XML parsing.	7.5	More Details
CVE-2018-21238	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows memory consumption via an ArrayBuffer(0xfffffffe) call.	7.5	More Details
CVE-2020-1206	An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.	7.5	More Details
CVE-2018-21236	An issue was discovered in Foxit Reader before 2.4.4. It has a NULL pointer dereference.	7.5	More Details
CVE-2018-21235	An issue was discovered in Foxit E-mail advertising system before September 2018. It allows authentication bypass and information disclosure, related to Interspire Email Marketer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20820	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference during the parsing of file data.	7.5	More Details
CVE-2020-13815	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It allows stack consumption via a loop of an indirect object reference.	7.5	More Details
CVE-2019-20821	An issue was discovered in Foxit PhantomPDF Mac before 3.4. It has a NULL pointer dereference.	7.5	More Details
CVE-2020-1215	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-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260.	7.5	More Details
CVE-2019-20836	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has mishandling of cloud credentials, as demonstrated by Google Drive.	7.5	More Details
CVE-2019-20837	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It allows signature validation bypass via a modified file or a file with non-standard signatures.	7.5	More Details
CVE-2020-1216	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-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260.	7.5	More Details
CVE-2020-13809	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via long strings in the content stream.	7.5	More Details
CVE-2020-13810	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows signature validation bypass via a modified file or a file with non-standard signatures.	7.5	More Details
CVE-2020-13783	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Storage of Sensitive Information.	7.5	More Details
CVE-2019-20809	The price oracle in PriceOracle.sol in Compound Finance Compound Price Oracle 1.0 through 2.0 allows a price poster to set an invalid asset price via the setPrice function, and consequently violate the intended limits on price swings.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13849	The MQTT protocol 3.1.1 requires a server to set a timeout value of 1.5 times the Keep-Alive value specified by a client, which allows remote attackers to cause a denial of service (loss of the ability to establish new connections), as demonstrated by SlowITe.	7.5	More Details
CVE-2020-13848	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c.	7.5	More Details
CVE-2020-10644	The affected product lacks proper validation of user-supplied data, which can result in deserialization of untrusted data on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information.	7.5	More Details
CVE-2020-12000	The affected product is vulnerable to the handling of serialized data. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information.	7.5	More Details
CVE-2020-12004	The affected product lacks proper authentication required to query the server on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information.	7.5	More Details
CVE-2020-11957	The Bluetooth Low Energy implementation in Cypress PSoC Creator BLE 4.2 component versions before 3.64 generates a random number (Pairing Random) with significantly less entropy than the specified 128 bits during BLE pairing. This is the case for both authenticated and unauthenticated pairing with both LE Secure Connections as well as LE Legacy Pairing. A predictable or brute-forceable random number allows an attacker (in radio range) to perform a MITM attack during BLE pairing.	7.5	More Details
CVE-2019-20813	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	7.5	More Details
CVE-2020-1219	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'.	7.5	More Details
CVE-2019-20814	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows memory consumption because data is created for each page of an application level.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1213	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-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260.	7.5	More Details
CVE-2019-20815	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows stack consumption via nested function calls for XML parsing.	7.5	More Details
CVE-2019-20816	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference during the parsing of file data.	7.5	More Details
CVE-2020-13836	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. HWRResProvider allows path traversal for data exposure. The Samsung ID is SVE-2020-16954 (June 2020).	7.5	More Details
CVE-2020-13834	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (with TEEGRIS) software. Secure Folder does not properly restrict use of Android Debug Bridge (adb) for arbitrary installations. The Samsung ID is SVE-2020-17369 (June 2020).	7.5	More Details
CVE-2020-13830	An issue was discovered on Samsung mobile devices with P(9.0) software. One UI HOME logging can leak information. The Samsung ID is SVE-2019-16382 (June 2020).	7.5	More Details
CVE-2020-13829	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can disable the SEAndroid protection mechanism in the RKP. The Samsung ID is SVE-2019-15998 (June 2020).	7.5	More Details
CVE-2020-5304	The dashboard in WhiteSource Application Vulnerability Management (AVM) before version 20.4.1 allows Log Injection via a %0A%0D substring in the idp parameter to the /saml/login URI. This closes the current log and creates a new log with one line of data. The attacker can also insert malicious data and false entries.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4038	GraphQL Playground (graphql-playground-html NPM package) before version 1.6.22 have a severe XSS Reflection attack vulnerability. All unsanitized user input passed into renderPlaygroundPage() method could trigger this vulnerability. This has been patched in graphql-playground-html version 1.6.22. Note that some of the associated dependent middleware packages are also affected including but not limited to graphql-playground-middleware-express before version 1.7.16, graphql-playground-middleware-koa before version 1.6.15, graphql-playground-middleware-lambda before version 1.7.17, and graphql-playground-middleware-hapi before 1.6.13.	7.4	More Details
CVE-2020-4041	In Bolt CMS before version 3.7.1, the filename of uploaded files was vulnerable to stored XSS. It is not possible to inject javascript code in the file name when creating/uploading the file. But, once created/uploaded, it can be renamed to inject the payload in it. Additionally, the measures to prevent renaming the file to disallowed filename extensions could be circumvented. This is fixed in Bolt 3.7.1.	7.4	More Details
CVE-2020-8172	TLS session reuse can lead to host certificate verification bypass in node version < 12.18.0 and < 14.4.0.	7.4	More Details
CVE-2020-13817	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.	7.4	More Details
CVE-2020-13777	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application.	7.4	More Details
