SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 April 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-2020-10505	The School Manage System before 2020, developed by ALLE INFORMATION CO., LTD., contains a vulnerability of SQL Injection, an attacker can use a union based injection query string to get databases schema and username/password.	9.8	More Details
CVE-2019-12002	A remote session reuse vulnerability leading to access restriction bypass was discovered in HPE MSA 2040 SAN Storage; HPE MSA 1040 SAN Storage; HPE MSA 1050 SAN Storage; HPE MSA 2042 SAN Storage; HPE MSA 2050 SAN Storage; HPE MSA 2052 SAN Storage version(s): GL225P001 and earlier; GL225P001 and earlier; VE270R001-01 and earlier; GL225P001 and earlier; VL270R001-01 and earlier; VL270R001-01 and earlier.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10211	A remote code execution vulnerability in UCB component of Mitel MiVoice Connect before 19.1 SP1 could allow an unauthenticated remote attacker to execute arbitrary scripts due to insufficient validation of URL parameters. A successful exploit could allow an attacker to gain access to sensitive information.	9.8	More Details
CVE-2019-20730	Certain NETGEAR devices are affected by SQL injection. This affects D3600 before 1.0.0.68, D6000 before 1.0.0.68, D6200 before 1.1.00.28, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7000v2 before 1.0.0.74, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DC112A before 1.0.0.40, EX8000 before 1.0.0.118, JR6150 before 1.0.1.18, R6050 before 1.0.1.18, R6220 before 1.1.0.66, R6250 before 1.0.4.26, R6300v2 before 1.0.4.24, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6700v2 before 1.2.0.16, R6800 before 1.2.0.16, R6900v2 before 1.2.0.16, R6900 before 1.0.1.44, R7000 before 1.0.9.26, R6900P before 1.3.0.20, R7000P before 1.3.0.20, R7100LG before 1.0.0.40, R7300DST before 1.0.0.62, R7500 before 1.0.0.118, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R7900 before 1.0.2.10, R8000 before 1.0.4.12, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, R8900 before 1.0.3.6, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.102, WNDR3700v5 before 1.1.0.54, WNDR4300v1 before 1.0.2.98, WNDR4300v2 before 1.0.0.56, and WNDR4500v3 before 1.0.0.56.	9.8	More Details
CVE-2020-7485	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy support account in the TriStation software version v4.9.0 and earlier could cause improper access to the TriStation host machine. This was addressed in TriStation version v4.9.1 and v4.10.1 released on May 30, 2013.1	9.8	More Details
CVE-2020-7224	The Aviatrix OpenVPN client through 2.5.7 on Linux, macOS, and Windows is vulnerable when OpenSSL parameters are altered from the issued value set; the parameters could allow unauthorized third-party libraries to load.	9.8	More Details
CVE-2020-7114	A vulnerability exists allowing attackers, when present in the same network segment as ClearPass' management interface, to make changes to certain databases in ClearPass by crafting HTTP packets. As a result of this attack, a possible complete cluster compromise might occur. Resolution: Fixed in 6.7.13, 6.8.4, 6.9.0 and higher.	9.8	More Details
CVE-2020-1964	It was noticed that Apache Heron 0.20.2-incubating, Release 0.20.1-incubating, and Release v-0.20.0-incubating does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerabilities (CWE-502: Deserialization of Untrusted Data).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11820	Rukovoditel 2.5.2 is affected by a SQL injection vulnerability because of improper handling of the entities_id parameter.	9.8	More Details
CVE-2020-11819	In Rukovoditel 2.5.2, an attacker may inject an arbitrary .php file location instead of a language file and thus achieve command execution.	9.8	More Details
CVE-2020-11816	Rukovoditel 2.5.2 is affected by a SQL injection vulnerability because of improper handling of the reports_id (POST) parameter.	9.8	More Details
CVE-2020-11815	In Rukovoditel 2.5.2, attackers can upload arbitrary file to the server by just changing the content-type value. As a result of that, an attacker can execute a command on the server. This specific attack only occurs without the Maintenance Mode setting.	9.8	More Details
CVE-2020-11812	Rukovoditel 2.5.2 is affected by a SQL injection vulnerability because of improper handling of the filters[0][value] or filters[1][value] parameter.	9.8	More Details
CVE-2020-11811	In qdPM 9.1, an attacker can upload a malicious .php file to the server by exploiting the Add Profile Photo capability with a crafted content-type value. After that, the attacker can execute an arbitrary command on the server using this malicious file.	9.8	More Details
CVE-2019-20699	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects GS105Ev2 before 1.6.0.4, GS105PE before 1.6.0.4, GS408EPP before 1.0.0.15, GS808E before 1.7.0.7, GS908E before 1.7.0.3, GSS108E before 1.6.0.4, and GSS108EPP before 1.0.0.15.	9.8	More Details
CVE-2019-14134	Possible out of bound access in WLAN handler when the received value of length in rx path is shorter than the expected value of country IE in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-14132	Buffer over-write when this 0-byte buffer is typecasted to some other structure and hence memory corruption in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SA6155P, SM8150	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14131	Out of bound write can occur in radio measurement request if STA receives multiple invalid rrm measurement request from AP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8998, Nicobar, QCA6574AU, QCS605, Rennell, SA6155P, Saipan, SC8180X, SDM660, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2019-14127	Possible buffer overflow while playing mkv clip due to lack of validation of atom size buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2020-10507	The School Manage System before 2020, developed by ALLE INFORMATION CO., LTD., contains a vulnerability of Unrestricted file upload (RCE) , that would allow attackers to gain access in the hosting machine.	9.8	More Details
CVE-2019-14113	Buffer overflow can occur in In WLAN firmware while unwraping data using CCMP cipher suite during parsing of EAPOL handshake frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, Nicobar, QCA4531, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS404, QCS405, QCS605, Rennell, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130, SXR2130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10377	A weak encryption vulnerability in Mitel MiVoice Connect Client before 214.100.1214.0 could allow an unauthenticated attacker to gain access to user credentials. A successful exploit could allow an attacker to access the system with compromised user credentials.	9.8	More Details
CVE-2019-20772	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Account subsystem allows authorization bypass. The LG ID is LVE-SMP-190007 (August 2019).	9.8	More Details
CVE-2019-14111	Possible buffer overflow while handling NAN reception of NMF in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, Rennell, SC7180, SC8180X, SM6150, SM7150, SM8150, SXR2130	9.8	More Details
CVE-2019-20777	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService mishandles OTA Provisioning on V40 and G7 devices. The LG ID is LVE-SMP-190006 (July 2019).	9.8	More Details
CVE-2020-11967	In IQrouter through 3.3.1, remote attackers can control the device (restart network, reboot, upgrade, reset) because of Incorrect Access Control. Note: The vendor claims that this vulnerability can only occur on a brand-new network that, after initiating the forced initial configuration (which has a required step for setting a secure password on the system), makes this CVE invalid. This vulnerability is “true for any unconfigured release of OpenWRT, and true of many other new Linux distros prior to being configured for the first time”	9.8	More Details
CVE-2020-11966	In IQrouter through 3.3.1, the Lua function reset_password in the web-panel allows remote attackers to change the root password arbitrarily. Note: The vendor claims that this vulnerability can only occur on a brand-new network that, after initiating the forced initial configuration (which has a required step for setting a secure password on the system), makes this CVE invalid. This vulnerability is “true for any unconfigured release of OpenWRT, and true of many other new Linux distros prior to being configured for the first time”	9.8	More Details
