SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 October 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-2020-6364	SAP Solution Manager and SAP Focused Run (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7), allows an attacker to modify a cookie in a way that OS commands can be executed and potentially gain control over the host running the CA Introscope Enterprise Manager,leading to Code Injection. With this, the attacker is able to read and modify all system files and also impact system availability.	10.0	More Details
CVE-2020-26943	An issue was discovered in OpenStack blazar-dashboard before 1.3.1, 2.0.0, and 3.0.0. A user allowed to access the Blazar dashboard in Horizon may trigger code execution on the Horizon host as the user the Horizon service runs under (because the Python eval function is used). This may result in Horizon host unauthorized access and further compromise of the Horizon service. All setups using the Horizon dashboard with the blazar-dashboard plugin are affected.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7143	A faultdevparasset expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7152	A faultparasset expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7157	A selviewnavcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7156	A faultinfo_content expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7155	A select expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7154	A ifviewselectpage expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7153	A iccselectdevtype expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7151	A faulttrapgroupselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7159	A customtemplateselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7150	A faultstatchoosefaulttype expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7149	A ictexpertcsvdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7148	A deployselectsoftware expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7147	A deployselectbootrom expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7146	A devgroupselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7158	A perfselecttask expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7161	A reporttaskselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7160	A iccselectdeviceseries expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7144	A comparefilesresult expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7162	A operatorgroupselectcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7163	A navigationto expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7164	A operationselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7165	A iccselectcommand expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7166	A operatorgrouptreeselectcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7167	A quicktemplateselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7168	A selectusergroup expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7169	A ictexpertcsvdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7170	A select expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7171	A guidatadetail expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7172	A templateselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-5640	Local file inclusion vulnerability in OneThird CMS v1.96c and earlier allows a remote unauthenticated attacker to execute arbitrary code or obtain sensitive information via unspecified vectors.	9.8	More Details
CVE-2020-7145	A chooseperfview expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-3992	OpenSLP as used in VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202010401-SG, 6.5 before ESXi650-202010401-SG) has a use-after-free issue. A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger a use-after-free in the OpenSLP service resulting in remote code execution.	9.8	More Details
CVE-2020-9864	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with kernel privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27197	TAXII libtaxii through 1.1.117, as used in EclecticIQ OpenTAXII through 0.2.0 and other products, allows SSRF via an initial http:// substring to the parse method, even when the no_network setting is used for the XML parser. NOTE: the vendor points out that the parse method "wraps the lxml library" and that this may be an issue to "raise ... to the lxml group.	9.8	More Details
CVE-2020-27156	Veritas APTARE versions prior to 10.5 did not perform adequate authorization checks. This vulnerability could allow for remote code execution by an unauthenticated user.	9.8	More Details
CVE-2020-4499	IBM Security Access Manager 9.0.7 and IBM Security Verify Access 10.0.0 could allow an unauthorized public Oauth client to bypass some or all of the authentication checks and gain access to applications. IBM X-Force ID: 182216.	9.8	More Details
CVE-2020-12500	Improper Authorization vulnerability of Pepperl+Fuchs P+F Comtrol RocketLinx ES7510-XT, ES8509-XT, ES8510-XT, ES9528-XTv2, ES7506, ES7510, ES7528, ES8508, ES8508F, ES8510, ES8510-XTE, ES9528/ES9528-XT (all versions) allows unauthenticated device administration.	9.8	More Details
CVE-2020-12501	Improper Authorization vulnerability of Pepperl+Fuchs P+F Comtrol RocketLinx ES7510-XT, ES8509-XT, ES8510-XT, ES9528-XTv2, ES7506, ES7510, ES7528, ES8508, ES8508F, ES8510, ES8510-XTE, ES9528/ES9528-XT (all versions) use undocumented accounts.	9.8	More Details
CVE-2020-12504	Improper Authorization vulnerability of Pepperl+Fuchs P+F Comtrol RocketLinx ES7510-XT, ES8509-XT, ES8510-XT, ES9528-XTv2, ES7506, ES7510, ES7528, ES8508, ES8508F, ES8510, ES8510-XTE, ES9528/ES9528-XT (all versions) and ICRL-M-8RJ45/4SFP-G-DIN, ICRL-M-16RJ45/4CP-G-DIN FW 1.2.3 and below has an active TFTP-Service.	9.8	More Details
CVE-2019-17640	In Eclipse Vert.x 3.4.x up to 3.9.4, 4.0.0.milestone1, 4.0.0.milestone2, 4.0.0.milestone3, 4.0.0.milestone4, 4.0.0.milestone5, 4.0.0.Beta1, 4.0.0.Beta2, and 4.0.0.Beta3, StaticHandler doesn't correctly processes back slashes on Windows Operating systems, allowing, escape the webroot folder to the current working directory.	9.8	More Details
CVE-2019-19513	The BASSMIDI plugin 2.4.12.1 for Un4seen BASS Audio Library on Windows is prone to an out of bounds write vulnerability. An attacker may exploit this to execute code on the target machine. A failure in exploitation leads to a denial of service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26944	An issue was discovered in Aptean Product Configurator 4.61.0000 on Windows. A Time based SQL injection affects the nameTxt parameter on the main login page (aka cse?cmd=LOGIN). This can be exploited directly, and remotely.	9.8	More Details
CVE-2020-7142	A eventinfo_content expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-9895	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details
CVE-2020-9918	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	9.8	More Details
CVE-2020-24629	A remote urlaccesscontroller authentication bypass vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-24646	A tftpserver stack-based buffer overflow remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-24647	A remote accessmgrservlet classname input validation code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-24648	A accessmgrservlet classname deserialization of untrusted data remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-24649	A remote bytemessageresource transformentity" input validation code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-24650	A legend expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24651	A syslogtempletselectwin expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-24652	A addvsiinterfaceinfo expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-7141	A adddevicetoview expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	9.8	More Details
CVE-2020-8349	An internal security review has identified an unauthenticated remote code execution vulnerability in Cloud Networking Operating System (CNOS)' optional REST API management interface. This interface is disabled by default and not vulnerable unless enabled. When enabled, it is only vulnerable where attached to a VRF and as allowed by defined ACLs. Lenovo strongly recommends upgrading to a non-vulnerable CNOS release. Where not possible, Lenovo recommends disabling the REST API management interface or restricting access to the management VRF and further limiting access to authorized management stations via ACL.	9.8	More Details
CVE-2020-0376	There is a possible out of bounds read due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-163003156	9.1	More Details
CVE-2020-0367	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-162980455	9.1	More Details
CVE-2020-0371	There is a possible out of bounds read due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-163008256	9.1	More Details
CVE-2020-0339	There is a possible out of bounds read due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-162980705	9.1	More Details
CVE-2019-19885	In Bender COMTRAXX, user authorization is validated for most, but not all, routes in the system. A user with knowledge about the routes can read and write configuration data without prior authorization. This affects COM465IP, COM465DP, COM465ID, CP700, CP907, and CP915 devices before 4.2.0.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16159	GoPro gpmf-parser 1.5 has a heap out-of-bounds read and segfault in GPMF_ScaledData(). Parsing malicious input can result in a crash or information disclosure.	9.1	More Details
CVE-2020-0283	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-163008257	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-7191	A devsoftsel expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-1656	The DHCPv6 Relay-Agent service, part of the Juniper Enhanced jdhcpd daemon shipped with Juniper Networks Junos OS has an Improper Input Validation vulnerability which will result in a Denial of Service (DoS) condition when a DHCPv6 client sends a specific DHPCv6 message allowing an attacker to potentially perform a Remote Code Execution (RCE) attack on the target device. Continuous receipt of the specific DHCPv6 client message will result in an extended Denial of Service (DoS) condition. If adjacent devices are also configured to relay DHCP packets, and are not affected by this issue and simply transparently forward unprocessed client DHCPv6 messages, then the attack vector can be a Network-based attack, instead of an Adjacent-device attack. No other DHCP services are affected. Receipt of the packet without configuration of the DHCPv6 Relay-Agent service, will not result in exploitability of this issue. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15; 12.3X48 versions prior to 12.3X48-D95; 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D200; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D44; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S6, 18.2R3-S2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D435, 18.2X75-D60; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8350	An authentication bypass vulnerability was reported in Lenovo ThinkPad Stack Wireless Router firmware version 1.1.3.4 that could allow escalation of privilege.	8.8	More Details
CVE-2020-9983	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to code execution.	8.8	More Details
CVE-2020-16158	GoPro gpmf-parser through 1.5 has a stack out-of-bounds write vulnerability in GPMF_ExpandComplexTYPE(). Parsing malicious input can result in a crash or potentially arbitrary code execution.	8.8	More Details
CVE-2020-7591	A vulnerability has been identified in SIPORT MP (All versions < 3.2.1). Vulnerable versions of the device could allow an authenticated attacker to impersonate other users of the system and perform (potentially administrative) actions on behalf of those users if the single sign-on feature ("Allow logon without password") is enabled.	8.8	More Details
CVE-2020-7195	A iccselectrules expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7194	A perfaddormoddevicemonitor expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7193	A ictexpertcsvdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7192	A devicethresholdconfig expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-5642	Cross-site request forgery (CSRF) vulnerability in Live Chat - Live support version 3.1.0 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2020-24630	A remote operatoronlinelist_content privilege escalation vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-9951	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7190	A deviceselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7189	A faultflasheventselectfact expression language injectionremote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7188	A userselectpagingcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7187	A reportpage index expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-9948	A type confusion issue was addressed with improved memory handling. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-7186	A powershellconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7185	A tvxlanlegend expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7184	A viewbatchtaskresultdetailfact expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7183	A forwardredirect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7182	A sshconfig expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7181	A smsrulesdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7173	A actionselectcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7180	A ictexpertdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7179	A thirdpartyperfselecttask expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7178	A mediaforaction expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7177	A wmiconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7176	A viewtaskresultdetailfact expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7175	A iccselectdymicparam expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-7174	A soapconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).	8.8	More Details
CVE-2020-12502	Improper Authorization vulnerability of Pepperl+Fuchs P+F Comtrol RocketLinx ES7510-XT, ES8509-XT, ES8510-XT, ES9528-XTv2, ES7506, ES7510, ES7528, ES8508, ES8508F, ES8510, ES8510-XTE, ES9528/ES9528-XT (all versions) and ICRL-M-8RJ45/4SFP-G-DIN, ICRL-M-16RJ45/4CP-G-DIN FW 1.2.3 and below is prone to unauthenticated device administration.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16911	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit the vulnerability: - In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message. - In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory.	8.8	More Details
CVE-2020-26682	In libass 0.14.0, the `ass_outline_construct`'s call to `outline_stroke` causes a signed integer overflow.	8.8	More Details
CVE-2020-9910	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	8.8	More Details