CVE-2020-4529	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 182713.	7.4	More Details
CVE-2020-4229	IBM Worklight/MobileFoundation 8.0.0.0 does not properly invalidate session cookies when a user logs out of a session, which could allow another user to gain unauthorized access to a user's session. IBM X-Force ID: 175211.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13912	SolarWinds Advanced Monitoring Agent before 10.8.9 allows local users to gain privileges via a Trojan horse .exe file, because everyone can write to a certain .exe file.	7.3	More Details
CVE-2020-3218	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code with root privileges on the underlying Linux shell. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by first creating a malicious file on the affected device itself and then uploading a second malicious file to the device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or bypass licensing requirements on the device.	7.2	More Details
CVE-2020-8103	A vulnerability in the improper handling of symbolic links in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects Bitdefender Antivirus Free versions prior to 1.0.17.178.	7.2	More Details
CVE-2020-7117	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	7.2	More Details
CVE-2020-7116	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	7.2	More Details
CVE-2020-3211	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker who has valid administrative access to an affected device could exploit this vulnerability by supplying a crafted input parameter on a form in the web UI and then submitting that form. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device, which could lead to complete system compromise.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3212	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by uploading a crafted file to the web UI of an affected device. A successful exploit could allow the attacker to inject and execute arbitrary commands with root privileges on the device.	7.2	More Details
CVE-2020-7013	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	7.2	More Details
CVE-2020-13978	Monstra CMS 3.0.4 allows an attacker, who already has administrative access to modify .chunk.php files on the Edit Chunk screen, to execute arbitrary OS commands via the Theme Module by visiting the admin/index.php?id=themes&action=edit_chunk URI. NOTE: there is no indication that the Edit Chunk feature was intended to prevent an administrator from using PHP's exec feature	7.2	More Details
CVE-2020-12847	Pydio Cells 2.0.4 web application offers an administrative console named “Cells Console” that is available to users with an administrator role. This console provides an administrator user with the possibility of changing several settings, including the application’s mailer configuration. It is possible to configure a few engines to be used by the mailer application to send emails. If the user selects the “sendmail” option as the default one, the web application offers to edit the full path where the sendmail binary is hosted. Since there is no restriction in place while editing this value, an attacker authenticated as an administrator user could force the web application into executing any arbitrary binary.	7.2	More Details
CVE-2020-9805	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting.	7.1	More Details
CVE-2020-1204	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9842	An entitlement parsing issue was addressed with improved parsing. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application could interact with system processes to access private information and perform privileged actions.	7.1	More Details
CVE-2020-13902	ImageMagick 7.0.9-27 through 7.0.10-17 has a heap-based buffer over-read in BlobToStringInfo in MagickCore/string.c during TIFF image decoding.	7.1	More Details
CVE-2020-1244	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-2020-1120.	7.1	More Details
CVE-2020-9843	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack.	7.1	More Details
CVE-2020-3267	A vulnerability in the API subsystem of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to change the availability state of any agent. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by authenticating to an affected system with valid agent credentials and performing a specific API call with crafted input. A successful exploit could allow the attacker to change the availability state of an agent, potentially causing a denial of service condition.	7.1	More Details
CVE-2020-9808	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2020-9839	A race condition was addressed with improved state handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to gain elevated privileges.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3220	A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle.	6.8	More Details
CVE-2020-3216	A vulnerability in Cisco IOS XE SD-WAN Software could allow an unauthenticated, physical attacker to bypass authentication and gain unrestricted access to the root shell of an affected device. The vulnerability exists because the affected software has insufficient authentication mechanisms for certain commands. An attacker could exploit this vulnerability by stopping the boot initialization of an affected device. A successful exploit could allow the attacker to bypass authentication and gain unrestricted access to the root shell of the affected device.	6.8	More Details
CVE-2020-10063	A remote adversary with the ability to send arbitrary CoAP packets to be parsed by Zephyr is able to cause a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	6.8	More Details
CVE-2020-3209	A vulnerability in software image verification in Cisco IOS XE Software could allow an unauthenticated, physical attacker to install and boot a malicious software image or execute unsigned binaries on an affected device. The vulnerability is due to an improper check on the area of code that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to install and boot a malicious software image or execute unsigned binaries on the targeted device.	6.8	More Details
CVE-2020-7456	In FreeBSD 12.1-STABLE before r361918, 12.1-RELEASE before p6, 11.4-STABLE before r361919, 11.3-RELEASE before p10, and 11.4-RC2 before p1, an invalid memory location may be used for HID items if the push/pop level is not restored within the processing of that HID item allowing an attacker with physical access to a USB port to be able to use a specially crafted USB device to gain kernel or user-space code execution.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12852	The update feature for Pydio Cells 2.0.4 allows an administrator user to set a custom update URL and the public RSA key used to validate the downloaded update package. The update process involves downloading the updated binary file from a URL indicated in the update server response, validating its checksum and signature with the provided public key and finally replacing the current application binary. To complete the update process, the application's service or appliance needs to be restarted. An attacker with administrator access can leverage the software update feature to force the application to download a custom binary that will replace current Pydio Cells binary. When the server or service is eventually restarted the attacker will be able to execute code under the privileges of the user running the application. In the Pydio Cells enterprise appliance this is with the privileges of the user named "pydio".	6.8	More Details