CVE-2020-11965	In IQrouter through 3.3.1, there is a root user without a password, which allows attackers to gain full remote access via SSH. Note: The vendor claims that this vulnerability can only occur on a brand-new network that, after initiating the forced initial configuration (which has a required step for setting a secure password on the system), makes this CVE invalid. This vulnerability is “true for any unconfigured release of OpenWRT, and true of many other new Linux distros prior to being configured for the first time”	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11963	IQrouter through 3.3.1, when unconfigured, has multiple remote code execution vulnerabilities in the web-panel because of Bash Shell Metacharacter Injection. Note: The vendor claims that this vulnerability can only occur on a brand-new network that, after initiating the forced initial configuration (which has a required step for setting a secure password on the system), makes this CVE invalid. This vulnerability is “true for any unconfigured release of OpenWRT, and true of many other new Linux distros prior to being configured for the first time”	9.8	More Details
CVE-2020-9279	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A hard-coded account allows management-interface login with high privileges. The logged-in user can perform critical tasks and take full control of the device.	9.8	More Details
CVE-2020-9277	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. Authentication can be bypassed when accessing cgi modules. This allows one to perform administrative tasks (e.g., modify the admin password) with no authentication.	9.8	More Details
CVE-2020-9275	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A cfm UDP service listening on port 65002 allows remote, unauthenticated exfiltration of administrative credentials.	9.8	More Details
CVE-2020-11928	In the media-library-assistant plugin before 2.82 for WordPress, Remote Code Execution can occur via the tax_query, meta_query, or date_query parameter in mla_gallery via an admin.	9.8	More Details
CVE-2019-20786	handleIncomingPacket in conn.go in Pion DTLS before 1.5.2 lacks a check for application data with epoch 0, which allows remote attackers to inject arbitrary unencrypted data after handshake completion.	9.8	More Details
CVE-2020-0073	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147309942	9.8	More Details
CVE-2020-0072	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310271	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0071	In rw_t2t_extract_default_locks_info of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310721	9.8	More Details
CVE-2020-0070	In rw_t2t_update_lock_attributes of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148159613	9.8	More Details
CVE-2019-6203	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. An attacker in a privileged network position may be able to intercept network traffic.	9.8	More Details
CVE-2020-11878	The Jitsi Meet (aka docker-jitsi-meet) stack on Docker before stable-4384-1 uses default passwords (such as passw0rd) for system accounts.	9.8	More Details
CVE-2020-11873	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A stack-based buffer overflow in the logging tool could allow an attacker to gain privileges. The LG ID is LVE-SMP-200005 (April 2020).	9.8	More Details
CVE-2019-20782	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. LG Advanced Flash (LAF) has a buffer overflow. The LG ID is LVE-SMP-190001 (March 2019).	9.8	More Details
CVE-2019-20780	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. Certain security settings, related to whether packages are verified and accepted only from known sources, are mishandled. The LG ID is LVE-SMP-190002 (April 2019).	9.8	More Details
CVE-2019-20778	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Backup subsystem does not properly restrict operations or validate their input. The LG ID is LVE-SMP-190004 (June 2019).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14112	Potential buffer overflow while processing CBF frames due to lack of check of buffer length before copy in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ6018, IPQ8074, MSM8998, Nicobar, QCA8081, QCN7605, QCS404, QCS605, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130	9.8	More Details
CVE-2019-14114	Buffer overflow in WLAN firmware while parsing GTK IE containing GTK key having length more than the buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, Nicobar, QCA4531, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS404, QCS405, QCS605, Rennell, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130, SXR2130	9.8	More Details
CVE-2019-14110	Buffer overflow can occur in function wlan firmware while copying association frame content if frame length is more than the maximum buffer size in case of SAP mode in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA4531, QCA6174A, QCA6564, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS404, QCS405, QCS605, Rennell, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130, SXR2130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10611	Triangle MicroWorks SCADA Data Gateway 3.02.0697 through 4.0.122, 2.41.0213 through 4.0.122 allows remote attackers to execute arbitrary code due to the lack of proper validation of user-supplied data, which can result in a type confusion condition. Authentication is not required to exploit this vulnerability. Only applicable to installations using DNP3 Data Sets.	9.8	More Details
CVE-2020-11789	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects R6400v2 before 1.0.4.84, R6700 before 1.0.2.8, R6700v3 before 1.0.4.84, R6900 before 1.0.2.8, and R7900 before 1.0.3.10.	9.8	More Details
CVE-2019-20646	NETGEAR RAX40 devices before 1.0.3.64 are affected by disclosure of administrative credentials.	9.8	More Details
CVE-2020-11729	An issue was discovered in DAViCal Andrew's Web Libraries (AWL) through 0.60. Long-term session cookies, uses to provide long-term session continuity, are not generated securely, enabling a brute-force attack that may be successful.	9.8	More Details
CVE-2020-1026	A Security Feature Bypass vulnerability exists in the MSR JavaScript Cryptography Library that is caused by multiple bugs in the libraryâ€™s Elliptic Curve Cryptography (ECC) implementation.An attacker could potentially abuse these bugs to learn information about a serverâ€™s private ECC key (a key leakage attack) or craft an invalid ECDSA signature that nevertheless passes as valid.The security update addresses the vulnerability by fixing the bugs disclosed in the ECC implementation, aka 'MSR JavaScript Cryptography Library Security Feature Bypass Vulnerability'.	9.8	More Details
CVE-2020-11537	A SQL Injection issue was discovered in ONLYOFFICE Document Server 5.5.0. An attacker can execute arbitrary SQL queries via injection to DocID parameter of Websocket API.	9.8	More Details
CVE-2020-11536	An issue was discovered in ONLYOFFICE Document Server 5.5.0. An attacker can craft a malicious .docx file, and exploit the unzip function to rewrite a binary and remotely execute code on a victim's server.	9.8	More Details
CVE-2020-11535	An issue was discovered in ONLYOFFICE Document Server 5.5.0. An attacker can craft a malicious .docx file, and exploit XML injection to enter an attacker-controlled parameter into the x2t binary, to rewrite this binary and/or libxcb.so.1, and execute code on a victim's server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11534	An issue was discovered in ONLYOFFICE Document Server 5.5.0. An attacker can craft a malicious .docx file, and exploit the NSFileDownloader function to pass parameters to a binary (such as curl or wget) and remotely execute code on a victim's server.	9.8	More Details