CVE-2020-0416	In multiple settings screens, there are possible tapjacking attacks due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.0 Android-8.1Android ID: A-155288585	8.8	More Details
CVE-2020-9893	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16891	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code. An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.	8.8	More Details
CVE-2020-1080	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory. An attacker who successfully exploited these vulnerabilities could gain elevated privileges on a target operating system. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerabilities by correcting how Windows Hyper-V handles objects in memory.	8.8	More Details
CVE-2019-4680	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.2.2 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 171733.	8.8	More Details
CVE-2020-16898	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer. The update addresses the vulnerability by correcting how the Windows TCP/IP stack handles ICMPv6 Router Advertisement packets.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1673	Insufficient Cross-Site Scripting (XSS) protection in Juniper Networks J-Web and web based (HTTP/HTTPS) services allows an unauthenticated attacker to hijack the target user's HTTP/HTTPS session and perform administrative actions on the Junos device as the targeted user. This issue only affects Juniper Networks Junos OS devices with HTTP/HTTPS services enabled such as J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Zero Touch Provisioning (ZTP). Junos OS devices with HTTP/HTTPS services disabled are not affected. If HTTP/HTTPS services are enabled, the following command will show the httpd processes: user@device> show system processes l match http 5260 - S 0:00.13 /usr/sbin/httpd-gk - N 5797 - I 0:00.10 /usr/sbin/httpd --config /jail/var/etc/httpd.conf In order to successfully exploit this vulnerability, the attacker needs to convince the device administrator to take action such as clicking the crafted URL sent via phishing email or convince the administrator to input data in the browser console. This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3-S1; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S2; 19.1 versions prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1.	8.8	More Details
CVE-2020-15909	SolarWinds N-central through 2020.1 allows session hijacking and requires user interaction or physical access. The N-Central JSESSIONID cookie attribute is not checked against multiple sources such as sourceip, MFA claim, etc. as long as the victim stays logged in within N-Central. To take advantage of this, cookie could be stolen and the JSESSIONID can be captured. On its own this is not a surprising result; low security tools allow the cookie to roam from machine to machine. The JSESSION cookie can then be used on the attackers' workstation by browsing to the victim's NCentral server URL and replacing the JSESSIONID attribute value by the captured value. Expected behavior would be to check this against a second source and enforce at least a reauthentication or multi factor request as N-Central is a highly privileged service.	8.8	More Details
CVE-2020-13778	rConfig 3.9.4 and earlier allows authenticated code execution (of system commands) by sending a forged GET request to lib/ajaxHandlers/ajaxAddTemplate.php or lib/ajaxHandlers/ajaxEditTemplate.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9870	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. An attacker with memory write capability may be able to bypass pointer authentication codes and run arbitrary code.	8.8	More Details
CVE-2020-16946	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	8.7	More Details
CVE-2020-16945	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16944	This vulnerability is caused when SharePoint Server does not properly sanitize a specially crafted request to an affected SharePoint server. An authenticated attacker could exploit this vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited this vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the victim, such as change permissions, delete content, steal sensitive information (such as browser cookies) and inject malicious content in the browser of the victim. For this vulnerability to be exploited, a user must click a specially crafted URL that takes the user to a targeted SharePoint Web App site. In an email attack scenario, an attacker could exploit the vulnerability by sending an email message containing the specially crafted URL to the user of the targeted SharePoint Web App site and convincing the user to click the specially crafted URL. In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted URL to the targeted SharePoint Web App site that is used to attempt to exploit these vulnerabilities. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. An attacker would have no way to force users to visit a specially crafted website. Instead, an attacker would have to convince them to visit the website, typically by getting them to click a link in an instant messenger or email message that takes them to the attacker's website, and then convince them to click the specially crafted URL. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes user web requests.	8.7	More Details
CVE-2020-15255	In Anuko Time Tracker before verion 1.19.23.5325, due to not properly filtered user input a CSV export of a report could contain cells that are treated as formulas by spreadsheet software (for example, when a cell value starts with an equal sign). This is fixed in version 1.19.23.5325.	8.7	More Details
CVE-2020-9865	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to break out of its sandbox.	8.6	More Details
CVE-2020-27153	In BlueZ before 5.55, a double free was found in the gatttool disconnect_cb() routine from shared/att.c. A remote attacker could potentially cause a denial of service or code execution, during service discovery, due to a redundant disconnect MGMT event.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16951	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	8.6	More Details
CVE-2020-16952	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	8.6	More Details
CVE-2020-15252	In XWiki before version 12.5 and 11.10.6, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which contains tools allowing to instantiate arbitrary Java objects and invoke methods that may lead to arbitrary code execution. This is patched in XWiki 12.5 and XWiki 11.10.6.	8.5	More Details
CVE-2020-1667	When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets processed by the Multiservices PIC Management Daemon (mspmand) process might be bypassed due to a race condition. Due to this vulnerability, mspmand process, responsible for managing "URL Filtering service", can crash, causing the Services PIC to restart. While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC completes its boot process. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect Juniper Networks Junos OS 17.4, 18.1, and 18.2.	8.3	More Details
CVE-2020-27176	Mutation XSS exists in Mark Text through 0.16.2 that leads to Remote Code Execution. NOTE: this might be considered a duplicate of CVE-2020-26870; however, it can also be considered an issue in the design of the "source code mode" feature, which parses HTML even though HTML support is not one of the primary advertised roles of the product.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1660	When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets processed by the Multiservices PIC Management Daemon (mspmand) process, responsible for managing "URL Filtering service", may crash, causing the Services PIC to restart. While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC completes its boot process. This vulnerability might allow an attacker to cause an extended Denial of Service (DoS) attack against the device and to cause clients to be vulnerable to DNS based attacks by malicious DNS servers when they send DNS requests through the device. As a result, devices which were once protected by the DNS Filtering service are no longer protected and at risk of exploitation. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect Juniper Networks Junos OS 17.4, 18.1, and 18.2.	8.3	More Details
CVE-2020-1675	When Security Assertion Markup Language (SAML) authentication is enabled, Juniper Networks Mist Cloud UI might incorrectly process invalid authentication certificates which could allow a malicious network-based user to access unauthorized data. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020.	8.3	More Details
CVE-2020-15229	Singularity (an open source container platform) from version 3.1.1 through 3.6.3 has a vulnerability. Due to insecure handling of path traversal and the lack of path sanitization within `unsquashfs`, it is possible to overwrite/create any files on the host filesystem during the extraction with a crafted squashfs filesystem. The extraction occurs automatically for unprivileged (either installation or with `allow setuid = no`) run of Singularity when a user attempt to run an image which is a local SIF image or a single file containing a squashfs filesystem and is coming from remote sources `library://` or `shub://`. Image build is also impacted in a more serious way as it can be used by a root user, allowing an attacker to overwrite/create files leading to a system compromise, so far bootstrap methods `library`, `shub` and `localimage` are triggering the squashfs extraction. This issue is addressed in Singularity 3.6.4. All users are advised to upgrade to 3.6.4 especially if they use Singularity mainly for building image as root user. There is no solid workaround except to temporary avoid to use unprivileged mode with single file images in favor of sandbox images instead. Regarding image build, temporary avoid to build from `library` and `shub` sources and as much as possible use `--fakeroot` or a VM for that.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15254	Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel incorrectly assumes that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect capacity when `Vec::from_iter` has allocated different sizes with the number of iterator elements. This has been fixed in crossbeam-channel 0.4.4.	8.1	More Details
CVE-2020-27157	Veritas APTARE versions prior to 10.5 included code that bypassed the normal login process when specific authentication credentials were provided to the server. An unauthenticated user could login to the application and gain access to the data and functionality accessible to the targeted user account.	8.1	More Details
CVE-2020-25214	In the client in Overwolf 0.149.2.30, a channel can be accessed or influenced by an actor that is not an endpoint.	8.1	More Details
CVE-2020-15258	In Wire before 3.20.x, `shell.openExternal` was used without checking the URL. This vulnerability allows an attacker to execute code on the victims machine by sending messages containing links with arbitrary protocols. The victim has to interact with the link and sees the URL that is opened. The issue was patched by implementing a helper function which checks if the URL's protocol is common. If it is common, the URL will be opened externally. If not, the URL will not be opened and a warning appears for the user informing them that a probably insecure URL was blocked from being executed. The issue is patched in Wire 3.20.x. More technical details about exploitation are available in the linked advisory.	8.0	More Details
CVE-2020-15261	On Windows the Veyon Service before version 4.4.2 contains an unquoted service path vulnerability, allowing locally authenticated users with administrative privileges to run malicious executables with LocalSystem privileges. Since Veyon users (both students and teachers) usually don't have administrative privileges, this vulnerability is only dangerous in anyway unsafe setups. The problem has been fixed in version 4.4.2. As a workaround, the exploitation of the vulnerability can be prevented by revoking administrative privileges from all potentially untrustworthy users.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15264	The Boxstarter installer before version 2.13.0 configures C:\ProgramData\Boxstarter to be in the system-wide PATH environment variable. However, this directory is writable by normal, unprivileged users. To exploit the vulnerability, place a DLL in this directory that a privileged service is looking for. For example, WptsExtensions.dll When Windows starts, it'll execute the code in DllMain() with SYSTEM privileges. Any unprivileged user can execute code with SYSTEM privileges. The issue is fixed in version 3.13.0	8.0	More Details
CVE-2020-15263	In platform before version 9.4.4, inline attributes are not properly escaped. If the data that came from users was not escaped, then an XSS vulnerability is possible. The issue was introduced in 9.0.0 and fixed in 9.4.4.	8.0	More Details
CVE-2020-9113	HUAWEI Mate 20 versions earlier than 10.0.0.188(C00E74R3P8) have a buffer overflow vulnerability in the Bluetooth module. Due to insufficient input validation, an unauthenticated attacker may craft Bluetooth messages after successful paring, causing buffer overflow. Successful exploit may cause code execution.	8.0	More Details
CVE-2020-9891	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-16973	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-9884	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9878	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16972	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-9923	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-9889	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9907	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-16954	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16968	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of the Windows Camera Codec Pack. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how the Windows Camera Codec Pack handles objects in memory.	7.8	More Details
CVE-2020-16955	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files. An attacker who successfully exploited the vulnerability could elevate privileges. To exploit this vulnerability, an attacker would need to convince a user to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office Click-to-Run (C2R) components handle these files.	7.8	More Details
CVE-2020-16957	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16967	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of the Windows Camera Codec Pack. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how the Windows Camera Codec Pack handles objects in memory.	7.8	More Details