CVE-2020-3214	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	6.7	More Details
CVE-2020-3213	A vulnerability in the ROMMON of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to those of the root user of the underlying operating system. The vulnerability is due to the ROMMON allowing for special parameters to be passed to the device at initial boot up. An attacker could exploit this vulnerability by sending parameters to the device at initial boot up. An exploit could allow the attacker to elevate from a Priv15 user to the root user and execute arbitrary commands with the privileges of the root user.	6.7	More Details
CVE-2020-13883	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle.	6.7	More Details
CVE-2020-3208	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3207	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges.	6.7	More Details
CVE-2020-3204	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to cause memory corruption or execute the code with root privileges on the underlying OS of the affected device.	6.7	More Details
CVE-2020-3215	A vulnerability in the Virtual Services Container of Cisco IOS XE Software could allow an authenticated, local attacker to gain root-level privileges on an affected device. The vulnerability is due to insufficient validation of a user-supplied open virtual appliance (OVA). An attacker could exploit this vulnerability by installing a malicious OVA on an affected device.	6.7	More Details
CVE-2020-3210	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user.	6.7	More Details
CVE-2020-1258	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8337	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code.	6.7	More Details
CVE-2020-13776	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082.	6.7	More Details
CVE-2020-1253	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-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310.	6.7	More Details
CVE-2020-4190	IBM Security Guardium 10.6, 11.0, and 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174851.	6.7	More Details
CVE-2019-6196	A symbolic link vulnerability in some Lenovo installation packages, prior to version 1.2.9.3, could allow privileged file operations during file extraction and installation.	6.7	More Details
CVE-2020-1310	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-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1253.	6.7	More Details
CVE-2020-1251	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-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310.	6.7	More Details
CVE-2019-6173	A DLL search path vulnerability could allow privilege escalation in some Lenovo installation packages, prior to version 1.2.9.3, during installation if an attacker already has administrative privileges.	6.7	More Details
CVE-2020-9829	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted text message may lead to application denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1329	A spoofing vulnerability exists when Microsoft Bing Search for Android improperly handles specific HTML content, aka 'Microsoft Bing Search Spoofing Vulnerability'.	6.5	More Details
CVE-2020-11680	Castel NextGen DVR v1.0.0 is vulnerable to authorization bypass on all administrator functionality. The application fails to check that a request was submitted by an administrator. Consequently, a normal user can perform actions including, but not limited to, creating/modifying the file store, creating/modifying alerts, creating/modifying users, etc.	6.5	More Details
CVE-2020-13868	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. CSRF affects comment integrity.	6.5	More Details
CVE-2020-1322	An information disclosure vulnerability exists when Microsoft Project reads out of bound memory due to an uninitialized variable, aka 'Microsoft Project Information Disclosure Vulnerability'.	6.5	More Details
CVE-2020-6495	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	6.5	More Details
CVE-2019-16384	Cybele Thinfinity VirtualUI 2.5.17.2 allows ../ path traversal that can be used for data exfiltration. This enables files outside of the web directory to be retrieved if the exact location is known and the user has permissions.	6.5	More Details
CVE-2020-11682	Castel NextGen DVR v1.0.0 is vulnerable to CSRF in all state-changing request. A __RequestVerificationToken is set by the web interface, and included in requests sent by web interface. However, this token is not verified by the application: the token can be removed from all requests and the request will succeed.	6.5	More Details
CVE-2020-6494	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2011-2863	Insufficient policy enforcement in V8 in Google Chrome prior to 14.0.0.0 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2020-1232	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1348	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.	6.5	More Details
CVE-2020-6497	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted URI.	6.5	More Details
CVE-2020-2198	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not redact encrypted secrets in the 'getConfigAsXML' API URL when transmitting job config.xml data to users without Job/Configure.	6.5	More Details
CVE-2020-6500	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2020-3882	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.5. Importing a maliciously crafted calendar invitation may exfiltrate user information.	6.5	More Details
CVE-2020-6503	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2020-6499	Inappropriate implementation in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-6501	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	6.5	More Details
CVE-2020-6502	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details
CVE-2020-1283	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.	6.5	More Details
CVE-2020-4307	IBM Security Guardium 11.1 could allow an attacker on the same network to gain access to the Solr dashboard and cause a denial of service attack. IBM X-Force ID: 176997.	6.5	More Details
CVE-2020-1284	A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Denial of Service Vulnerability'.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12803	ODF documents can contain forms to be filled out by the user. Similar to HTML forms, the contained form data can be submitted to a URI, for example, to an external web server. To create submittable forms, ODF implements the XForms W3C standard, which allows data to be submitted without the need for macros or other active scripting Prior to version 6.4.4 LibreOffice allowed forms to be submitted to any URI, including file: URIs, enabling form submissions to overwrite local files. User-interaction is required to submit the form, but to avoid the possibility of malicious documents engineered to maximize the possibility of inadvertent user submission this feature has now been limited to http[s] URIs, removing the possibility to overwrite local files. This issue affects: The Document Foundation LibreOffice versions prior to 6.4.4.	6.5	More Details