CVE-2020-2961	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Discovery Framework (Oracle OHS)). Supported versions that are affected are 13.2.0.0 and 13.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Enterprise Manager Base Platform. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2953	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Promotions). The supported version that is affected is 18.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in takeover of Oracle Retail Customer Management and Segmentation Foundation. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2950	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2931	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Web Applications - InfoCenter). Supported versions that are affected are 8.6.0-8.6.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks of this vulnerability can result in takeover of Oracle Knowledge. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2915	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Caching, CacheStore, Invocation). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2884	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2883	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2801	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. Note: The patch for this issue will address the vulnerability only if the WLS instance is using JDK 1.7.0_191 or later, or JDK 1.8.0_181 or later. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2791	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Information Manager Console). Supported versions that are affected are 8.6.0-8.6.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks of this vulnerability can result in takeover of Oracle Knowledge. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-2733	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Monitoring and Diagnostics). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-10511	HGiga C&Cmail CCMAILQ before olln-base-6.0-418.i386.rpm and CCMAILN before olln-base-5.0-418.i386.rpm contains insecure configurations. Attackers can exploit these flaws to access unauthorized functionality via a crafted URL.	9.8	More Details
CVE-2019-12524	An issue was discovered in Squid through 4.7. When handling requests from users, Squid checks its rules to see if the request should be denied. Squid by default comes with rules to block access to the Cache Manager, which serves detailed server information meant for the maintainer. This rule is implemented via url_regex. The handler for url_regex rules URL decodes an incoming request. This allows an attacker to encode their URL to bypass the url_regex check, and gain access to the blocked resource.	9.8	More Details
CVE-2020-11790	NETGEAR R7800 devices before 1.0.2.68 are affected by remote code execution by unauthenticated attackers.	9.8	More Details
CVE-2020-11799	Z-Cron 5.6 Build 04 allows an unprivileged attacker to elevate privileges by modifying a privileged user's task. This can also affect all users who are signed in on the system if a shell is placed in a location that other unprivileged users have access to.	9.8	More Details
CVE-2020-3247	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10609	Out of bound write can happen due to lack of check of array index value while calculating it. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-10589	Lack of length check of response buffer can lead to buffer over-flow while GP command response buffer handling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, MDM9206, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QM215, SDA660, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660	9.8	More Details
CVE-2020-6996	Triangle MicroWorks DNP3 Outstation LibrariesDNP3 Outstation .NET Protocol components and DNP3 Outstation ANSI C source code libraries are affected:3.16.00 through 3.25.01. A specially crafted message may cause a stack-based buffer overflow. Authentication is not required to exploit this vulnerability.	9.8	More Details
CVE-2019-10588	Copying RTCP messages into the output buffer without checking the destination buffer size which could lead to a remote stack overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3250	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2020-3248	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2020-10569	SysAid On-Premise 20.1.11, by default, allows the AJP protocol port, which is vulnerable to a GhostCat attack. Additionally, it allows unauthenticated access to upload files, which can be used to execute commands on the system by chaining it with a GhostCat attack. NOTE: This may be a duplicate of CVE-2020-1938	9.8	More Details
CVE-2020-3243	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2019-20679	NETGEAR MR1100 devices before 12.06.08.00 are affected by lack of access control at the function level.	9.8	More Details
CVE-2020-11658	CA API Developer Portal 4.3.1 and earlier handles shared secret keys in an insecure manner, which allows attackers to bypass authorization.	9.8	More Details
CVE-2019-12519	An issue was discovered in Squid through 4.7. When handling the tag esi:when when ESI is enabled, Squid calls ESIExpression::Evaluate. This function uses a fixed stack buffer to hold the expression while it's being evaluated. When processing the expression, it could either evaluate the top of the stack, or add a new member to the stack. When adding a new member, there is no check to ensure that the stack won't overflow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3161	A vulnerability in the web server for Cisco IP Phones could allow an unauthenticated, remote attacker to execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web server of a targeted device. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a DoS condition.	9.8	More Details
CVE-2019-19108	An authentication weakness in the SNMP service in B&R Automation Runtime versions 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, 4.72 and above allows unauthenticated users to modify the configuration of B&R products via SNMP.	9.4	More Details
CVE-2020-11895	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (2 bytes) in the function decompileIF() in decompile.c.	9.1	More Details
CVE-2019-10551	String error while processing non standard SIP messages received can lead to buffer overread and then denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-14033	Multiple Read overflows issue due to improper length check while decoding tau reject/tau accept/detach request/attach reject/attach accept in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20783	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (North America CDMA) software. The LTE protocol implementation allows a bypass of AKA (Authentication and Key Agreement). The LG ID is LVE-SMP-180014 (February 2019).	9.1	More Details
CVE-2020-3653	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850	9.1	More Details
CVE-2020-3652	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850	9.1	More Details
CVE-2020-9278	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The device can be reset to its default configuration by accessing an unauthenticated URL.	9.1	More Details
CVE-2019-10610	Possible buffer over read when trying to process SDP message Video media line with frame-size attribute in video Media line in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-10622	Out of bound memory access can happen while parsing ADSP message due to lack of check of size of payload received from userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, QCN7605, QCS605, SC8180X, SDM710, SDX24, SDX55, SM8150, SM8250, SXR2130	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14011	Multiple Read overflows issue due to improper length check while decoding 3G attach accept/ SMS/ pdn connection reject/ esm data transport/ bearer modify context reject in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-14019	Multiple Read overflows issue due to improper length check while decoding RAU accept/PDN disconnect Rej/Modify EPS ctxt req/bearer resource alloc Rej/Deact EPs bearer REq in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-14020	Multiple Read overflows issue due to improper length check while decoding dedicated_eps_bearer_req/ act_def_context_req/ cs_serv_notification/ emm_info/ guti_realloc_cmd in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11894	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (8 bytes) in the function decompileIF() in decompile.c.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-11753	An issue was discovered in Sonatype Nexus Repository Manager in versions 3.21.1 and 3.22.0. It is possible for a user with appropriate privileges to create, modify, and execute scripting tasks without use of the UI or API. NOTE: in 3.22.0, scripting is disabled by default (making this not exploitable).	8.8	More Details
CVE-2020-0929	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0931, CVE-2020-0932, CVE-2020-0971, CVE-2020-0974.	8.8	More Details
CVE-2020-10786	A remote command execution in Vesta Control Panel through 0.9.8-26 allows any authenticated user to execute arbitrary commands on the system via cron jobs.	8.8	More Details
CVE-2020-10787	An elevation of privilege in Vesta Control Panel through 0.9.8-26 allows an attacker to gain root system access from the admin account via v-change-user-password (aka the user password change script).	8.8	More Details
CVE-2020-0950	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0948, CVE-2020-0949.	8.8	More Details
CVE-2020-0949	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0948, CVE-2020-0950.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2944	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.8	More Details