CVE-2020-9890	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9888	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-17023	A remote code execution vulnerability exists in Visual Studio Code when a user is tricked into opening a malicious 'package.json' file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to clone a repository and open it in Visual Studio Code. Attacker-specified code would execute when the target opens the malicious 'package.json' file. The update address the vulnerability by modifying the way Visual Studio Code handles JSON files.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9936	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-16918	A remote code execution vulnerability exists when the Base3D rendering engine improperly handles memory. An attacker who successfully exploited the vulnerability would gain execution on a victim system. The security update addresses the vulnerability by correcting how the Base3D rendering engine handles memory.	7.8	More Details
CVE-2020-16890	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	7.8	More Details
CVE-2020-16895	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash. An attacker who successfully exploited this vulnerability could delete a targeted file leading to an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows Error Reporting manager handles process crashes.	7.8	More Details
CVE-2020-16887	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Network Connections Service properly handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16885	An elevation of privilege vulnerability exists when the Windows Storage VSP Driver improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Storage VSP Driver properly handles file operations.	7.8	More Details
CVE-2020-0764	An elevation of privilege vulnerability exists when the Windows Storage Services improperly handle file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Storage Services properly handle file operations.	7.8	More Details
CVE-2020-16902	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. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting the input sanitization error to preclude unintended elevation.	7.8	More Details
CVE-2019-2194	In SurfaceFlinger::createLayer of SurfaceFlinger.cpp, there is a possible arbitrary code execution due to improper casting. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-137284057	7.8	More Details
CVE-2020-16907	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16908	An elevation of privilege vulnerability exists in Windows Setup in the way it handles directories. A locally authenticated attacker could run arbitrary code with elevated system privileges. After successfully exploiting the vulnerability, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by ensuring Windows Setup properly handles directories.	7.8	More Details
CVE-2020-16909	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files.	7.8	More Details
CVE-2020-16912	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-16913	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16915	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.	7.8	More Details
CVE-2020-16916	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how the Windows COM Server creates COM objects.	7.8	More Details
CVE-2020-16920	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Application Compatibility Client Library properly handles registry operations.	7.8	More Details
CVE-2020-9799	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-16923	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16924	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.8	More Details
CVE-2020-16928	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files. An attacker who successfully exploited the vulnerability could elevate privileges. To exploit this vulnerability, an attacker would need to convince a user to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office Click-to-Run (C2R) components handle these files.	7.8	More Details
CVE-2020-16929	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1664	A stack buffer overflow vulnerability in the device control daemon (DCD) on Juniper Networks Junos OS allows a low privilege local user to create a Denial of Service (DoS) against the daemon or execute arbitrary code in the system with root privilege. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. Versions of Junos OS prior to 17.3 are unaffected by this vulnerability.	7.8	More Details
CVE-2020-16930	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16931	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details
CVE-2020-16932	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16935	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how the Windows COM Server creates COM objects.	7.8	More Details
CVE-2020-9992	This issue was addressed by encrypting communications over the network to devices running iOS 14, iPadOS 14, tvOS 14, and watchOS 7. This issue is fixed in iOS 14.0 and iPadOS 14.0, Xcode 12.0. An attacker in a privileged network position may be able to execute arbitrary code on a paired device during a debug session over the network.	7.8	More Details
CVE-2020-16936	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-16939	An elevation of privilege vulnerability exists when Group Policy improperly checks access. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how Group Policy checks access.	7.8	More Details
CVE-2020-16940	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points. An attacker who successfully exploited this vulnerability could delete files and folders in an elevated context. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and delete files or folders of their choosing. The security update addresses the vulnerability by correcting how the Windows User Profile Service handles junction points.	7.8	More Details
CVE-2020-9958	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 14.0 and iPadOS 14.0. An application may be able to cause unexpected system termination or write kernel memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9862	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection.	7.8	More Details
CVE-2020-16892	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in memory.	7.8	More Details
CVE-2020-16974	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-24412	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-0408	In remove of String16.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-156999009	7.8	More Details
CVE-2020-0423	In binder_release_work of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-161151868References: N/A	7.8	More Details
CVE-2020-24413	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6105	An exploitable code execution vulnerability exists in the multiple devices functionality of F2fs-Tools F2fs.Fsck 1.13. A specially crafted f2fs filesystem can cause Information overwrite resulting in a code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2020-6374	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated Jupiter Tessallation(.jt) file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	7.8	More Details
CVE-2020-6373	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PDF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	7.8	More Details
CVE-2020-6372	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PDF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	7.8	More Details
CVE-2020-9112	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have a privilege elevation vulnerability. Due to lack of privilege restrictions on some of the business functions of the device. An attacker could exploit this vulnerability to access the protecting information, resulting in the elevation of the privilege.	7.8	More Details
CVE-2020-24415	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-24411	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds write vulnerability when handling crafted PDF files. This could result in a write past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-8338	A DLL search path vulnerability was reported in Lenovo Diagnostics prior to version 4.35.4 that could allow a user with local access to execute code on the system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9263	HUAWEI Mate 30 versions earlier than 10.1.0.150(C00E136R5P3) and HUAWEI P30 version earlier than 10.1.0.160(C00E160R2P11) have a use after free vulnerability. There is a condition exists that the system would reference memory after it has been freed, the attacker should trick the user into running a crafted application with common privilege, successful exploit could cause code execution.	7.8	More Details
CVE-2020-24410	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing crafted PDF files. This could result in a read past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-24409	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing crafted PDF files. This could result in a read past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-0420	In setUpdatableDriverPath of GpuService.cpp, there is a possible memory corruption due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162383705	7.8	More Details
CVE-2020-0421	In appendFormatV of String8.cpp, there is a possible out of bounds write due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-161894517	7.8	More Details
CVE-2020-24414	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-6108	An exploitable code execution vulnerability exists in the fsck_chk_orphan_node functionality of F2fs-Tools F2fs.Fsck 1.13. A specially crafted f2fs filesystem can cause a heap buffer overflow resulting in a code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16995	An elevation of privilege vulnerability exists in Network Watcher Agent virtual machine extension for Linux. An attacker who successfully exploited this vulnerability could execute code with elevated privileges. To exploit this vulnerability, an attacker would have to be present as a user on the affected virtual machine. The security update addresses this vulnerability by correcting how Network Watcher Agent virtual machine extension for Linux executes with elevated privileges.	7.8	More Details
CVE-2020-16980	An elevation of privilege vulnerability exists when the Windows iSCSI Target Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows iSCSI Target Service properly handles file operations.	7.8	More Details
CVE-2020-17003	A remote code execution vulnerability exists when the Base3D rendering engine improperly handles memory. An attacker who successfully exploited the vulnerability would gain execution on a victim system. The security update addresses the vulnerability by correcting how the Base3D rendering engine handles memory.	7.8	More Details
CVE-2020-16975	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-25188	An attacker who convinces a valid user to open a specially crafted project file to exploit could execute code under the privileges of the application due to an out-of-bounds read vulnerability on the LAquis SCADA (Versions prior to 4.3.1.870).	7.8	More Details
CVE-2020-17022	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1047	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory. An attacker who successfully exploited these vulnerabilities could gain elevated privileges on a target operating system. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerabilities by correcting how Windows Hyper-V handles objects in memory.	7.8	More Details
CVE-2020-16976	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Backup Service handles file operations.	7.8	More Details
CVE-2020-1243	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests.	7.8	More Details
CVE-2020-26893	An issue was discovered in ClamXAV 3 before 3.1.1. A malicious actor could use a properly signed copy of ClamXAV 2 (running with an injected malicious dylib) to communicate with ClamXAV 3's helper tool and perform privileged operations. This occurs because of inadequate client verification in the helper tool.	7.8	More Details
CVE-2020-1167	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16894	A denial of service vulnerability exists when Windows Network Address Translation (NAT) on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. The update addresses the vulnerability by modifying how Windows NAT accesses the host.	7.7	More Details
CVE-2020-15256	A prototype pollution vulnerability has been found in `object-path` <= 0.11.4 affecting the `set()` method. The vulnerability is limited to the `includeInheritedProps` mode (if version >= 0.11.0 is used), which has to be explicitly enabled by creating a new instance of `object-path` and setting the option `includeInheritedProps: true`, or by using the default `withInheritedProps` instance. The default operating mode is not affected by the vulnerability if version >= 0.11.0 is used. Any usage of `set()` in versions < 0.11.0 is vulnerable. The issue is fixed in object-path version 0.11.5 As a workaround, don't use the `includeInheritedProps: true` options or the `withInheritedProps` instance if using a version >= 0.11.0.	7.7	More Details
CVE-2020-11641	A local file inclusion vulnerability in B&R SiteManager versions <9.2.620236042 allows authenticated users to read sensitive files from SiteManager instances.	7.7	More Details
CVE-2020-7334	Improper privilege assignment vulnerability in the installer McAfee Application and Change Control (MACC) prior to 8.3.2 allows local administrators to change or update the configuration settings via a carefully constructed MSI configured to mimic the genuine installer. This version adds further controls for installation/uninstallation of software.	7.7	More Details
CVE-2020-11642	The local file inclusion vulnerability present in B&R SiteManager versions <9.2.620236042 allows authenticated users to impact availability of SiteManager instances.	7.7	More Details
CVE-2020-3982	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to crash the virtual machine's vmx process or corrupt hypervisor's memory heap.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7749	This affects all versions of package osm-static-maps. User input given to the package is passed directly to a template without escaping ({{{ ... }}}). As such, it is possible for an attacker to inject arbitrary HTML/JS code and depending on the context. It will be outputted as an HTML on the page which gives opportunity for XSS or rendered on the server (puppeteer) which also gives opportunity for SSRF and Local File Read.	7.6	More Details
CVE-2020-9417	The Transaction Insight reporting component of TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System, TIBCO Foresight Archive and Retrieval System Healthcare Edition, TIBCO Foresight Operational Monitor, TIBCO Foresight Operational Monitor Healthcare Edition, TIBCO Foresight Transaction Insight, and TIBCO Foresight Transaction Insight Healthcare Edition contains a vulnerability that theoretically allows an authenticated attacker to perform SQL injection. Affected releases are TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Archive and Retrieval System Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Transaction Insight: versions 5.1.0 and below, version 5.2.0, and TIBCO Foresight Transaction Insight Healthcare Edition: versions 5.1.0 and below, version 5.2.0.	7.6	More Details