CVE-2020-6498	Incorrect implementation in user interface in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	6.5	More Details
CVE-2018-21243	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has COM object mishandling when Microsoft Word is used.	6.5	More Details
CVE-2020-2192	A cross-site request forgery vulnerability in Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier allows attackers to add or remove agent labels.	6.5	More Details
CVE-2020-8321	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	6.4	More Details
CVE-2020-8320	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege.	6.4	More Details
CVE-2020-8322	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	6.4	More Details
CVE-2020-8323	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	6.4	More Details
CVE-2020-8336	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8555	The Kubernetes kube-controller-manager in versions v1.0-1.14, versions prior to v1.15.12, v1.16.9, v1.17.5, and version v1.18.0 are vulnerable to a Server Side Request Forgery (SSRF) that allows certain authorized users to leak up to 500 bytes of arbitrary information from unprotected endpoints within the master's host network (such as link-local or loopback services).	6.3	More Details
CVE-2020-3237	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, local attacker to overwrite arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by including a crafted file in an application package. An exploit could allow the attacker to overwrite files.	6.3	More Details
CVE-2020-5296	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to delete arbitrary local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	6.2	More Details
CVE-2020-4182	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174738.	6.1	More Details
CVE-2020-2199	Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier does not escape the error message for the repository URL field form validation, resulting in a reflected cross-site scripting vulnerability.	6.1	More Details
CVE-2020-13596	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. Query parameters generated by the Django admin ForeignKeyRawIdWidget were not properly URL encoded, leading to a possibility of an XSS attack.	6.1	More Details
CVE-2020-1220	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11094	The October CMS debugbar plugin before version 3.1.0 contains a feature where it will log all requests (and all information pertaining to each request including session data) whenever it is enabled. This presents a problem if the plugin is ever enabled on a system that is open to untrusted users as the potential exists for them to use this feature to view all requests being made to the application and obtain sensitive information from those requests. There even exists the potential for account takeovers of authenticated users by non-authenticated public users, which would then lead to a number of other potential issues as an attacker could theoretically get full access to the system if the required conditions existed. Issue has been patched in v3.1.0 by locking down access to the debugbar to all users; it now requires an authenticated backend user with a specifically enabled permission before it is even usable, and the feature that allows access to stored request information is restricted behind a different permission that's more restrictive.	6.1	More Details
CVE-2019-16385	Cybele Thinfinity VirtualUI 2.5.17.2 allows HTTP response splitting via the mimetype parameter within a PDF viewer request, as demonstrated by an example.pdf?mimetype= substring. The victim user must load an application request to view a PDF, containing the malicious payload. This results in a reflected XSS payload being executed.	6.1	More Details
CVE-2020-11697	In Combodo iTop, dashboard ids can be exploited with a reflective XSS payload. This is fixed in all iTop packages (community, essential, professional) for version 2.7.0 and in iTop essential and iTop professional packages for version 2.6.4.	6.1	More Details
CVE-2020-13897	HESK before 3.1.10 allows reflected XSS.	6.1	More Details
CVE-2020-8334	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access.	6.1	More Details
CVE-2020-11696	In Combodo iTop a menu shortcut name can be exploited with a stored XSS payload. This is fixed in all iTop packages (community, essential, professional) in version 2.7.0 and iTop essential and iTop professional in version 2.6.4.	6.1	More Details
CVE-2020-12853	Pydio Cells 2.0.4 allows XSS. A malicious user can either upload or create a new file that contains potentially malicious HTML and JavaScript code to personal folders or accessible cells.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13797	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/websites/website.class.php.	6.1	More Details
CVE-2020-13973	OWASP json-sanitizer before 1.2.1 allows XSS. An attacker who controls a substring of the input JSON, and controls another substring adjacent to a SCRIPT element in which the output is embedded as JavaScript, may be able to confuse the HTML parser as to where the SCRIPT element ends, and cause non-script content to be interpreted as JavaScript.	6.1	More Details
CVE-2020-13965	An issue was discovered in Roundcube Webmail before 1.3.12 and 1.4.x before 1.4.5. There is XSS via a malicious XML attachment because text/xml is among the allowed types for a preview.	6.1	More Details
CVE-2020-13796	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/structure/structure.class.php.	6.1	More Details
CVE-2020-1323	An open redirect vulnerability exists in Microsoft SharePoint that could lead to spoofing.To exploit the vulnerability, an attacker could send a link that has a specially crafted URL and convince the user to click the link, aka 'SharePoint Open Redirect Vulnerability'.	6.1	More Details
CVE-2020-13964	An issue was discovered in Roundcube Webmail before 1.3.12 and 1.4.x before 1.4.5. include/rcmail_output_html.php allows XSS via the username template object.	6.1	More Details
CVE-2020-4183	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174739.	6.1	More Details
CVE-2020-13827	phpList before 3.5.4 allows XSS via /lists/admin/user.php and /lists/admin/users.php.	6.1	More Details
CVE-2020-13798	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/feeds/feed.class.php.	6.1	More Details
CVE-2020-1327	A spoofing vulnerability exists in Microsoft Azure DevOps Server when it fails to properly handle web requests, aka 'Azure DevOps Server HTML Injection Vulnerability'.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7011	Elastic App Search versions before 7.7.0 contain a cross site scripting (XSS) flaw when displaying document URLs in the Reference UI. If the Reference UI injects a URL into a result, that URL will be rendered by the web browser. If an attacker is able to control the contents of such a field, they could execute arbitrary JavaScript in the victimï¿½s web browser.	6.1	More Details
CVE-2020-3201	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	6.0	More Details
CVE-2020-10749	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious containers in Kubernetes clusters to perform man-in-the-middle (MitM) attacks. A malicious container can exploit this flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container.	6.0	More Details