CVE-2020-0948	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0949, CVE-2020-0950.	8.8	More Details
CVE-2020-1020	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0938.	8.8	More Details
CVE-2020-0932	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0929, CVE-2020-0931, CVE-2020-0971, CVE-2020-0974.	8.8	More Details
CVE-2020-0931	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0929, CVE-2020-0932, CVE-2020-0971, CVE-2020-0974.	8.8	More Details
CVE-2019-20682	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.32, D7000 before 1.0.1.68, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.38, R6050 before 1.0.1.18, R6080 before 1.0.0.38, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.40, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.32.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20683	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.32, D7000 before 1.0.1.68, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.38, R6050 before 1.0.1.18, R6080 before 1.0.0.38, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.40, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.32.	8.8	More Details
CVE-2019-20684	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6200 before 1.1.00.32, D7000 before 1.0.1.68, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.38, R6050 before 1.0.1.18, R6080 before 1.0.0.38, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.40, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.32.	8.8	More Details
CVE-2019-20685	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6200 before 1.1.00.32, D7000 before 1.0.1.68, DM200 before 1.0.0.58, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.38, R6050 before 1.0.1.18, R6080 before 1.0.0.38, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.40, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.32.	8.8	More Details
CVE-2019-20686	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.36, D7000 before 1.0.1.74, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.40, R6080 before 1.0.0.40, R6050 before 1.0.1.18, R6120 before 1.0.0.48, R6220 before 1.1.0.86, R6260 before 1.1.0.64, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, and WNR2020 before 1.1.0.62.	8.8	More Details
CVE-2019-20690	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.30, D7000 before 1.0.1.66, R6020 before 1.0.0.34, R6080 before 1.0.0.34, R6120 before 1.0.0.44, R6220 before 1.1.0.68, WNR2020 before 1.1.0.54, and WNR614 before 1.1.0.54.	8.8	More Details
CVE-2019-20691	Certain NETGEAR devices are affected by CSRF. This affects D3600 before 1.0.0.72, D6000 before 1.0.0.72, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, and WN2500RPv2 before 1.0.1.54.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20697	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects GS728TPPv2 before 6.0.0.48, GS728TPv2 before 6.0.0.48, GS750E before 1.0.1.4, GS752TPP before 6.0.0.48, and GS752TPv2 before 6.0.0.48.	8.8	More Details
CVE-2020-3251	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2020-3239	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2020-11666	CA API Developer Portal 4.3.1 and earlier contains an access control flaw that allows malicious users to elevate privileges.	8.8	More Details
CVE-2019-20656	Certain NETGEAR devices are affected by a hardcoded password. This affects D6200 before 1.1.00.36, D7000 before 1.0.1.74, PR2000 before 1.0.0.30, R6020 before 1.0.0.42, R6080 before 1.0.0.42, R6050 before 1.0.1.24, JR6150 before 1.0.1.24, R6120 before 1.0.0.48, R6220 before 1.1.0.86, R6230 before 1.1.0.86, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, and WNR2020 before 1.1.0.62.	8.8	More Details
CVE-2020-0577	Insufficient control flow for Intel(R) Modular Server MFS2600KISPP Compute Module may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-0578	Improper conditions check for Intel(R) Modular Server MFS2600KISPP Compute Module may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20640	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.32, D7000 before 1.0.1.68, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.38, R6050 before 1.0.1.18, R6080 before 1.0.0.38, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.40, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.32.	8.8	More Details
CVE-2019-20641	NETGEAR RAX40 devices before 1.0.3.64 are affected by lack of access control at the function level.	8.8	More Details
CVE-2020-0981	A security feature bypass vulnerability exists when Windows fails to properly handle token relationships.An attacker who successfully exploited the vulnerability could allow an application with a certain integrity level to execute code at a different integrity level, leading to a sandbox escape.The update addresses the vulnerability by correcting how Windows handles token relationships, aka 'Windows Token Security Feature Bypass Vulnerability'.	8.8	More Details
CVE-2020-11788	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.34, D7000 before 1.0.1.68, PR2000 before 1.0.0.28, R6050 before 1.0.1.18, JR6150 before 1.0.1.18, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6230 before 1.1.0.80, R6260 before 1.1.0.64, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, and R6900v2 before 1.2.0.36.	8.8	More Details
CVE-2020-0979	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0906.	8.8	More Details
CVE-2020-0974	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0929, CVE-2020-0931, CVE-2020-0932, CVE-2020-0971.	8.8	More Details
CVE-2020-9276	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The function do_cgi(), which processes cgi requests supplied to the device's web servers, is vulnerable to a remotely exploitable stack-based buffer overflow. Unauthenticated exploitation is possible by combining this vulnerability with CVE-2020-9277.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0971	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0929, CVE-2020-0931, CVE-2020-0932, CVE-2020-0974.	8.8	More Details
CVE-2020-0967	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0966.	8.8	More Details
CVE-2020-0966	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0967.	8.8	More Details
CVE-2020-2902	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.8	More Details
CVE-2017-18848	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.0.36, AC1450 before 1.0.0.36, R7300 before 1.0.0.54, and R8500 before 1.0.2.94.	8.8	More Details
CVE-2020-0964	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2019-20681	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.34, D7000 before 1.0.1.68, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6050 before 1.0.1.18, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, and R6900v2 before 1.2.0.36.	8.8	More Details
CVE-2017-18791	Certain NETGEAR devices are affected by CSRF. This affects R6050/JR6150 before 1.0.1.7, PR2000 before 1.0.0.17, R6220 before 1.1.0.50, WNDR3700v5 before 1.1.0.48, JNR1010v2 before 1.1.0.40, JWNR2010v5 before 1.1.0.40, WNR1000v4 before 1.1.0.40, WNR2020 before 1.1.0.40, WNR2050 before 1.1.0.40, WNR614 before 1.1.0.40, WNR618 before 1.1.0.40, and D7000 before 1.0.1.50.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18842	Certain NETGEAR devices are affected by CSRF. This affects R7300 before 1.0.0.54, R8500 before 1.0.2.94, DGN2200v1 before 1.0.0.55, and D2200D/D2200DW-1FRNAS before 1.0.0.32.	8.8	More Details
CVE-2020-4272	IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow a remote attacker to include arbitrary files. A remote attacker could send a specially-crafted request specify a malicious file from a remote system, which could allow the attacker to execute arbitrary code on the vulnerable server. IBM X-ForceID: 175898.	8.8	More Details
CVE-2020-11793	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash).	8.8	More Details
CVE-2019-20734	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.40, D8500 before 1.0.3.39, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6300v2 before 1.0.4.18, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6700v3 before 1.0.2.32, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R6900P before 1.0.0.56, R7000P before 1.0.0.56, R7100LG before 1.0.0.42, R7300DST before 1.0.0.54, R7900 before 1.0.1.26, R8300 before 1.0.2.106, R8500 before 1.0.2.106, WN2500RPv2 before 1.0.1.54, and WNR3500Lv2 before 1.2.0.46. NOTE: this may be a result of an incomplete fix for CVE-2017-18864.	8.8	More Details
CVE-2019-20739	NETGEAR R8500 devices before v1.0.2.128 are affected by a buffer overflow by an unauthenticated attacker.	8.8	More Details