CVE-2020-0413	In gatt_process_read_by_type_rsp of gatt_cl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the Bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-158778659	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1679	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1.	7.5	More Details
CVE-2020-1672	On Juniper Networks Junos OS devices configured with DHCPv6 relay enabled, receipt of a specific DHCPv6 packet might crash the jdhcpd daemon. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of specific crafted DHCP messages will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. Only DHCPv6 packet can trigger this issue. DHCPv4 packet cannot trigger this issue. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16863	A denial of service vulnerability exists in Windows Remote Desktop Service when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the Remote Desktop Service on the target system to stop responding. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Service. The update addresses the vulnerability by correcting how Remote Desktop Service handles connection requests.	7.5	More Details
CVE-2020-1683	On Juniper Networks Junos OS devices, a specific SNMP OID poll causes a memory leak which over time leads to a kernel crash (vmcore). Prior to the kernel crash other processes might be impacted, such as failure to establish SSH connection to the device. The administrator can monitor the output of the following command to check if there is memory leak caused by this issue: user@device> show system virtual-memory | match "pfe_ipclkmem" pfe_ipc 147 5K - 164352 16,32,64,8192 <-- increasing vm.kmem_map_free: 127246336 <-- decreasing pfe_ipc 0 0K - 18598 32,8192 vm.kmem_map_free: 134582272 This issue affects Juniper Networks Junos OS: 17.4R3; 18.1 version 18.1R3-S5 and later versions prior to 18.1R3-S10; 18.2 version 18.2R3 and later versions prior to 18.2R3-S3; 18.2X75 version 18.2X75-D420, 18.2X75-D50 and later versions prior to 18.2X75-D430, 18.2X75-D53, 18.2X75-D60; 18.3 version 18.3R3 and later versions prior to 18.3R3-S2; 18.4 version 18.4R1-S4, 18.4R2 and later versions prior to 18.4R2-S5, 18.4R3-S1; 19.1 version 19.1R2 and later versions prior to 19.1R2-S2, 19.1R3; 19.2 version 19.2R1 and later versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS prior to 17.4R3.	7.5	More Details
CVE-2020-0377	In gatt_process_read_by_type_rsp of gatt_cl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the Bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-158833854	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1684	On Juniper Networks SRX Series configured with application identification inspection enabled, receipt of specific HTTP traffic can cause high CPU load utilization, which could lead to traffic interruption. Application identification is enabled by default and is automatically turned on when Intrusion Detection and Prevention (IDP), AppFW, AppQoS, or AppTrack is configured. Thus, this issue might occur when IDP, AppFW, AppQoS, or AppTrack is configured. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S1; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2.	7.5	More Details
CVE-2020-6083	An exploitable denial of service vulnerability exists in the ENIP Request Path Port Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2020-6086	An exploitable denial of service vulnerability exists in the ENIP Request Path Data Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.If the Simple Segment Sub-Type is supplied, the device treats the byte following as the Data Size in words. When this value represents a size greater than what remains in the packet data, the device enters a fault state where communication with the device is lost and a physical power cycle is required.	7.5	More Details
CVE-2020-16896	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services. The update addresses the vulnerability by correcting how RDP handles connection requests.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1686	On Juniper Networks Junos OS devices, receipt of a malformed IPv6 packet may cause the system to crash and restart (vmcore). This issue can be trigged by a malformed IPv6 packet destined to the Routing Engine. An attacker can repeatedly send the offending packet resulting in an extended Denial of Service condition. Only IPv6 packets can trigger this issue. IPv4 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS prior to 18.4R1.	7.5	More Details
CVE-2020-6087	An exploitable denial of service vulnerability exists in the ENIP Request Path Data Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability If the ANSI Extended Symbol Segment Sub-Type is supplied, the device treats the byte following as the Data Size in words. When this value represents a size greater than what remains in the packet data, the device enters a fault state where communication with the device is lost and a physical power cycle is required.	7.5	More Details
CVE-2020-25648	A flaw was found in the way NSS handled CCS (ChangeCipherSpec) messages in TLS 1.3. This flaw allows a remote attacker to send multiple CCS messages, causing a denial of service for servers compiled with the NSS library. The highest threat from this vulnerability is to system availability. This flaw affects NSS versions before 3.58.	7.5	More Details
CVE-2020-16899	A denial of service vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer. The vulnerability would not allow an attacker to execute code or to elevate user rights directly. The update addresses the vulnerability by correcting how the Windows TCP/IP stack handles ICMPv6 Router Advertisement packets.	7.5	More Details
CVE-2020-25157	The R-SeeNet webpage (1.5.1 through 2.4.10) suffers from SQL injection, which allows a remote attacker to invoke queries on the database and retrieve sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1671	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash with a core dump if a malformed DHCPv6 packet is received, resulting with the restart of the daemon. This issue only affects DHCPv6, it does not affect DHCPv4. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.2 version 19.2R2 and later versions; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2; This issue does not affect Juniper Networks Junos OS prior to 17.4R1.	7.5	More Details
CVE-2020-6085	An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less than 0x18 bytes following the Key Format field.	7.5	More Details
CVE-2020-24765	InterMind iMind Server through 3.13.65 allows remote unauthenticated attackers to read the self-diagnostic archive via a direct api/rs/monitoring/rs/api/system/dump-diagnostic-info?server=127.0.0.1 request.	7.5	More Details
CVE-2020-16927	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RDP service on the target system to stop responding. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services. The update addresses the vulnerability by correcting how RDP handles connection requests.	7.5	More Details
CVE-2020-27178	Apereo CAS 5.3.x before 5.3.16, 6.x before 6.1.7.2, 6.2.x before 6.2.4, and 6.3.x before 6.3.0-RC4 mishandles secret keys with Google Authenticator for multifactor authentication.	7.5	More Details
CVE-2020-9903	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. A malicious attacker may cause Safari to suggest a password for the wrong domain.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25829	An issue has been found in PowerDNS Recursor before 4.1.18, 4.2.x before 4.2.5, and 4.3.x before 4.3.5. A remote attacker can cause the cached records for a given name to be updated to the Bogus DNSSEC validation state, instead of their actual DNSSEC Secure state, via a DNS ANY query. This results in a denial of service for installation that always validate (dnssec=validate), and for clients requesting validation when on-demand validation is enabled (dnssec=process).	7.5	More Details
CVE-2020-24265	An issue was discovered in tcpreplay tcpprep v4.3.3. There is a heap buffer overflow vulnerability in MemcmpInterceptorCommon() that can make tcpprep crash and cause a denial of service.	7.5	More Details
CVE-2020-9911	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. An issue in Safari Reader mode may allow a remote attacker to bypass the Same Origin Policy.	7.5	More Details
CVE-2020-27174	In Amazon AWS Firecracker before 0.21.3, and 0.22.x before 0.22.1, the serial console buffer can grow its memory usage without limit when data is sent to the standard input. This can result in a memory leak on the microVM emulation thread, possibly occupying more memory than intended on the host.	7.5	More Details
CVE-2020-27173	In vm-superio before 0.1.1, the serial console FIFO can grow to unlimited memory usage when data is sent to the input source (i.e., standard input). This behavior cannot be reproduced from the guest side. When no rate limiting is in place, the host can be subject to memory pressure, impacting all other VMs running on the same host.	7.5	More Details
CVE-2020-9914	An input validation issue existed in Bluetooth. This issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An attacker in a privileged network position may be able to perform denial of service attack using malformed Bluetooth packets.	7.5	More Details
CVE-2020-24266	An issue was discovered in tcpreplay tcpprep v4.3.3. There is a heap buffer overflow vulnerability in get_l2len() that can make tcpprep crash and cause a denial of service.	7.5	More Details
CVE-2020-16160	GoPro gpmf-parser 1.5 has a division-by-zero vulnerability in GPMF_Decompress(). Parsing malicious input can result in a crash.	7.5	More Details
CVE-2020-9917	This issue was addressed with improved checks. This issue is fixed in iOS 13.6 and iPadOS 13.6. A remote attacker may be able to cause a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16161	GoPro gpmf-parser 1.5 has a division-by-zero vulnerability in GPMF_ScaledData(). Parsing malicious input can result in a crash.	7.5	More Details
CVE-2020-25858	The QCMAP_Web_CLIENT binary in the Qualcomm QCMAP software suite prior to versions released in October 2020 does not validate the return value of a strstr() or strchr() call in the Tokenizer() function. An attacker who invokes the web interface with a crafted URL can crash the process, causing denial of service. This version of QCMAP is used in many kinds of networking devices, primarily mobile hotspots and LTE routers.	7.5	More Details
CVE-2020-9931	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6. A remote attacker may cause an unexpected application termination.	7.5	More Details
CVE-2020-16947	A remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the targeted user. If the targeted user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Outlook software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that where severity is indicated as Critical in the Affected Products table, the Preview Pane is an attack vector. The security update addresses the vulnerability by correcting how Outlook handles objects in memory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24387	An issue was discovered in the yh_create_session() function of yubihsm-shell through 2.0.2. The function does not explicitly check the returned session id from the device. An invalid session id would lead to out-of-bounds read and write operations in the session array. This could be used by an attacker to cause a denial of service attack.	7.5	More Details
CVE-2020-24388	An issue was discovered in the _send_secure_msg() function of yubihsm-shell through 2.0.2. The function does not validate the embedded length field of a message received from the device. This could lead to an oversized memcpy() call that will crash the running process. This could be used by an attacker to cause a denial of service.	7.5	More Details
CVE-2020-6084	An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less bytes than required by the Key Format Table.	7.5	More Details
CVE-2020-4254	IBM Security Guardium Big Data Intelligence 1.0 (SonarG) uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 175560.	7.5	More Details
CVE-2020-1657	On SRX Series devices, a vulnerability in the key-management-daemon (kmd) daemon of Juniper Networks Junos OS allows an attacker to spoof packets targeted to IPSec peers before a security association (SA) is established thereby causing a failure to set up the IPSec channel. Sustained receipt of these spoofed packets can cause a sustained Denial of Service (DoS) condition. This issue affects IPv4 and IPv6 implementations. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D90; 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S6, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2. This issue does not affect 12.3 or 15.1 releases which are non-SRX Series releases.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1662	On Juniper Networks Junos OS and Junos OS Evolved devices, BGP session flapping can lead to a routing process daemon (RPD) crash and restart, limiting the attack surface to configured BGP peers. This issue only affects devices with BGP damping in combination with accepted-prefix-limit configuration. When the issue occurs the following messages will appear in the /var/log/messages: rpd[6046]: %DAEMON-4-BGP_PREFIX_THRESH_EXCEEDED: XXXX (External AS x): Configured maximum accepted prefix-limit threshold(1800) exceeded for inet6-unicast nlri: 1984 (instance master) rpd[6046]: %DAEMON-3-BGP_CEASE_PREFIX_LIMIT_EXCEEDED: 2001:x:x:x::2 (External AS x): Shutting down peer due to exceeding configured maximum accepted prefix-limit(2000) for inet6-unicast nlri: 2001 (instance master) rpd[6046]: %DAEMON-4: bgp_rt_maxprefixes_check_common:9284: NOTIFICATION sent to 2001:x:x:x::2 (External AS x): code 6 (Cease) subcode 1 (Maximum Number of Prefixes Reached) AFI: 2 SAFI: 1 prefix limit 2000 kernel: %KERN-5: mastership_relinquish_on_process_exit: RPD crashed on master RE. Sending SIGUSR2 to chassisd (5612:chassisd) to trigger RE switchover This issue affects: Juniper Networks Junos OS: 17.2R3-S3; 17.3 version 17.3R3-S3 and later versions, prior to 17.3R3-S8; 17.4 version 17.4R2-S4, 17.4R3 and later versions, prior to 17.4R2-S10, 17.4R3-S2; 18.1 version 18.1R3-S6 and later versions, prior to 18.1R3-S10; 18.2 version 18.2R3 and later versions, prior to 18.2R3-S4; 18.2X75 version 18.2X75-D50, 18.2X75-D60 and later versions, prior to 18.2X75-D53, 18.2X75-D65; 18.3 version 18.3R2 and later versions, prior to 18.3R2-S4, 18.3R3-S2; 18.4 version 18.4R2 and later versions, prior to 18.4R2-S5, 18.4R3-S2; 19.1 version 19.1R1 and later versions, prior to 19.1R2-S2, 19.1R3-S1; 19.2 version 19.2R1 and later versions, prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved prior to 20.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R3-S3.	7.5	More Details
CVE-2019-9080	DomainMOD before 4.14.0 uses MD5 without a salt for password storage.	7.5	More Details