CVE-2020-13597	Clusters using Calico (version 3.14.0 and below), Calico Enterprise (version 2.8.2 and below), may be vulnerable to information disclosure if IPv6 is enabled but unused. A compromised pod with sufficient privilege is able to reconfigure the node's IPv6 interface due to the node accepting route advertisement by default, allowing the attacker to redirect full or partial network traffic from the node to the compromised pod.	6.0	More Details
CVE-2020-13800	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value during an ati_mm_read or ati_mm_write call.	6.0	More Details
CVE-2020-3353	A vulnerability in the syslog processing engine of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a race condition that may occur when syslog messages are processed. An attacker could exploit this vulnerability by sending a high rate of syslog messages to an affected device. A successful exploit could allow the attacker to cause the Application Server process to crash, resulting in a DoS condition.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13254	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage.	5.9	More Details
CVE-2020-4035	In WatermelonDB (NPM package "@nozbe/watermelondb") before versions 0.15.1 and 0.16.2, a maliciously crafted record ID can exploit a SQL Injection vulnerability in iOS adapter implementation and cause the app to delete all or selected records from the database, generally causing the app to become unusable. This may happen in apps that don't validate IDs (valid IDs are `/^[a-zA-Z0-9_-.]+$/`) and use Watermelon Sync or low-level `database.adapter.destroyDeletedRecords` method. The integrity risk is low due to the fact that maliciously deleted records won't synchronize, so logout-login will restore all data, although some local changes may be lost if the malicious deletion causes the sync process to fail to proceed to push stage. No way to breach confidentiality with this vulnerability is known. Full exploitation of SQL Injection is mitigated, because it's not possible to nest an insert/update query inside a delete query in SQLite, and it's not possible to pass a semicolon-separated second query. There's also no known practicable way to breach confidentiality by selectively deleting records, because those records will not be synchronized. It's theoretically possible that selective record deletion could cause an app to behave insecurely if lack of a record is used to make security decisions by the app. This is patched in versions 0.15.1, 0.16.2, and 0.16.1-fix	5.9	More Details
CVE-2020-1343	An information disclosure vulnerability exists in Visual Studio Code Live Share Extension when it exposes tokens in plain text, aka 'Visual Studio Code Live Share Information Disclosure Vulnerability'.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11091	In Weave Net before version 2.6.3, an attacker able to run a process as root in a container is able to respond to DNS requests from the host and thereby insert themselves as a fake service. In a cluster with an IPv4 internal network, if IPv6 is not totally disabled on the host (via ipv6.disable=1 on the kernel cmdline), it will be either unconfigured or configured on some interfaces, but it's pretty likely that ipv6 forwarding is disabled, ie /proc/sys/net/ipv6/conf//forwarding == 0. Also by default, /proc/sys/net/ipv6/conf//accept_ra == 1. The combination of these 2 sysctls means that the host accepts router advertisements and configure the IPv6 stack using them. By sending rogue router advertisements, an attacker can reconfigure the host to redirect part or all of the IPv6 traffic of the host to the attacker controlled container. Even if there was no IPv6 traffic before, if the DNS returns A (IPv4) and AAAA (IPv6) records, many HTTP libraries will try to connect via IPv6 first then fallback to IPv4, giving an opportunity to the attacker to respond. If by chance you also have on the host a vulnerability like last year's RCE in apt (CVE-2019-3462), you can now escalate to the host. Weave Net version 2.6.3 disables the accept_ra option on the veth devices that it creates.	5.8	More Details
CVE-2020-13765	rom_copy() in hw/core/loader.c in QEMU 4.0 and 4.1.0 does not validate the relationship between two addresses, which allows attackers to trigger an invalid memory copy operation.	5.6	More Details
CVE-2020-1290	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1268	An information disclosure vulnerability exists when a Windows service improperly handles objects in memory, aka 'Windows Service Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1263	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261.	5.5	More Details
CVE-2020-1261	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1263.	5.5	More Details
CVE-2020-1296	A vulnerability exists in the way the Windows Diagnostics & feedback settings app handles objects in memory, aka 'Windows Diagnostics & feedback Information Disclosure Vulnerability'.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20810	go7007_snd_init in drivers/media/usb/go7007/snd-go7007.c in the Linux kernel before 5.6 does not call snd_card_free for a failure path, which causes a memory leak, aka CID-9453264ef586.	5.5	More Details
CVE-2020-1194	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'.	5.5	More Details
CVE-2020-9831	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2020-10702	A flaw was found in QEMU in the implementation of the Pointer Authentication (PAuth) support for ARM introduced in version 4.0 and fixed in version 5.0.0. A general failure of the signature generation process caused every PAuth-enforced pointer to be signed with the same signature. A local attacker could obtain the signature of a protected pointer and abuse this flaw to bypass PAuth protection for all programs running on QEMU.	5.5	More Details
CVE-2020-13791	hw/pci/pci.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access by providing an address near the end of the PCI configuration space.	5.5	More Details
CVE-2020-13843	An issue was discovered on LG mobile devices with Android OS software before 2020-06-01. Local users can cause a denial of service because checking of the userdata partition is mishandled. The LG ID is LVE-SMP-200014 (June 2020).	5.5	More Details
CVE-2019-16150	Use of a hard-coded cryptographic key to encrypt security sensitive data in local storage and configuration in FortiClient for Windows prior to 6.4.0 may allow an attacker with access to the local storage or the configuration backup file to decrypt the sensitive data via knowledge of the hard-coded key.	5.5	More Details
CVE-2020-7030	A sensitive information disclosure vulnerability was discovered in the web interface component of IP Office that may potentially allow a local user to gain unauthorized access to the component. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 though 11.0.4.3.	5.5	More Details
CVE-2020-13867	Open-iSCSI targetcli-fb through 2.1.52 has weak permissions for /etc/target (and for the backup directory and backup files).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13904	FFmpeg 2.8 and 4.2.3 has a use-after-free via a crafted EXTINF duration in an m3u8 file because parse_playlist in libavformat/hls.c frees a pointer, and later that pointer is accessed in av_probe_input_format3 in libavformat/format.c.	5.5	More Details