CVE-2019-17525	The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20753	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects DGN2200v1 before 1.0.0.58, D8500 before 1.0.3.42, D7000v2 before 1.0.0.51, D6400 before 1.0.0.78, D6220 before 1.0.0.44, JNDR3000 before 1.0.0.24, R8000 before 1.0.4.18, R8500 before 1.0.2.122, R8300 before 1.0.2.122, R7900 before 1.0.2.16, R7000P before 1.3.2.34, R7300DST before 1.0.0.68, R7100LG before 1.0.0.46, R6900P before 1.3.2.34, R7000 before 1.0.9.28, R6900 before 1.0.1.46, R6700 before 1.0.1.46, R6400v2 before 1.0.2.56, R6400 before 1.0.1.42, R6300v2 before 1.0.4.28, R6250 before 1.0.4.26, WNDR3400v3 before 1.0.1.22, WNDR4500v2 before 1.0.0.72, and WNR3500Lv2 before 1.2.0.50.	8.8	More Details
CVE-2019-20760	NETGEAR R9000 devices before 1.0.4.26 are affected by authentication bypass.	8.8	More Details
CVE-2020-11770	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7000v2 before 1.0.0.53, D8500 before 1.0.3.44, R6220 before 1.1.0.80, R6250 before 1.0.4.34, R6260 before 1.1.0.64, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6700v3 before 1.0.2.66, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7100LG before 1.0.0.50, R7300DST before 1.0.0.70, R7800 before 1.0.2.60, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, R8500 before 1.0.2.128, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.32.	8.8	More Details
CVE-2020-10947	Mac Endpoint for Sophos Central before 9.9.6 and Mac Endpoint for Sophos Home before 2.2.6 allow Privilege Escalation.	8.8	More Details
CVE-2019-2880	Vulnerability in the Oracle Retail Store Inventory Management product of Oracle Retail Applications (component: Security). The supported version that is affected is 16.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Store Inventory Management. Successful attacks of this vulnerability can result in takeover of Oracle Retail Store Inventory Management. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2179	Jenkins Yaml Axis Plugin 0.2.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-0920	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0929, CVE-2020-0931, CVE-2020-0932, CVE-2020-0971, CVE-2020-0974.	8.8	More Details
CVE-2020-9523	Insufficiently protected credentials vulnerability on Micro Focus enterprise developer and enterprise server, affecting all version prior to 4.0 Patch Update 16, and version 5.0 Patch Update 6. The vulnerability could allow an attacker to transmit hashed credentials for the user account running the Micro Focus Directory Server (MFDS) to an arbitrary site, compromising that account's security.	8.8	More Details
CVE-2020-0687	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-7081	A type confusion vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitary code read/write on the system running it.	8.8	More Details
CVE-2020-7082	A use-after-free vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to code execution on a system running it.	8.8	More Details
CVE-2020-0760	A remote code execution vulnerability exists when Microsoft Office improperly loads arbitrary type libraries, aka 'Microsoft Office Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0991.	8.8	More Details
CVE-2020-0906	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0979.	8.8	More Details
CVE-2020-2180	Jenkins AWS SAM Plugin 1.2.2 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-10514	iCatch DVR firmware before 20200103 do not validate function parameter properly, resulting attackers executing arbitrary command.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10512	HGiga C&Cmail CCMAILQ before olln-calendar-6.0-100.i386.rpm and CCMAILN before olln-calendar-5.0-100.i386.rpm contains a SQL Injection vulnerability which allows attackers to injecting SQL commands in the URL parameter to execute unauthorized commands.	8.8	More Details
CVE-2020-11825	In Dolibarr 10.0.6, forms are protected with a CSRF token against CSRF attacks. The problem is any CSRF token in any user's session can be used in another user's session. CSRF tokens should not be valid in this situation.	8.8	More Details
CVE-2020-11818	In Rukovoditel 2.5.2 has a form_session_token value to prevent CSRF attacks. This protection mechanism can be bypassed with another user's valid token. Thus, an attacker can change the Admin password by using a CSRF attack and escalate his/her privileges.	8.8	More Details
CVE-2017-18852	Certain NETGEAR devices are affected by CSRF and authentication bypass. This affects R7300DST before 1.0.0.54, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and WNDR3400v3 before 1.0.1.14.	8.8	More Details
CVE-2020-10513	The file management interface of iCatch DVR firmware before 20200103 contains broken access control which allows the attacker to remotely manipulate arbitrary file.	8.8	More Details
CVE-2020-2838	Vulnerability in the Oracle CRM Gateway for Mobile Devices product of Oracle E-Business Suite (component: Setup of Mobile Applications). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Gateway for Mobile Devices. While the vulnerability is in Oracle CRM Gateway for Mobile Devices, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Gateway for Mobile Devices accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2959	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via MLD to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).	8.6	More Details
CVE-2020-1632	In a certain condition, receipt of a specific BGP UPDATE message might cause Juniper Networks Junos OS and Junos OS Evolved devices to advertise an invalid BGP UPDATE message to other peers, causing the other peers to terminate the established BGP session, creating a Denial of Service (DoS) condition. For example, Router A sends a specific BGP UPDATE to Router B, causing Router B to send an invalid BGP UPDATE message to Router C, resulting in termination of the BGP session between Router B and Router C. This issue might occur when there is at least a single BGP session established on the device that does not support 4 Byte AS extension (RFC 4893). Repeated receipt of the same BGP UPDATE can result in an extended DoS condition. This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R1-S9, 17.2R2-S8, 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D105, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2-S6, 18.2R3-S2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D51, 18.2X75-D60; 18.3 versions prior to 18.3R1-S6, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R3; 18.4 version 18.4R2 and later versions; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S2, 19.2R2. This issue does not affect Juniper Networks Junos OS prior to 16.1R1. This issue affects Juniper Networks Junos OS Evolved prior to 19.2R2-EVO.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2776	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 8.6 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).	8.6	More Details
CVE-2020-2863	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. While the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	8.5	More Details
CVE-2020-5569	An unquoted search path vulnerability exists in HDD Password tool (for Windows) version 1.20.6620 and earlier which is stored in CANVIO PREMIUM 3TB(HD-MB30TY, HD-MA30TY, HD-MB30TS, HD-MA30TS), CANVIO PREMIUM 2TB(HD-MB20TY, HD-MA20TY, HD-MB20TS, HD-MA20TS), CANVIO PREMIUM 1TB(HD-MB10TY, HD-MA10TY, HD-MB10TS, HD-MA10TS), CANVIO SLIM 1TB(HD-SB10TK, HD-SB10TS), and CANVIO SLIM 500GB(HD-SB50GK, HD-SA50GK, HD-SB50GS, HD-SA50GS), and which was downloaded before 2020 May 10. Since it registers Windows services with unquoted file paths, when a registered path contains spaces, and a malicious executable is placed on a certain path, it may be executed with the privilege of the Windows service.	8.4	More Details
CVE-2020-7257	Privilege escalation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows local users to cause the deletion and creation of files they would not normally have permission to through altering the target of symbolic links whilst an anti-virus scan was in progress. This is timing dependent.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18792	NETGEAR D6100 devices before 1.0.0.50_0.0.50 are affected by command injection.	8.4	More Details
CVE-2020-0910	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, aka 'Windows Hyper-V Remote Code Execution Vulnerability'.	8.4	More Details
CVE-2017-18794	Certain NETGEAR devices are affected by command injection. This affects R6300v2 before 1.0.4.8_10.0.77, R6400 before 1.0.1.24, R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, R8500 before 1.0.2.100, and D6100 before 1.0.0.50_0.0.50.	8.4	More Details
CVE-2017-18850	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.01.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	8.4	More Details