CVE-2020-15931	Netwrix Account Lockout Examiner before 5.1 allows remote attackers to capture the Net-NTLMv1/v2 authentication challenge hash of the Domain Administrator (that is configured within the product in its installation state) by generating a single Kerberos Pre-Authentication Failed (ID 4771) event on a Domain Controller.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7330	Privilege Escalation vulnerability in McAfee Total Protection (MTP) trial prior to 4.0.176.1 allows local users to schedule tasks which call malicious software to execute with elevated privileges via editing of environment variables	7.5	More Details
CVE-2020-3994	VMware vCenter Server (6.7 before 6.7u3, 6.6 before 6.5u3k) contains a session hijack vulnerability in the vCenter Server Appliance Management Interface update function due to a lack of certificate validation. A malicious actor with network positioning between vCenter Server and an update repository may be able to perform a session hijack when the vCenter Server Appliance Management Interface is used to download vCenter updates.	7.4	More Details
CVE-2020-15269	In Spree before versions 3.7.11, 4.0.4, or 4.1.11, expired user tokens could be used to access Storefront API v2 endpoints. The issue is patched in versions 3.7.11, 4.0.4 and 4.1.11. A workaround without upgrading is described in the linked advisory.	7.4	More Details
CVE-2020-15822	In JetBrains YouTrack before 2020.2.10514, SSRF is possible because URL filtering can be escaped.	7.3	More Details
CVE-2020-8345	A DLL search path vulnerability was reported in the Lenovo HardwareScan Plugin for the Lenovo Vantage hardware scan feature prior to version 1.0.46.11 that could allow escalation of privilege.	7.3	More Details
CVE-2020-15253	Versions of Grocy <= 2.7.1 are vulnerable to Cross-Site Scripting via the Create Shopping List module, that is rendered upon deleting that Shopping List. The issue was also found in users, batteries, chores, equipment, locations, quantity units, shopping locations, tasks, taskcategories, product groups, recipes and products. Authentication is required to exploit these issues and Grocy should not be publicly exposed. The linked reference details a proof-of-concept.	7.3	More Details
CVE-2020-5791	Improper neutralization of special elements used in an OS command in Nagios XI 5.7.3 allows a remote, authenticated admin user to execute operating system commands with the privileges of the apache user.	7.2	More Details
CVE-2020-5792	Improper neutralization of argument delimiters in a command in Nagios XI 5.7.3 allows a remote, authenticated admin user to write to arbitrary files and ultimately execute code with the privileges of the apache user.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15867	The git hook feature in Gogs 0.5.5 through 0.12.2 allows for authenticated remote code execution. There can be a privilege escalation if access to this hook feature is granted to a user who does not have administrative privileges. NOTE: because this is mentioned in the documentation but not in the UI, it could be considered a "Product UI does not Warn User of Unsafe Actions" issue.	7.2	More Details
CVE-2020-4636	IBM Resilient OnPrem 38.2 could allow a privileged user to inject malicious commands through Python3 scripting. IBM X-Force ID: 185503.	7.2	More Details
CVE-2020-1676	When SAML authentication is enabled, Juniper Networks Mist Cloud UI might incorrectly handle SAML responses, allowing a remote attacker to modify a valid SAML response without invalidating its cryptographic signature to bypass SAML authentication security controls. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020.	7.2	More Details
CVE-2020-1677	When SAML authentication is enabled, Juniper Networks Mist Cloud UI might incorrectly handle child elements in SAML responses, allowing a remote attacker to modify a valid SAML response without invalidating its cryptographic signature to bypass SAML authentication security controls. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020.	7.2	More Details
CVE-2020-12503	Improper Authorization vulnerability of Pepperl+Fuchs P+F Comtrol RocketLinx ES7510-XT, ES8509-XT, ES8510-XT, ES9528-XTv2, ES7506, ES7510, ES7528, ES8508, ES8508F, ES8510, ES8510-XTE, ES9528/ES9528-XT (all versions) and ICRL-M-8RJ45/4SFP-G-DIN, ICRL-M-16RJ45/4CP-G-DIN FW 1.2.3 and below is prone to multiple authenticated command injections.	7.2	More Details
CVE-2020-14144	The git hook feature in Gitea 1.1.0 through 1.12.5 might allow for authenticated remote code execution in customer environments where the documentation was not understood (e.g., one viewpoint is that the dangerousness of this feature should be documented immediately above the ENABLE_GIT_HOOKS line in the config file). NOTE: The vendor has indicated this is not a vulnerability and states "This is a functionality of the software that is limited to a very limited subset of accounts. If you give someone the privilege to execute arbitrary code on your server, they can execute arbitrary code on your server. We provide very clear warnings to users around this functionality and what it provides.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7745	This affects the package MintegralAdSDK before 6.6.0.0. The SDK distributed by the company contains malicious functionality that acts as a backdoor. Mintegral and their partners (advertisers) can remotely execute arbitrary code on a user device.	7.1	More Details
CVE-2020-16969	An information disclosure vulnerability exists in how Microsoft Exchange validates tokens when handling certain messages. An attacker who successfully exploited the vulnerability could use this to gain further information from a user. To exploit the vulnerability, an attacker could include specially crafted OWA messages that could be loaded, without warning or filtering, from the attacker-controlled URL. This callback vector provides an information disclosure tactic used in web beacons and other types of tracking systems. The security update corrects the way that Exchange handles these token validations.	7.1	More Details
CVE-2020-3483	Duo has identified and fixed an issue with the Duo Network Gateway (DNG) product in which some customer-provided SSL certificates and private keys were not excluded from logging. This issue resulted in certificate and private key information being written out in plain-text to local files on the DNG host. Any private keys logged in this way could be viewed by those with access to the DNG host operating system without any need for reversing encrypted values or similar techniques. An attacker that gained access to the DNG logs and with the ability to intercept and manipulate network traffic between a user and the DNG, could decrypt and manipulate SSL/TLS connections to the DNG and to the protected applications behind it. Duo Network Gateway (DNG) versions 1.3.3 through 1.5.7 are affected.	7.1	More Details
CVE-2020-3991	VMware Horizon Client for Windows (5.x before 5.5.0) contains a denial-of-service vulnerability due to a file system access control issue during install time. Successful exploitation of this issue may allow an attacker to overwrite certain admin privileged files through a symbolic link attack at install time. This will result into a denial-of-service condition on the machine where Horizon Client for Windows is installed.	7.1	More Details
CVE-2020-9952	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16877	An elevation of privilege vulnerability exists when Microsoft Windows improperly handles reparse points. An attacker who successfully exploited this vulnerability could overwrite or delete a targeted file that would normally require elevated permissions. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and overwrite or delete files. The security update addresses the vulnerability by correcting how Windows handles reparse points.	7.1	More Details
CVE-2020-16876	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Application Compatibility Client Library properly handles registry operations.	7.1	More Details
CVE-2020-16933	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Word software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Word handles these files.	7.0	More Details
CVE-2020-9746	Adobe Flash Player version 32.0.0.433 (and earlier) are affected by an exploitable NULL pointer dereference vulnerability that could result in a crash and arbitrary code execution. Exploitation of this issue requires an attacker to insert malicious strings in an HTTP response that is by default delivered over TLS/SSL.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16934	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files. An attacker who successfully exploited the vulnerability could elevate privileges. To exploit this vulnerability, an attacker would need to convince a user to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office Click-to-Run (C2R) components handle these files.	7.0	More Details
CVE-2020-16977	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads a Jupyter notebook file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to open a specially crafted file in Visual Studio Code with the Python extension installed. The update addresses the vulnerability by modifying the way Visual Studio Code Python extension renders notebook content.	7.0	More Details
CVE-2020-16900	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Event System handles objects in memory.	7.0	More Details
CVE-2020-26183	Dell EMC NetWorker versions prior to 19.3.0.2 contain an improper authorization vulnerability. Certain remote users with low privileges may exploit this vulnerability to perform 'nsrmmdbd' operations in an unintended manner.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15224	In Open Enclave before version 0.12.0, an information disclosure vulnerability exists when an enclave application using the syscalls provided by the sockets.edl is loaded by a malicious host application. An attacker who successfully exploited the vulnerability could read privileged data from the enclave heap across trust boundaries. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to elevate user rights directly, but it could be used to obtain information otherwise considered confidential in an enclave, which could be used in further compromises. The issue has been addressed in version 0.12.0 and the current master branch. Users will need to to recompile their applications against the patched libraries to be protected from this vulnerability.	6.8	More Details
CVE-2020-16905	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files.	6.8	More Details
CVE-2020-9946	This issue was addressed with improved checks. This issue is fixed in iOS 14.0 and iPadOS 14.0, watchOS 7.0. The screen lock may not engage after the specified time period.	6.8	More Details
CVE-2020-26182	Dell EMC NetWorker versions prior to 19.3.0.2 contain an incorrect privilege assignment vulnerability. A non-LDAP remote user with low privileges may exploit this vulnerability to perform 'saveset' related operations in an unintended manner. The vulnerability is not exploitable by users authenticated via LDAP.	6.8	More Details
CVE-2020-25859	The QCMAP_CLI utility in the Qualcomm QCMAP software suite prior to versions released in October 2020 uses a system() call without validating the input, while handling a SetGatewayUrl() request. A local attacker with shell access can pass shell metacharacters and run arbitrary commands. If QCMAP_CLI can be run via sudo or setuid, this also allows elevating privileges to root. This version of QCMAP is used in many kinds of networking devices, primarily mobile hotspots and LTE routers.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11496	Sprecher SPRECON-E firmware prior to 8.64b might allow local attackers with access to engineering data to insert arbitrary code. This firmware lacks the validation of the input values on the device side, which is provided by the engineering software during parameterization. Attackers with access to local configuration files can therefore insert malicious commands that are executed after compiling them to valid parameter files (“PDLs”), transferring them to the device, and restarting the device.	6.7	More Details
CVE-2020-3427	The Windows Logon installer prior to 4.1.2 did not properly validate file installation paths. This allows an attacker with local user privileges to coerce the installer to write to arbitrary privileged directories. If successful, an attacker can manipulate files used by Windows Logon, cause Denial of Service (DoS) by deleting file(s), or replace system files to potentially achieve elevation of privileges. Note that this can only exploitable during new installations while the installer is running and is not exploitable once installation is finished. Versions 4.1.2 of Windows Logon addresses this issue.	6.6	More Details
CVE-2020-1666	The system console configuration option 'log-out-on-disconnect' In Juniper Networks Junos OS Evolved fails to log out an active CLI session when the console cable is disconnected. This could allow a malicious attacker with physical access to the console the ability to resume a previous interactive session and possibly gain administrative privileges. This issue affects all Juniper Networks Junos OS Evolved versions after 18.4R1-EVO, prior to 20.2R1-EVO.	6.6	More Details
CVE-2020-16953	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles objects in memory.	6.5	More Details
CVE-2020-6366	SAP NetWeaver (Compare Systems) versions - 7.20, 7.30, 7.40, 7.50, does not sufficiently validate uploaded XML documents. An attacker with administrative privileges can retrieve arbitrary files including files on OS level from the server and/or can execute a denial-of-service.	6.5	More Details
CVE-2020-11645	A denial of service vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to limit availability of GateManager instances.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16948	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles objects in memory.	6.5	More Details
CVE-2020-24375	A DNS rebinding vulnerability in the UPnP MediaServer implementation in Freebox Server before 4.2.3.	6.5	More Details
CVE-2020-6362	SAP Banking Services version 500, use an incorrect authorization object in some of its reports. Although the affected reports are protected with otherauthorization objects, exploitation of the vulnerability could lead to privilege escalation and violation in segregation of duties, which in turn could lead to Service interruptions and system unavailability for the victim and users of the component.	6.5	More Details
CVE-2020-9915	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	6.5	More Details
CVE-2020-21674	Heap-based buffer overflow in archive_string_append_from_wcs() (archive_string.c) in libarchive-3.4.1dev allows remote attackers to cause a denial of service (out-of-bounds write in heap memory resulting into a crash) via a crafted archive file. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected.	6.5	More Details