CVE-2020-12049	An issue was discovered in dbus >= 1.3.0 before 1.12.18. The DBusServer in libdbus, as used in dbus-daemon, leaks file descriptors when a message exceeds the per-message file descriptor limit. A local attacker with access to the D-Bus system bus or another system service's private AF_UNIX socket could use this to make the system service reach its file descriptor limit, denying service to subsequent D-Bus clients.	5.5	More Details
CVE-2020-3335	A vulnerability in the key store of Cisco Application Services Engine Software could allow an authenticated, local attacker to read sensitive information of other users on an affected device. The vulnerability is due to insufficient authorization limitations. An attacker could exploit this vulnerability by logging in to an affected device locally with valid credentials. A successful exploit could allow the attacker to read the sensitive information of other users on the affected device.	5.5	More Details
CVE-2020-9797	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine another application's memory layout.	5.5	More Details
CVE-2020-9809	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2020-9811	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory.	5.5	More Details
CVE-2020-9812	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory.	5.5	More Details
CVE-2020-13844	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation."	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9833	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.5. A local user may be able to read kernel memory.	5.5	More Details
CVE-2020-9832	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2020-1160	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-9851	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2020-1120	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-2020-1244.	5.5	More Details
CVE-2019-20811	An issue was discovered in the Linux kernel before 5.0.6. In rx_queue_add_kobject() and netdev_queue_add_kobject() in net/core/net-sysfs.c, a reference count is mishandled, aka CID-a3e23f719f5c.	5.5	More Details
CVE-2019-20812	An issue was discovered in the Linux kernel before 5.4.7. The prb_calc_retire_blk_tmo() function in net/packet/af_packet.c can result in a denial of service (CPU consumption and soft lockup) in a certain failure case involving TPACKET_V3, aka CID-b43d1f9f7067.	5.5	More Details
CVE-2020-2194	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the display name of the builds in the trend chart, resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2020-13869	An issue was discovered in the Comments plugin before 1.5.6 for Craft CMS. There is stored XSS via a guest name.	5.4	More Details
CVE-2020-13889	showAlert() in the administration panel in Bludit 3.12.0 allows XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13865	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from multiple stored XSS vulnerabilities. An author user can create posts that result in stored XSS vulnerabilities, by using a crafted link in the custom URL or by applying custom attributes.	5.4	More Details
CVE-2020-13864	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from a stored XSS vulnerability. An author user can create posts that result in a stored XSS by using a crafted payload in custom links.	5.4	More Details
CVE-2020-13870	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. There is stored XSS via an asset volume name.	5.4	More Details
CVE-2020-13911	Your Online Shop 1.8.0 allows authenticated users to trigger XSS via a Change Name or Change Surname operation.	5.4	More Details
CVE-2020-13892	The SportsPress plugin before 2.7.2 for WordPress allows XSS.	5.4	More Details
CVE-2020-1297	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-2020-1177, CVE-2020-1183, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320.	5.4	More Details
CVE-2020-6640	An improper neutralization of input vulnerability in the Admin Profile of FortiAnalyzer may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Description Area.	5.4	More Details
CVE-2020-12849	Pydio Cells 2.0.4 allows any user to upload a profile image to the web application, including standard and shared user roles. These profile pictures can later be accessed directly with the generated URL by any unauthenticated or authenticated user.	5.4	More Details
CVE-2020-12848	In Pydio Cells 2.0.4, once an authenticated user shares a file selecting the create a public link option, a hidden shared user account is created in the backend with a random username. An anonymous user that obtains a valid public link can get the associated hidden account username and password and proceed to login to the web application. Once logged into the web application with the hidden user account, some actions that were not available with the public share link can now be performed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1148	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-2020-1289.	5.4	More Details
CVE-2020-1183	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-2020-1177, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320.	5.4	More Details
CVE-2020-1177	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-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320.	5.4	More Details
CVE-2020-13890	The Neon theme 2.0 before 2020-06-03 for Bootstrap allows XSS via an Add Task Input operation in a dashboard.	5.4	More Details
CVE-2020-1298	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-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1318, CVE-2020-1320.	5.4	More Details
CVE-2020-7676	angular.js prior to 1.8.0 allows cross site scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one. Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code.	5.4	More Details
CVE-2020-1320	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-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318.	5.4	More Details
CVE-2020-2193	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the parser identifier when rendering charts, resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2020-2195	Jenkins Compact Columns Plugin 1.11 and earlier displays the unprocessed job description in tooltips, resulting in a stored cross-site scripting vulnerability that can be exploited by users with Job/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1340	A spoofing vulnerability exists when the NuGetGallery does not properly sanitize input on package metadata values, aka 'NuGetGallery Spoofing Vulnerability'.	5.4	More Details
CVE-2020-2190	Jenkins Script Security Plugin 1.72 and earlier does not correctly escape pending or approved classpath entries on the In-process Script Approval page, resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2020-1331	A spoofing vulnerability exists when System Center Operations Manager (SCOM) does not properly sanitize a specially crafted web request to an affected SCOM instance, aka 'System Center Operations Manager Spoofing Vulnerability'.	5.4	More Details
CVE-2020-1318	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-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1320.	5.4	More Details