CVE-2020-2803	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2805	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	8.3	More Details
CVE-2020-2879	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2860	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2871	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2872	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Profile). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2873	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2881	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2837	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2836	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2835	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2861	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2855	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Admin). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2834	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2833	Vulnerability in the Oracle Quoting product of Oracle E-Business Suite (component: Courseware). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Quoting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Quoting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Quoting accessible data as well as unauthorized update, insert or delete access to some of Oracle Quoting accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2832	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2831	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2874	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Customer Search). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2827	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2826	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2825	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2839	Vulnerability in the Oracle Service Intelligence product of Oracle E-Business Suite (component: Internal Operations- Search). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Service Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle Service Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2870	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2840	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2841	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2854	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2852	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Calendar). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2856	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2823	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Notes). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2867	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).	8.2	More Details
CVE-2020-2850	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2878	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Mail). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2849	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2848	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2857	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2847	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2877	Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Attribute Admin Setup). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2846	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2880	Vulnerability in the Oracle Learning Management product of Oracle E-Business Suite (component: OTA Training Activities). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Learning Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Learning Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Learning Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2858	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2845	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2844	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2843	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Profile). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2842	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2824	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2808	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2822	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Claims). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2758	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2020-2890	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2794	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Email Address list and Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2796	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-7250	Symbolic link manipulation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows authenticated local user to potentially gain an escalation of privileges by pointing the link to files which the user which not normally have permission to alter via carefully creating symbolic links from the ENS log file directory.	8.2	More Details
CVE-2020-2905	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2908	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2020-2807	Vulnerability in the Oracle Marketing Encyclopedia System product of Oracle E-Business Suite (component: Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing Encyclopedia System. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing Encyclopedia System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing Encyclopedia System accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing Encyclopedia System accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2876	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2809	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2813	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: KB Search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2815	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Profile). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2885	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Attachments). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Document Management and Collaboration, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Document Management and Collaboration accessible data as well as unauthorized update, insert or delete access to some of Oracle Document Management and Collaboration accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2817	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2742	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2818	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data as well as unauthorized update, insert or delete access to some of Oracle Universal Work Queue accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2819	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data as well as unauthorized update, insert or delete access to some of Oracle Universal Work Queue accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-2820	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Notes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2821	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Budget). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-11886	OpenNMS Horizon and Meridian allows HQL Injection in element/nodeList.htm (aka the NodeListController) via snmpParm or snmpParmValue to addCriteriaForSnmpParm. This affects Horizon before 25.2.1, Meridian 2019 before 2019.1.4, Meridian 2018 before 2018.1.16, and Meridian 2017 before 2017.1.21.	8.1	More Details
CVE-2020-2746	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Admin privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-1757	A flaw was found in all undertow-2.x.x SP1 versions prior to undertow-2.0.30.SP1, all undertow-1.x.x and undertow-2.x.x versions prior to undertow-2.1.0.Final, where the Servlet container causes servletPath to normalize incorrectly by truncating the path after semicolon which may lead to an application mapping resulting in the security bypass.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2882	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: Hierarchy Diagrammers). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-2956	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: Hierarchy Diagrammers). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-11661	CA API Developer Portal 4.3.1 and earlier contains an access control flaw that allows privileged users to view and edit user data.	8.1	More Details
CVE-2020-2735	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).	8.0	More Details