CVE-2020-16943	An elevation of privilege vulnerability exists in Microsoft Dynamics 365 Commerce. An unauthenticated attacker who successfully exploited this vulnerability could update data without proper authorization. To exploit the vulnerability, an attacker would need to send a specially crafted request to an affected server. The security update addresses the vulnerability by correcting how Microsoft Dynamics 365 Commerce performs authorization checks.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11643	An information disclosure vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to view information of devices belonging to foreign domains.	6.5	More Details
CVE-2020-14299	A flaw was found in JBoss EAP, where the authentication configuration is set-up using a legacy SecurityRealm, to delegate to a legacy PicketBox SecurityDomain, and then reloaded to admin-only mode. This flaw allows an attacker to perform a complete authentication bypass by using an arbitrary user and password. The highest threat to vulnerability is to system availability.	6.5	More Details
CVE-2019-18796	The BASS Audio Library 2.4.14 under Windows is prone to a BASS_StreamCreateFile Denial of Service vulnerability (infinite loop) via a crafted .mp3 file. This weakness could allow attackers to consume excessive CPU and the application becomes unresponsive.	6.5	More Details
CVE-2019-18795	The BASS Audio Library 2.4.14 under Windows is prone to a BASS_StreamCreateFile out of bounds read vulnerability via a crafted .wav file. An attacker can exploit this issues to gain access to sensitive information that may aid in further attacks. A failure in exploitation leads to denial of service.	6.5	More Details
CVE-2019-18794	The BASS Audio Library 2.4.14 under Windows is prone to a BASS_StreamCreateFile Use after Free vulnerability via a crafted .ogg file. An attacker can exploit this to gain access to sensitive information that may aid in further attacks. A failure in exploitation leads to denial of service.	6.5	More Details
CVE-2020-7383	A SQL Injection issue in Rapid7 Nexpose version prior to 6.6.49 that may have allowed an authenticated user with a low permission level to access resources & make changes they should not have been able to access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1689	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2.	6.5	More Details
CVE-2020-11644	The information disclosure vulnerability present in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to generate fake audit log messages.	6.5	More Details
CVE-2020-1678	On Juniper Networks Junos OS and Junos OS Evolved platforms with EVPN configured, receipt of specific BGP packets causes a slow memory leak. If the memory is exhausted the rpd process might crash. If the issue occurs, the memory leak could be seen by executing the "show task memory detail | match policy | match evpn" command multiple times to check if memory (Alloc Blocks value) is increasing. root@device> show task memory detail | match policy | match evpn ---------- Allocator Memory Report ---------- Name | Size | Alloc DTXP Size | Alloc Blocks | Alloc Bytes | MaxAlloc Blocks | MaxAlloc Bytes Policy EVPN Params 20 24 3330678 79936272 3330678 79936272 root@device> show task memory detail | match policy | match evpn ---------- Allocator Memory Report ---------- Name | Size | Alloc DTXP Size | Alloc Blocks | Alloc Bytes | MaxAlloc Blocks | MaxAlloc Bytes Policy EVPN Params 20 24 36620255 878886120 36620255 878886120 This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R2; 20.1 versions prior to 20.1R1-S4, 20.1R2; Juniper Networks Junos OS Evolved: 19.4 versions; 20.1 versions prior to 20.1R1-S4-EVO, 20.1R2-EVO; 20.2 versions prior to 20.2R1-EVO; This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1687	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in (Ethernet VPN) EVPN-(Virtual Extensible LAN) VXLAN configuration, receipt of a stream of specific VXLAN encapsulated layer 2 frames can cause high CPU load, which could lead to network protocol operation issue and traffic interruption. This issue affects devices that are configured as a Layer 2 or Layer 3 gateway of an EVPN-VXLAN deployment. The offending layer 2 frames that cause the issue originate from a different access switch that get encapsulated within the same EVPN-VXLAN domain. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2.	6.5	More Details
CVE-2020-1681	Receipt of a specifically malformed NDP packet sent from the local area network (LAN) to a device running Juniper Networks Junos OS Evolved can cause the ndp process to crash, resulting in a Denial of Service (DoS). The process automatically restarts without intervention, but a continuous receipt of the malformed NDP packets could leaded to an extended Denial of Service condition. During this time, IPv6 neighbor learning will be affected. The issue occurs when parsing the incoming malformed NDP packet. Rather than simply discarding the packet, the process asserts, performing a controlled exit and restart, thereby avoiding any chance of an unhandled exception. Exploitation of this vulnerability is limited to a temporary denial of service, and cannot be leveraged to cause additional impact on the system. This issue is limited to the processing of IPv6 NDP packets. IPv4 packet processing cannot trigger, and is unaffected by this vulnerability. This issue affects all Juniper Networks Junos OS Evolved versions prior to 20.1R2-EVO. Junos OS is unaffected by this vulnerability.	6.5	More Details
CVE-2020-0414	In AudioFlinger::RecordThread::threadLoop of audioflinger/Threads.cpp, there is a possible non-silenced audio buffer due to a permissions bypass. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-157708122	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1670	On Juniper Networks EX4300 Series, receipt of a stream of specific IPv4 packets can cause Routing Engine (RE) high CPU load, which could lead to network protocol operation issue and traffic interruption. This specific packets can originate only from within the broadcast domain where the device is connected. This issue occurs when the packets enter to the IRB interface. Only IPv4 packets can trigger this issue. IPv6 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS on EX4300 series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S4; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S3, 20.1R2.	6.5	More Details
CVE-2020-1668	On Juniper Networks EX2300 Series, receipt of a stream of specific multicast packets by the layer2 interface can cause high CPU load, which could lead to traffic interruption. This issue occurs when multicast packets are received by the layer 2 interface. To check if the device has high CPU load due to this issue, the administrator can issue the following command: user@host> show chassis routing-engine Routing Engine status: ... Idle 2 percent the "Idle" value shows as low (2 % in the example above), and also the following command: user@host> show system processes summary ... PID USERNAME PRI NICE SIZE RES STATE TIME WCPU COMMAND 11639 root 52 0 283M 11296K select 12:15 44.97% eventd 11803 root 81 0 719M 239M RUN 251:12 31.98% fxpc{fxpc} the eventd and the fxpc processes might use higher WCPU percentage (respectively 44.97% and 31.98% in the above example). This issue affects Juniper Networks Junos OS on EX2300 Series: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2.	6.5	More Details
CVE-2019-12305	In EZCast Pro II, the administrator password md5 hash is provided upon a web request. This hash can be cracked to access the administration panel of the device.	6.5	More Details
CVE-2020-0411	In ~AACExtractor() of AACExtractor.cpp, there is a possible out of bounds write due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-142641801	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1688	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2.	6.5	More Details
CVE-2020-5790	Cross-site request forgery in Nagios XI 5.7.3 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link.	6.5	More Details
CVE-2020-8332	A potential vulnerability in the SMI callback function used in the legacy BIOS mode USB drivers in some legacy Lenovo and IBM System x servers may allow arbitrary code execution. Servers operating in UEFI mode are not affected.	6.4	More Details
CVE-2020-7747	This affects all versions of package lightning-server. It is possible to inject malicious JavaScript code as part of a session controller.	6.3	More Details
CVE-2020-1669	The Juniper Device Manager (JDM) container, used by the disaggregated Junos OS architecture on Juniper Networks NFX350 Series devices, stores password hashes in the world-readable file /etc/passwd. This is not a security best current practice as it can allow an attacker with access to the local filesystem the ability to brute-force decrypt password hashes stored on the system. This issue affects Juniper Networks Junos OS on NFX350: 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16910	A security feature bypass vulnerability exists when Microsoft Windows fails to handle file creation permissions, which could allow an attacker to create files in a protected Unified Extensible Firmware Interface (UEFI) location. To exploit this vulnerability, an attacker could run a specially crafted application to bypass Unified Extensible Firmware Interface (UEFI) variable security in Windows. The security update addresses the vulnerability by correcting security feature behavior to enforce permissions.	6.2	More Details
CVE-2019-13633	Blinger.io v.1.0.2519 is vulnerable to Blind/Persistent XSS. An attacker can send arbitrary JavaScript code via a built-in communication channel, such as Telegram, WhatsApp, Viber, Skype, Facebook, Vkontakte, or Odnoklassniki. This is mishandled within the administration panel for conversations/all, conversations/inbox, conversations/unassigned, and conversations/closed.	6.1	More Details
CVE-2019-4552	IBM Security Access Manager 9.0.7 and IBM Security Verify Access 10.0.0 are vulnerable to HTTP response splitting attacks. A remote attacker could exploit this vulnerability using specially-crafted URL to cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning, cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 165960.	6.1	More Details
CVE-2020-24551	IProom MMC+ Server login page does not validate specific parameters properly. Attackers can use the vulnerability to redirect to any malicious site and steal the victim's login credentials.	6.1	More Details
CVE-2020-24416	Marketo Sales Insight plugin version 1.4355 (and earlier) is affected by a blind stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	6.1	More Details
CVE-2020-26584	An issue was discovered in Sage DPW 2020_06_x before 2020_06_002. The search field "Kurs suchen" on the page Kurskatalog is vulnerable to Reflected XSS. If the attacker can lure a user into clicking a crafted link, he can execute arbitrary JavaScript code in the user's browser. The vulnerability can be used to change the contents of the displayed site, redirect to other sites, or steal user credentials. Additionally, users are potential victims of browser exploits and JavaScript malware.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6365	SAP NetWeaver AS Java, versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, Start Page allows an unauthenticated remote attacker to redirect users to a malicious site due to insufficient reverse tabnabbing URL validation. The attacker could execute phishing attacks to steal credentials of the victim or to redirect users to untrusted web pages containing malware or similar malicious exploits.	6.1	More Details
CVE-2020-26891	AuthRestServlet in Matrix Synapse before 1.21.0 is vulnerable to XSS due to unsafe interpolation of the session GET parameter. This allows a remote attacker to execute an XSS attack on the domain Synapse is hosted on, by supplying the victim user with a malicious URL to the /_matrix/client/r0/auth/*/fallback/web or /_matrix/client/unstable/auth/*/fallback/web Synapse endpoints.	6.1	More Details
CVE-2020-26583	An issue was discovered in Sage DPW 2020_06_x before 2020_06_002. It allows unauthenticated users to upload JavaScript (in a file) via the expenses claiming functionality. However, to view the file, authentication is required. By exploiting this vulnerability, an attacker can persistently include arbitrary HTML or JavaScript code into the affected web page. The vulnerability can be used to change the contents of the displayed site, redirect to other sites, or steal user credentials. Additionally, users are potential victims of browser exploits and JavaScript malware.	6.1	More Details
CVE-2020-4748	IBM Spectrum Scale 5.0.0 through 5.0.5.2 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: 188517.	6.1	More Details
CVE-2020-6323	SAP NetWeaver Enterprise Portal (Fiori Framework Page) versions - 7.50, 7.31, 7.40, does not sufficiently encode user-controlled inputs and allows an attacker on a valid session to create an XSS that will be both reflected immediately and also be persisted and returned in further access to the system, resulting in Cross Site Scripting.	6.1	More Details
CVE-2020-27163	phpRedisAdmin before 1.13.2 allows XSS via the login.php username parameter.	6.1	More Details
CVE-2020-6319	SAP NetWeaver Application Server Java, versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, and 7.50 allows an unauthenticated attacker to include JavaScript blocks in any web page or URL with different symbols which are otherwise not allowed. On successful exploitation an attacker can steal authentication information of the user, such as data relating to his or her current session and limitedly impact confidentiality and integrity of the application, leading to Reflected Cross Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6367	There is a reflected cross site scripting vulnerability in SAP NetWeaver Composite Application Framework, versions - 7.20, 7.30, 7.31, 7.40, 7.50. An unauthenticated attacker can trick an unsuspecting authenticated user to click on a malicious link. The end users browser has no way to know that the script should not be trusted, and will execute the script, resulting in sensitive information being disclosed or modified.	6.1	More Details
CVE-2020-9925	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2020-16246	The affected Reason S20 Ethernet Switch is vulnerable to cross-site scripting (XSS), which may allow attackers to trick users into following a link or navigating to a page that posts a malicious JavaScript statement to the vulnerable site, causing the malicious JavaScript to be rendered by the site and executed by the victim client.	6.1	More Details
CVE-2020-24408	Magento versions 2.4.0 and 2.3.5p1 (and earlier) are affected by a persistent XSS vulnerability that allows users to upload malicious JavaScript via the file upload component. This vulnerability could be abused by an unauthenticated attacker to execute XSS attacks against other Magento users. This vulnerability requires a victim to browse to the uploaded file.	6.1	More Details