CVE-2020-3233	A vulnerability in the web-based Local Manager interface of the Cisco IOx Application Framework could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based Local Manager interface of an affected device. The attacker must have valid Local Manager credentials. The vulnerability is due to insufficient validation of user-supplied input by the web-based Local Manager interface of the affected software. An attacker could exploit this vulnerability by injecting malicious code into a system settings tab. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information.	5.4	More Details
CVE-2020-8954	OpenSearch Web browser 1.0.4.9 allows Intent Scheme Hijacking.[a link that opens another app in the browser can be manipulated]	5.4	More Details
CVE-2020-7015	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3339	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	5.4	More Details
CVE-2020-1289	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-2020-1148.	5.4	More Details
CVE-2020-1315	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'.	5.3	More Details
CVE-2020-13795	An issue was discovered in Navigate CMS through 2.8.7. It allows Directory Traversal because lib/packages/templates/template.class.php mishandles ../ and ..\ substrings.	5.3	More Details
CVE-2018-21239	An issue was discovered in Foxit Reader and PhantomPDF before 9.2. It allows NTLM credential theft via a GoToE or GoToR action.	5.3	More Details
CVE-2020-3333	A vulnerability in the API of Cisco Application Services Engine Software could allow an unauthenticated, remote attacker to update event policies on an affected device. The vulnerability is due to insufficient authentication of users who modify policies on an affected device. An attacker could exploit this vulnerability by crafting a malicious HTTP request to contact an affected device. A successful exploit could allow the attacker to update event policies on the affected device.	5.3	More Details
CVE-2020-4187	IBM Security Guardium 11.1 could disclose sensitive information on the login page that could aid in further attacks against the system. IBM X-Force ID: 174805.	5.3	More Details
CVE-2018-21237	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows NTLM credential theft via a GoToE or GoToR action.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12802	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed where remote graphic links loaded from docx documents were omitted from this protection prior to version 6.4.4. This issue affects: The Document Foundation LibreOffice versions prior to 6.4.4.	5.3	More Details
CVE-2020-9835	An issue existed in the pausing of FaceTime video. The issue was resolved with improved logic. This issue is fixed in iOS 13.5 and iPadOS 13.5. A user’s video may not be paused in a FaceTime call if they exit the FaceTime app while the call is ringing.	5.3	More Details
CVE-2020-9856	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.5. An application may be able to gain elevated privileges.	5.3	More Details
CVE-2020-1242	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.	5.3	More Details
CVE-2020-9801	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1.1. A malicious process may cause Safari to launch an application.	5.3	More Details
CVE-2020-9074	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones.	5.3	More Details
CVE-2020-10068	In the Zephyr project Bluetooth subsystem, certain duplicate and back-to-back packets can cause incorrect behavior, resulting in a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	5.1	More Details
CVE-2020-10761	An assertion failure issue was found in the Network Block Device(NBD) Server in all QEMU versions before QEMU 5.0.1. This flaw occurs when an nbd-client sends a spec-compliant request that is near the boundary of maximum permitted request length. A remote nbd-client could use this flaw to crash the qemu-nbd server resulting in a denial of service.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3223	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the filesystem and then accessing it through the web UI. An exploit could allow the attacker to read arbitrary files from the underlying operating system's filesystem.	4.9	More Details
CVE-2020-13977	Nagios 4.4.5 allows an attacker, who already has administrative access to change the "URL for JSON CGIs" configuration setting, to modify the Alert Histogram and Trends code via crafted versions of the archivejson.cgi, objectjson.cgi, and statusjson.cgi files. NOTE: this vulnerability has been mistakenly associated with CVE-2020-1408.	4.9	More Details
CVE-2020-1883	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal.	4.9	More Details
CVE-2020-13980	OpenCart 3.0.3.3 allows remote authenticated users to conduct XSS attacks via a crafted filename in the users' image upload section because of a lack of entity encoding. NOTE: this issue exists because of an incomplete fix for CVE-2020-10596. The vendor states "this is not a massive issue as you are still required to be logged into the admin.	4.8	More Details
CVE-2020-5295	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to read local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	4.8	More Details
CVE-2020-3231	A vulnerability in the 802.1X feature of Cisco Catalyst 2960-L Series Switches and Cisco Catalyst CDB-8P Switches could allow an unauthenticated, adjacent attacker to forward broadcast traffic before being authenticated on the port. The vulnerability exists because broadcast traffic that is received on the 802.1X-enabled port is mishandled. An attacker could exploit this vulnerability by sending broadcast traffic on the port before being authenticated. A successful exploit could allow the attacker to send and receive broadcast traffic on the 802.1X-enabled port before authentication.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3206	A vulnerability in the handling of IEEE 802.11w Protected Management Frames (PMFs) of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to terminate a valid user connection to an affected device. The vulnerability exists because the affected software does not properly validate 802.11w disassociation and deauthentication PMFs that it receives. An attacker could exploit this vulnerability by sending a spoofed 802.11w PMF from a valid, authenticated client on a network adjacent to an affected device. A successful exploit could allow the attacker to terminate a single valid user connection to the affected device.	4.7	More Details
CVE-2019-19412	Huawei smart phones have a Factory Reset Protection (FRP) bypass security vulnerability. When re-configuring the mobile phone using the factory reset protection (FRP) function, an attacker login the Talkback mode and can perform some operations to install a third-Party application. Affected products can be found in https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200115-01-frp-en.	4.6	More Details
CVE-2020-9804	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.5. Inserting a USB device that sends invalid messages may cause a kernel panic.	4.6	More Details
CVE-2020-9792	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A USB device may be able to cause a denial of service.	4.6	More Details
CVE-2020-4191	IBM Security Guardium 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174852.	4.4	More Details