CVE-2019-20642	NETGEAR RAX40 devices before 1.0.3.64 are affected by authentication bypass.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20703	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20702	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20701	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20711	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20706	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.60 and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20657	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6200 before 1.1.00.36, D7000 before 1.0.1.74, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6080 before 1.0.0.42, R6050 before 1.0.1.24, JR6150 before 1.0.1.24, R6120 before 1.0.0.48, R6220 before 1.1.0.86, R6230 before 1.1.0.86, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, and WNR2020 before 1.1.0.62.	8.0	More Details
CVE-2020-1022	A remote code execution vulnerability exists in Microsoft Dynamics Business Central, aka 'Dynamics Business Central Remote Code Execution Vulnerability'.	8.0	More Details
CVE-2019-20705	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20758	NETGEAR R7000 devices before 1.0.9.42 are affected by a buffer overflow by an authenticated user.	8.0	More Details
CVE-2019-20707	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.60 and XR500 before 2.3.2.32.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20708	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20709	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20680	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7000v2 before 1.0.0.53, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.60, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.46, R8000P before 1.4.1.30, R8300 before 1.0.2.128, R8500 before 1.0.2.128, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20761	NETGEAR R7800 devices before 1.0.2.62 are affected by command injection by an authenticated user.	8.0	More Details
CVE-2019-20710	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2019-20704	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, and XR500 before 2.3.2.32.	8.0	More Details
CVE-2020-5350	Dell EMC Integrated Data Protection Appliance versions 2.0, 2.1, 2.2, 2.3, 2.4 contain a command injection vulnerability in the ACM component. A remote authenticated malicious user with root privileges could inject parameters in the ACM component APIs that could lead to manipulation of passwords and execution of malicious commands on ACM component.	7.9	More Details
CVE-2020-1001	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0940, CVE-2020-1006, CVE-2020-1017.	7.8	More Details
CVE-2020-1003	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1000, CVE-2020-1027.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1000	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1003, CVE-2020-1027.	7.8	More Details
CVE-2020-0999	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-1008.	7.8	More Details
CVE-2020-1004	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0994	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-0996	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0985.	7.8	More Details
CVE-2020-0995	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-0965	A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-0992	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0991	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0760.	7.8	More Details
CVE-2020-0907	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-0913	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1000, CVE-2020-1003, CVE-2020-1027.	7.8	More Details
CVE-2020-0919	An elevation of privilege vulnerability exists in Remote Desktop App for Mac in the way it allows an attacker to load unsigned binaries, aka 'Microsoft Remote Desktop App for Mac Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0934	An elevation of privilege vulnerability exists when the Windows WpcDesktopMonSvc improperly manages memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0983, CVE-2020-1009, CVE-2020-1011, CVE-2020-1015.	7.8	More Details
CVE-2020-0938	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020.	7.8	More Details
CVE-2020-0940	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1001, CVE-2020-1006, CVE-2020-1017.	7.8	More Details
CVE-2020-0944	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0942, CVE-2020-1029.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0953	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-0956	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0957, CVE-2020-0958.	7.8	More Details
CVE-2020-0957	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0956, CVE-2020-0958.	7.8	More Details
CVE-2020-0958	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0956, CVE-2020-0957.	7.8	More Details
CVE-2020-0959	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-0960	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-0961	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-0980	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0983	An elevation of privilege vulnerability exists when the Windows Delivery Optimization service improperly handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0934, CVE-2020-1009, CVE-2020-1011, CVE-2020-1015.	7.8	More Details
CVE-2020-0984	An elevation of privilege vulnerability exists when the Microsoft AutoUpdate (MAU) application for Mac improperly validates updates before executing them, aka 'Microsoft (MAU) Office Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0078	In releaseSecureStops of DrmPlugin.cpp, there is a possible out of bounds write due to a missing bounds 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-9 Android-10Android ID: A-144766455	7.8	More Details
CVE-2020-0988	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-1006	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0940, CVE-2020-1001, CVE-2020-1017.	7.8	More Details
CVE-2020-0985	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0996.	7.8	More Details
CVE-2020-1008	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0889, CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999.	7.8	More Details
CVE-2020-1009	An elevation of privilege vulnerability exists in the way that the Microsoft Store Install Service handles file operations in protected locations, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0934, CVE-2020-0983, CVE-2020-1011, CVE-2020-1015.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10547	When issuing IOCTL calls to ION, Memory leak can occur due to failure in unassign pages under certain conditions in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096AU, APQ8098, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8953, MSM8996AU, Nicobar, QCN7605, QCS605, Rennell, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDX24, SDX55, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2019-10556	Missing length check before copying the data from kernel space to userspace through the copy function can lead to buffer overflow in some cases in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MSM8909W, MSM8917, MSM8953, Nicobar, QCN7605, QCS405, QCS605, QM215, Rennell, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-10575	Wlan binary which is not signed with OEMs RoT is working on secure device without authentication failure in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in SDA845, SDM845, SDM850	7.8	More Details
CVE-2019-10620	Kernel memory error in debug module due to improper check of user data length before copying into memory in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, MSM8996AU, QCN7605, SDM439, SDX24, SM8150	7.8	More Details
CVE-2019-10621	Use after free issue when MAP and UNMAP calls at same time as data structure used my MAP may be freed by UNMAP function in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in Nicobar, QCS405, Rennell, Saipan, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10624	While handling the vendor command there is an integer truncation issue that could yield a buffer overflow due to int data type copied to u8 data type in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, MSM8996AU, QCA6574AU, QCN7605, Rennell, SC8180X, SDM710, SDX55, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2019-14001	Wrong public key usage from existing oem_keystore for hash generation in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, QM215, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDX20	7.8	More Details
CVE-2019-14009	Out of bound memory access while processing TZ command handler due to improper input validation on response length received from user in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, MDM9150, MDM9607, MDM9650, MSM8905, MSM8909, MSM8998, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDM850, SXR2130	7.8	More Details