CVE-2020-10746	A flaw was found in Infinispan (org.infinispan:infinispan-server-runtime) version 10, where it permits local access to controls via both REST and HotRod APIs. This flaw allows a user authenticated to the local machine to perform all operations on the caches, including the creation, update, deletion, and shutdown of the entire server.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15157	In containerd (an industry-standard container runtime) before version 1.2.14 there is a credential leaking vulnerability. If a container image manifest in the OCI Image format or Docker Image V2 Schema 2 format includes a URL for the location of a specific image layer (otherwise known as a “foreign layer”), the default containerd resolver will follow that URL to attempt to download it. In v1.2.x but not 1.3.0 or later, the default containerd resolver will provide its authentication credentials if the server where the URL is located presents an HTTP 401 status code along with registry-specific HTTP headers. If an attacker publishes a public image with a manifest that directs one of the layers to be fetched from a web server they control and they trick a user or system into pulling the image, they can obtain the credentials used for pulling that image. In some cases, this may be the user's username and password for the registry. In other cases, this may be the credentials attached to the cloud virtual instance which can grant access to other cloud resources in the account. The default containerd resolver is used by the cri-containerd plugin (which can be used by Kubernetes), the ctr development tool, and other client programs that have explicitly linked against it. This vulnerability has been fixed in containerd 1.2.14. containerd 1.3 and later are not affected. If you are using containerd 1.3 or later, you are not affected. If you are using cri-containerd in the 1.2 series or prior, you should ensure you only pull images from trusted sources. Other container runtimes built on top of containerd but not using the default resolver (such as Docker) are not affected.	6.1	More Details
CVE-2020-16270	OLIMPOKS under 3.3.39 allows Auth/Admin ErrorMessage XSS. Remote Attacker can use discovered vulnerability to inject malicious JavaScript payload to victim’s browsers in context of vulnerable applications. Executed code can be used to steal administrator’s cookies, influence HTML content of targeted application and perform phishing-related attacks. Vulnerable application used in more than 3000 organizations in different sectors from retail to industries.	6.1	More Details
CVE-2020-24188	Cross-site scripting (XSS) vulnerability in the search functionality in Intrexx before 9.4.0 allows remote attackers to inject arbitrary web script or HTML via the request parameter.	6.1	More Details
CVE-2020-7326	Improperly implemented security check in McAfee Active Response (MAR) prior to 2.4.4 may allow local administrators to execute malicious code via stopping a core Windows service leaving McAfee core trust component in an inconsistent state resulting in MAR failing open rather than closed	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25778	Trend Micro Antivirus for Mac 2020 (Consumer) has a vulnerability in a specific kernel extension where an attacker could supply a kernel pointer and leak several bytes of memory. An attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability.	6.0	More Details
CVE-2020-7327	Improperly implemented security check in McAfee MVISION Endpoint Detection and Response Client (MVEDR) prior to 3.2.0 may allow local administrators to execute malicious code via stopping a core Windows service leaving McAfee core trust component in an inconsistent state resulting in MVEDR failing open rather than closed	6.0	More Details
CVE-2020-6369	SAP Solution Manager and SAP Focused Run (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7), allows an unauthenticated attackers to bypass the authentication if the default passwords for Admin and Guest have not been changed by the administrator.This may impact the confidentiality of the service.	5.9	More Details
CVE-2020-3993	VMware NSX-T (3.x before 3.0.2, 2.5.x before 2.5.2.2.0) contains a security vulnerability that exists in the way it allows a KVM host to download and install packages from NSX manager. A malicious actor with MITM positioning may be able to exploit this issue to compromise the transport node.	5.9	More Details
CVE-2020-9909	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	5.9	More Details
CVE-2020-11637	A memory leak in the TFTP service in B&R Automation Runtime versions <N4.26, <N4.34, <F4.45, <E4.53, <D4.63, <A4.73 and prior could allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1685	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2.	5.8	More Details
CVE-2020-3981	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds read vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process.	5.8	More Details
CVE-2020-7748	This affects the package @tsed/core before 5.65.7. This vulnerability relates to the deepExtend function which is used as part of the utils directory. Depending on if user input is provided, an attacker can overwrite and pollute the object prototype of a program.	5.6	More Details
CVE-2020-0378	In onWnmFrameReceived of PasspointManager.java, there is a missing permission check. This could lead to local information disclosure of location data with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-157748906	5.5	More Details
CVE-2020-4756	IBM Spectrum Scale V4.2.0.0 through V4.2.3.23 and V5.0.0.0 through V5.0.5.2 as well as IBM Elastic Storage System 6.0.0 through 6.0.1.0 could allow a local attacker to invoke a subset of ioctls on the device with invalid arguments that could crash the keneral and cause a denial of service. IBM X-Force ID: 188599.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0246	In getCarrierPrivilegeStatus of UiccAccessRule.java, there is a missing permission check. This could lead to local information disclosure of EID data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-159062405	5.5	More Details
CVE-2020-0410	In setNotification of SapServer.java, there is a possible permission bypass due to a PendingIntent error. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-156021269	5.5	More Details
CVE-2020-6376	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated Right Hemisphere Binary (.rh) file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2020-6375	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated Right Computer Graphics Metafile (.cgm) file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	5.5	More Details
CVE-2020-6933	An improper input validation vulnerability in the UEM Core of BlackBerry UEM version(s) 12.13.0, 12.12.1a QF2 (and earlier), and 12.11.1 QF3 (and earlier) could allow an attacker to potentially cause a Denial of Service (DoS) of the UEM Core service.	5.5	More Details
CVE-2020-6315	SAP 3D Visual Enterprise Viewer, version 9, allows an attacker to send certain manipulated file to the victim, which can lead to leakage of sensitive information when the victim loads the malicious file into the VE viewer, leading to Information Disclosure.	5.5	More Details
CVE-2020-0419	In generateInfo of PackageInstallerSession.java, there is a possible leak of cross-profile URI data during app installation due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-142125338	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0415	In various locations in SystemUI, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure of contact data with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.0 Android-8.1Android ID: A-156020795	5.5	More Details
CVE-2020-0398	In updateMwi of NotificationMgr.java, there is a possible permission bypass due to a PendingIntent error. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-154323381	5.5	More Details
CVE-2020-0400	In showDataRoamingNotification of NotificationMgr.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-153356561	5.5	More Details
CVE-2020-4491	IBM Spectrum Scale V4.2.0.0 through V4.2.3.22 and V5.0.0.0 through V5.0.5 could allow a local attacker to cause a denial of service by sending a large number of RPC requests to the mmfsd daemon which would cause the service to crash. IBM X-Force ID: 181991.	5.5	More Details
CVE-2020-16889	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows KernelStream handles objects in memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16921	An information disclosure vulnerability exists in Text Services Framework when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. To exploit this vulnerability, an attacker would have to log on to an affected system and open a specially crafted file. The update addresses the vulnerability by correcting how Text Services Framework handles objects in memory.	5.5	More Details
CVE-2020-9913	This issue was addressed with improved data protection. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to leak sensitive user information.	5.5	More Details
CVE-2020-16914	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how GDI+ handles memory addresses.	5.5	More Details
CVE-2020-9968	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.7, tvOS 14.0, watchOS 7.0. A malicious application may be able to access restricted files.	5.5	More Details
CVE-2020-9976	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0. A malicious application may be able to leak sensitive user information.	5.5	More Details
CVE-2020-24352	An issue was discovered in QEMU through 5.1.0. An out-of-bounds memory access was found in the ATI VGA device implementation. This flaw occurs in the ati_2d_blt() routine in hw/display/ati_2d.c while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9885	An issue existed in the handling of iMessage tapbacks. The issue was resolved with additional verification. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A user that is removed from an iMessage group could rejoin the group.	5.5	More Details
CVE-2020-16919	An information disclosure vulnerability exists when the Windows Enterprise App Management Service improperly handles certain file operations. An attacker who successfully exploited this vulnerability could read arbitrary files. An attacker with unprivileged access to a vulnerable system could exploit this vulnerability. The security update addresses the vulnerability by ensuring the Windows Enterprise App Management Service properly handles file operations.	5.5	More Details
CVE-2020-1682	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version.	5.5	More Details
CVE-2020-16938	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9964	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 14.0 and iPadOS 14.0. A local user may be able to read kernel memory.	5.5	More Details
CVE-2020-27194	An issue was discovered in the Linux kernel before 5.8.15. scalar32_min_max_or in kernel/bpf/verifier.c mishandles bounds tracking during use of 64-bit values, aka CID-5b9fbeb75b6a.	5.5	More Details
CVE-2020-6104	An exploitable information disclosure vulnerability exists in the get_dnode_of_data functionality of F2fs-Tools F2fs.Fsck 1.13. A specially crafted f2fs filesystem can cause information disclosure resulting in a information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2020-16897	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how a NetBT handles objects in memory.	5.5	More Details
CVE-2020-6107	An exploitable information disclosure vulnerability exists in the dev_read functionality of F2fs-Tools F2fs.Fsck 1.13. A specially crafted f2fs filesystem can cause an uninitialized read resulting in an information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2020-6106	An exploitable information disclosure vulnerability exists in the init_node_manager functionality of F2fs-Tools F2fs.Fsck 1.12 and 1.13. A specially crafted filesystem can be used to disclose information. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2020-9934	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A local user may be able to view sensitive user information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16978	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-4395	IBM Security Access Manager Appliance 9.0.7 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 179358.	5.4	More Details
CVE-2020-16956	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-4755	IBM Spectrum Scale 5.0.0 through 5.0.5.2 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: 188595.	5.4	More Details
CVE-2020-26672	Testimonial Rotator Wordpress Plugin 3.0.2 is affected by Cross Site Scripting (XSS) in /wp-admin/post.php. If a user intercepts a request and inserts a payload in "cite" parameter, the payload will be stored in the database.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13893	Multiple stored cross-site scripting (XSS) vulnerabilities in Sage EasyPay 10.7.5.10 allow authenticated attackers to inject arbitrary web script or HTML via multiple parameters through Unicode Transformations (Best-fit Mapping), as demonstrated by the full-width variants of the less-than sign (%EF%BC%9C) and greater-than sign (%EF%BC%9E).	5.4	More Details
CVE-2020-4564	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.1 and IBM Sterling File Gateway 2.2.0.0 through 6.0.3.1 are 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: 183933.	5.4	More Details
CVE-2020-25777	Trend Micro Antivirus for Mac 2020 (Consumer) is vulnerable to a specific kernel extension request attack where an attacker could bypass the Web Threat Protection feature of the product. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	5.4	More Details
CVE-2020-6368	SAP Business Planning and Consolidation, versions - 750, 751, 752, 753, 754, 755, 810, 100, 200, can be abused by an attacker, allowing them to modify displayed application content without authorization, and to potentially obtain authentication information from other legitimate users, leading to Cross Site Scripting.	5.4	More Details
CVE-2020-15793	A vulnerability has been identified in Desigo Insight (All versions). The device does not properly set the X-Frame-Options HTTP Header which makes it vulnerable to Clickjacking attacks. This could allow an unauthenticated attacker to retrieve or modify data in the context of a legitimate user by tricking that user to click on a website controlled by the attacker.	5.4	More Details
CVE-2020-6272	SAP Commerce Cloud versions - 1808, 1811, 1905, 2005, does not sufficiently encode user inputs, which allows an authenticated and authorized content manager to inject malicious script into several web CMS components. These can be saved and later triggered, if an affected web page is visited, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16886	A security feature bypass vulnerability exists in the PowerShellGet V2 module. An attacker who successfully exploited this vulnerability could bypass WDAC (Windows Defender Application Control) policy and execute arbitrary code on a policy locked-down machine. An attacker must have administrator privileges to create a configuration that includes installing PowerShellGet V2 module onto a machine from the PowerShell Gallery. The WDAC policy must be configured to allow the module to run. After this is done, PowerShell script can be injected and run fully trusted, allowing the attacker arbitrary code execution on the machine. The update addresses the vulnerability by changing how URLs are processed.	5.3	More Details