CVE-2020-13696	An issue was discovered in LinuxTV xawtv before 3.107. The function dev_open() in v4l-conf.c does not perform sufficient checks to prevent an unprivileged caller of the program from opening unintended filesystem paths. This allows a local attacker with access to the v4l-conf setuid-root program to test for the existence of arbitrary files and to trigger an open on arbitrary files with mode O_RDWR. To achieve this, relative path components need to be added to the device path, as demonstrated by a v4l-conf -c /dev/../root/.bash_history command.	4.4	More Details
CVE-2020-2197	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not require users to have Job/ExtendedRead permission to access Inheritance Project job configurations in XML format.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13266	Insecure authorization in Project Deploy Keys in GitLab CE/EE 12.8 and later through 13.0.1 allows users to update permissions of other users' deploy keys under certain conditions	4.3	More Details
CVE-2020-9819	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5, watchOS 5.3.7. Processing a maliciously crafted mail message may lead to heap corruption.	4.3	More Details
CVE-2020-2191	Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier does not check permissions on API endpoints that allow adding and removing agent labels.	4.3	More Details
CVE-2020-1229	A security feature bypass vulnerability exists in Microsoft Outlook when Office fails to enforce security settings configured on a system, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'.	4.3	More Details
CVE-2020-3222	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass access control restrictions on an affected device. The vulnerability is due to the presence of a proxy service at a specific endpoint of the web UI. An attacker could exploit this vulnerability by connecting to the proxy service. An exploit could allow the attacker to bypass access restrictions on the network by proxying their access request through the management network of the affected device. As the proxy is reached over the management virtual routing and forwarding (VRF), this could reduce the effectiveness of the bypass.	4.3	More Details
CVE-2019-20832	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has homograph mishandling.	4.3	More Details
CVE-2019-20835	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has homograph mishandling.	4.3	More Details
CVE-2020-10754	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely.	4.3	More Details
CVE-2020-1259	A security feature bypass vulnerability exists when Windows Host Guardian Service improperly handles hashes recorded and logged, aka 'Windows Host Guardian Service Security Feature Bypass Vulnerability'.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13792	PlayTube 1.8 allows disclosure of user details via ajax.php?type=../admin-panel/autoload&page=manage-users directory traversal, aka local file inclusion.	4.3	More Details
CVE-2020-9462	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks.	4.3	More Details
CVE-2020-4026	The CustomAppsRestResource list resource in Atlassian Navigator Links before version 3.3.23, from version 4.0.0 before version 4.3.7, from version 5.0.0 before 5.0.1, and from version 5.1.0 before 5.1.1 allows remote attackers to enumerate all linked applications, including those that are restricted or otherwise hidden, through an incorrect authorization check.	4.3	More Details
CVE-2020-6504	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass notification restrictions via a crafted HTML page.	4.3	More Details
CVE-2020-5299	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, any users with the ability to modify any data that could eventually be exported as a CSV file from the `ImportExportController` could potentially introduce a CSV injection into the data to cause the generated CSV export file to be malicious. This requires attackers to achieve the following before a successful attack can be completed: 1. Have found a vulnerability in the victims spreadsheet software of choice. 2. Control data that would potentially be exported through the `ImportExportController` by a theoretical victim. 3. Convince the victim to export above data as a CSV and run it in vulnerable spreadsheet software while also bypassing any sanity checks by said software. Issue has been patched in Build 466 (v1.0.466).	4.0	More Details
CVE-2020-5298	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, a user with the ability to use the import functionality of the `ImportExportController` behavior can be socially engineered by an attacker to upload a maliciously crafted CSV file which could result in a reflected XSS attack on the user in question Issue has been patched in Build 466 (v1.0.466).	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11080	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.	3.7	More Details
CVE-2020-1775	BCC recipients in mails sent from OTRS are visible in article detail on external interface. This issue affects OTRS: 8.0.3 and prior versions, 7.0.17 and prior versions.	3.5	More Details
CVE-2020-13837	An issue was discovered on Samsung mobile devices with Q(10.0) software. The Lockscreen feature does not block Quick Panel access to Music Share. The Samsung ID is SVE-2020-17145 (June 2020).	3.5	More Details
CVE-2020-13838	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. The DeX Lockscreen feature does not block access to Quick Panel and notifications. The Samsung ID is SVE-2020-17187 (June 2020).	3.5	More Details
CVE-2020-5297	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	3.4	More Details
CVE-2020-3319	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3321	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.	3.3	More Details
CVE-2020-3322	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.	3.3	More Details
CVE-2020-9848	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5. A person with physical access to an iOS device may be able to view notification contents from the lockscreen.	2.4	More Details
CVE-2019-19213	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 in customer-controlled software. Notes: none	N/A	More Details
CVE-2020-1703	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: Red Hat Product Security does not consider this as a security flaw. Password changes aren't expected to invalidate existing sessions. Though this is how Kerberos behaves: incrementing kvno will not invalidate any existing service tickets. This is not a concern because the lifetime on service tickets should be set appropriately (initially only a global, now also more finely configurable with the kdcpolicy plugin). This belief is reinforced by our use of mod_session: existing sessions there aren't terminated, but instead wait for expiration	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19214	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 in customer-controlled software. Notes: none	N/A	More Details
CVE-2020-13816	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-13817. Reason: This candidate is a reservation duplicate of CVE-2020-13817. Notes: All CVE users should reference CVE-2020-13817 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-8331	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details