CVE-2020-8929	A mis-handling of invalid unicode characters in the Java implementation of Tink versions prior to 1.5 allows an attacker to change the ID part of a ciphertext, which result in the creation of a second ciphertext that can decrypt to the same plaintext. This can be a problem with encrypting deterministic AEAD with a single key, and rely on a unique ciphertext-per-plaintext.	5.3	More Details
CVE-2020-3995	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time.	5.3	More Details
CVE-2020-1661	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16922	A spoofing vulnerability exists when Windows incorrectly validates file signatures. An attacker who successfully exploited this vulnerability could bypass security features and load improperly signed files. In an attack scenario, an attacker could bypass security features intended to prevent improperly signed files from being loaded. The update addresses the vulnerability by correcting how Windows validates file signatures.	5.3	More Details
CVE-2020-9916	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL.	5.3	More Details
CVE-2020-1665	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2.	5.3	More Details
CVE-2020-6308	SAP BusinessObjects Business Intelligence Platform (Web Services) versions - 410, 420, 430, allows an unauthenticated attacker to inject arbitrary values as CMS parameters to perform lookups on the internal network which is otherwise not accessible externally. On successful exploitation, attacker can scan internal network to determine internal infrastructure and gather information for further attacks like remote file inclusion, retrieve server files, bypass firewall and force the vulnerable server to perform malicious requests, resulting in a Server-Side Request Forgery vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13937	Apache Kylin 2.0.0, 2.1.0, 2.2.0, 2.3.0, 2.3.1, 2.3.2, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.5.2, 2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 3.0.0-alpha, 3.0.0-alpha2, 3.0.0-beta, 3.0.0, 3.0.1, 3.0.2, 3.1.0, 4.0.0-alpha has one restful api which exposed Kylin's configuration information without any authentication, so it is dangerous because some confidential information entries will be disclosed to everyone.	5.3	More Details
CVE-2020-16904	An elevation of privilege vulnerability exists in the way Azure Functions validate access keys. An unauthenticated attacker who successfully exploited this vulnerability could invoke an HTTP Function without proper authorization. This security update addresses the vulnerability by correctly validating access keys used to access HTTP Functions.	5.3	More Details
CVE-2020-14185	Affected versions of Jira Server allow remote unauthenticated attackers to enumerate issue keys via a missing permissions check in the ActionsAndOperations resource. The affected versions are before 7.13.18, from version 8.0.0 before 8.5.9, and from version 8.6.0 before version 8.12.2.	5.3	More Details
CVE-2020-1680	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2.	5.3	More Details
CVE-2020-16950	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles objects in memory.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16901	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory.	5.0	More Details
CVE-2020-6370	SAP NetWeaver Design Time Repository (DTR), versions - 7.11, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	4.8	More Details
CVE-2020-16937	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory. An attacker who successfully exploited the vulnerability could disclose contents of an affected system's memory. To exploit the vulnerability, an authenticated attacker would need to run a specially crafted application. The update addresses the vulnerability by correcting how the .NET Framework handles objects in memory.	4.7	More Details
CVE-2020-16949	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could cause a remote denial of service against a system. Exploitation of the vulnerability requires that a specially crafted email be sent to a vulnerable Outlook server. The security update addresses the vulnerability by correcting how Microsoft Outlook handles objects in memory.	4.7	More Details
CVE-2020-15910	SolarWinds N-Central version 12.3 GA and lower does not set the JSESSIONID attribute to HTTPOnly. This makes it possible to influence the cookie with javascript. An attacker could send the user to a prepared webpage or by influencing JavaScript to the extract the JESSIONID. This could then be forwarded to the attacker.	4.7	More Details
CVE-2020-7744	This affects all versions of package com.mintegral.msdk:alphab. The Android SDK distributed by the company contains malicious functionality in this module that tracks: 1. Downloads from Google urls either within Google apps or via browser including file downloads, e-mail attachments and Google Docs links. 2. All apk downloads, either organic or not. Mintegral listens to download events in Android's download manager and detects if the downloaded file's url contains: a. google.com or comes from a Google app (the com.android.vending package) b. Ends with .apk for apk downloads In both cases, the module sends the captured data back to Mintegral's servers. Note that the malicious functionality keeps running even if the app is currently not in focus (running in the background).	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7317	Cross-Site Scripting vulnerability in McAfee ePolicy Orchistrator (ePO) prior to 5.10.9 Update 9 allows administrators to inject arbitrary web script or HTML via parameter values for "syncPointList" not being correctly sanitsed.	4.6	More Details
CVE-2020-7318	Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10.9 Update 9 allows administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.	4.6	More Details
CVE-2020-9092	HUAWEI Mate 20 versions earlier than 10.1.0.163(C00E160R3P8) have a JavaScript injection vulnerability. A module does not verify a specific input. This could allow attackers to bypass filter mechanism to launch JavaScript injection. This could compromise normal service of the affected module.	4.6	More Details
CVE-2020-6363	SAP Commerce Cloud, versions - 1808, 1811, 1905, 2005, exposes several web applications that maintain sessions with a user. These sessions are established after the user has authenticated with username/passphrase credentials. The user can change their own passphrase, but this does not invalidate active sessions that the user may have with SAP Commerce Cloud web applications, which gives an attacker the opportunity to reuse old session credentials, resulting in Insufficient Session Expiration.	4.6	More Details
CVE-2020-9111	E6878-370 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP21C233) and E6878-870 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP11C233) have a denial of service vulnerability. The system does not properly check some events, an attacker could launch the events continually, successful exploit could cause reboot of the process.	4.5	More Details
CVE-2020-27013	Trend Micro Antivirus for Mac 2020 (Consumer) contains a vulnerability in the product that occurs when a webserver is started that implements an API with several properties that can be read and written to allowing the attacker to gather and modify sensitive product and user data. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	4.4	More Details
CVE-2020-7369	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of the Yandex Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects the Yandex Browser version 20.8.3 and prior versions, and was fixed in version 20.8.4 released October 1, 2020.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7371	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of the Yandex Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects the RITS Browser version 3.3.9 and prior versions.	4.3	More Details
CVE-2020-7370	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of Danyil Vasilenko's Bolt Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects the Bolt Browser version 1.4 and prior versions.	4.3	More Details
CVE-2020-11646	A log information disclosure vulnerability in B&R GateManager 4260 and 9250 versions <9.0.20262 and GateManager 8250 versions <9.2.620236042 allows authenticated users to view log information reserved for other users.	4.3	More Details
CVE-2020-7364	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of UCWeb's UC Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects UCWeb's UC Browser version 13.0.8 and prior versions.	4.3	More Details
CVE-2020-7363	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of UCWeb's UC Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects UCWeb's UC Browser version 13.0.8 and prior versions.	4.3	More Details
CVE-2020-6371	User enumeration vulnerability can be exploited to get a list of user accounts and personal user information can be exposed in SAP NetWeaver Application Server ABAP (POWL test application) versions - 710, 711, 730, 731, 740, 750, leading to Information Disclosure.	4.3	More Details
CVE-2020-15794	A vulnerability has been identified in Desigo Insight (All versions). Some error messages in the web application show the absolute path to the requested resource. This could allow an authenticated attacker to retrieve additional information about the host system.	4.3	More Details
CVE-2020-1777	Agent names that participates in a chat conversation are revealed in certain parts of the external interface as well as in chat transcriptions inside the tickets, when system is configured to mask real agent names. This issue affects OTRS; 7.0.21 and prior versions, 8.0.6 and prior versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15245	In Sylius before versions 1.6.9, 1.7.9 and 1.8.3, the user may register in a shop by email mail@example.com, verify it, change it to the mail another@domain.com and stay verified and enabled. This may lead to having accounts addressed to totally different emails, that were verified. Note, that this way one is not able to take over any existing account (guest or normal one). The issue has been patched in Sylius 1.6.9, 1.7.9 and 1.8.3. As a workaround, you may resolve this issue on your own by creating a custom event listener, which will listen to the sylius.customer.pre_update event. You can determine that email has been changed if customer email and user username are different. They are synchronized later on. Pay attention, to email changing behavior for administrators. You may need to skip this logic for them. In order to achieve this, you should either check master request path info, if it does not contain /admin prefix or adjust event triggered during customer update in the shop. You can find more information on how to customize the event here.	4.3	More Details
CVE-2020-9894	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	4.3	More Details
CVE-2020-15792	A vulnerability has been identified in Desigo Insight (All versions). The web service does not properly apply input validation for some query parameters in a reserved area. This could allow an authenticated attacker to retrieve data via a content-based blind SQL injection attack.	4.3	More Details
CVE-2020-4749	IBM Spectrum Scale 5.0.0 through 5.0.5.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 188518.	4.3	More Details
CVE-2020-16942	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages. An attacker who took advantage of this information disclosure could view the folder path of scripts loaded on the page. To take advantage of the vulnerability, an attacker would require access to the specific SharePoint page affected by this vulnerability. The security update addresses the vulnerability by correcting how scripts are referenced on some SharePoint pages.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16941	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages. An attacker who took advantage of this information disclosure could view the folder path of scripts loaded on the page. To take advantage of the vulnerability, an attacker would require access to the specific SharePoint page affected by this vulnerability. The security update addresses the vulnerability by correcting how scripts are referenced on some SharePoint pages.	4.1	More Details
CVE-2020-15262	In webpack-subresource-integrity before version 1.5.1, all dynamically loaded chunks receive an invalid integrity hash that is ignored by the browser, and therefore the browser cannot validate their integrity. This removes the additional level of protection offered by SRI for such chunks. Top-level chunks are unaffected. This issue is patched in version 1.5.1.	3.7	More Details
CVE-2020-9933	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to read sensitive location information.	3.3	More Details
CVE-2020-9912	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1.2. A malicious attacker may be able to change the origin of a frame for a download in Safari Reader mode.	3.3	More Details
CVE-2020-0422	In constructImportFailureNotification of NotificationImportExportListener.java, there is a possible permissions bypass due to an unsafe PendingIntent. This could lead to local information disclosure of contact data with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-161718556	3.3	More Details
CVE-2020-0412	In setProcessMemoryTrimLevel of ActivityManagerService.java, there is a missing permission check. This could lead to local information disclosure of foreground processes with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.0 Android-8.1 Android-9Android ID: A-160390416	3.3	More Details
CVE-2020-9959	A lock screen issue allowed access to messages on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0. A person with physical access to an iOS device may be able to view notification contents from the lockscreen.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25824	Telegram Desktop through 2.4.3 does not require passcode entry upon pushing the Export key within the Export Telegram Data wizard. The threat model is a victim who has voluntarily opened Export Wizard but is then distracted. An attacker then approaches the unattended desktop and pushes the Export key. This attacker may consequently gain access to all chat conversation and media files.	2.4	More Details
CVE-2020-1674	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a vulnerability. Notes: The fix resolved an issue when MACsec replay-protect was enabled and the replay-protect-window value was set to zero, Junos OS was incorrectly configuring the value to MAX_WINDOW size. Hence this is not a vulnerability and this CVE ID assignment has been withdrawn	N/A	More Details
CVE-2020-13939	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2019-12411	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details