CVE-2019-14018	Possible out of bound array access as there is no check on carrier index passed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14021	Possible buffer overrun when processing EFS filename and payload sent over diag interface due to lack of check for filename length and payload size received in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	7.8	More Details
CVE-2019-14105	Kernel was reading the CSL defined reserved field as uint16 instead of uint32 which could lead to memory overflow in Snapdragon Industrial IOT, Snapdragon Mobile in SDA845, SDM845, SM8150	7.8	More Details
CVE-2019-14116	Privilege escalation by using an altered debug policy image can occur as the XPU protecting the debug policy regions are disabled during the crash dump boot flow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018	7.8	More Details
CVE-2019-14122	Memory failure in SKB if it fails to to add the requested padding to the skb in low memory targets or targets with major memory fragmentation in Snapdragon Auto, Snapdragon Mobile in Saipan, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2019-14135	Possible integer overflow to buffer overflow in WLAN while parsing nonstandard NAN IE messages. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA4010, QCA6174A, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS405, QCS605, SA6155P, Saipan, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18838	Certain NETGEAR devices are affected by privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	7.8	More Details
CVE-2019-20769	An issue was discovered in LG PC Suite for LG G3 and earlier (aka LG PC Suite v5.3.27 and earlier). DLL Hijacking can occur via a Trojan horse DLL in the current working directory. The LG ID is LVE-MOT-190001 (November 2019).	7.8	More Details
CVE-2019-20770	An issue was discovered on LG mobile devices with Android OS 9.0 software. The HAL service has a buffer overflow that leads to arbitrary code execution. The LG ID is LVE-SMP-190013 (September 2019).	7.8	More Details
CVE-2019-20773	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. Unprivileged applications can execute shell commands via the connectivity service. The LG ID is LVE-SMP-190008 (August 2019).	7.8	More Details
CVE-2020-11875	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10.0 (MTK chipsets) software. The MTK kernel does not properly implement exception handling, allowing an attacker to gain privileges. The LG ID is LVE-SMP-200001 (February 2020).	7.8	More Details
CVE-2020-7079	An improper signature validation vulnerability in Autodesk Dynamo BIM versions 2.5.1 and 2.5.0 may lead to code execution through maliciously crafted DLL files.	7.8	More Details
CVE-2020-7080	A buffer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code execution on a system running it.	7.8	More Details
CVE-2020-7085	A heap overflow vulnerability in the Autodesk FBX-SDK versions 2019.2 and earlier may lead to arbitrary code execution on a system running it.	7.8	More Details
CVE-2020-0082	In ExternalVibration of ExternalVibration.java, there is a possible activation of an arbitrary intent due to unsafe deserialization. This could lead to local escalation of privilege to system_server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140417434	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0081	In finalize of AssetManager.java, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144028297	7.8	More Details
CVE-2020-0080	In onOpActiveChanged and related methods of AppOpsControllerImpl.java, there is a possible way to display an app overlaying other apps without the notification icon that it's overlaying. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144092031	7.8	More Details
CVE-2020-3194	A vulnerability in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details
CVE-2017-18843	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	7.8	More Details
CVE-2017-18844	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	7.8	More Details
CVE-2020-0547	Incorrect default permissions in the installer for Intel(R) Data Migration Software versions 3.3 and earlier may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-1011	An elevation of privilege vulnerability exists when the Windows System Assessment Tool improperly handles file operations, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0934, CVE-2020-0983, CVE-2020-1009, CVE-2020-1015.	7.8	More Details
CVE-2020-1014	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1015	An elevation of privilege vulnerability exists in the way that the User-Mode Power Service (UMPS) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0934, CVE-2020-0983, CVE-2020-1009, CVE-2020-1011.	7.8	More Details
CVE-2020-1017	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0940, CVE-2020-1001, CVE-2020-1006.	7.8	More Details
CVE-2020-1019	An elevation of privilege vulnerability exists in RMS Sharing App for Mac in the way it allows an attacker to load unsigned binaries, aka 'Microsoft RMS Sharing App for Mac Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1027	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1000, CVE-2020-1003.	7.8	More Details
CVE-2020-1029	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0942, CVE-2020-0944.	7.8	More Details
CVE-2020-1094	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-11958	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme.	7.8	More Details
CVE-2020-4270	IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow a local user to gain escalated privileges due to weak file permissions. IBM X-ForceID: 175846.	7.8	More Details
CVE-2020-8948	The Sierra Wireless Windows Mobile Broadband Driver Packages (MBDP) before build 5043 allows an unprivileged user to overwrite arbitrary files in arbitrary folders using hard links. An unprivileged user could leverage this vulnerability to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-0557	Insecure inherited permissions in Intel(R) PROSet/Wireless WiFi products before version 21.70 on Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18845	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38 and R6800 before 1.1.0.38.	7.8	More Details
CVE-2020-0598	Uncontrolled search path in the installer for the Intel(R) Binary Configuration Tool for Windows, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-0600	Improper buffer restrictions in firmware for some Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-10639	Eaton HMiSoft VU3 (HMIVU3 runtime not impacted), Version 3.00.23 and prior, however, the HMIVU runtimes are not impacted by these issues. A specially crafted input file could cause a buffer overflow when loaded by the affected product.	7.8	More Details
CVE-2020-0888	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0784.	7.8	More Details
CVE-2017-18837	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	7.8	More Details
CVE-2019-20655	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects XR500 before 2.3.2.56 and XR700 before 1.0.1.20.	7.8	More Details
CVE-2017-18830	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	7.8	More Details
CVE-2017-18829	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18826	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	7.8	More Details
CVE-2017-18822	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	7.8	More Details
CVE-2017-18849	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.01.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	7.8	More Details
CVE-2020-0889	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0953, CVE-2020-0959, CVE-2020-0960, CVE-2020-0988, CVE-2020-0992, CVE-2020-0994, CVE-2020-0995, CVE-2020-0999, CVE-2020-1008.	7.8	More Details
CVE-2020-0079	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144506242	7.8	More Details
CVE-2020-0835	An elevation of privilege vulnerability exists when Windows Defender antimalware platform improperly handles hard links, aka 'Windows Defender Antimalware Platform Hard Link Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0784	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0888.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2927	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	7.8	More Details
CVE-2020-8895	Untrusted Search Path vulnerability in the windows installer of Google Earth Pro versions prior to 7.3.3 allows an attacker to insert malicious local files to execute unauthenticated remote code on the targeted system.	7.8	More Details
CVE-2020-10699	A flaw was found in Linux, in targetcli-fb versions 2.1.50 and 2.1.51 where the socket used by targetclid was world-writable. If a system enables the targetclid socket, a local attacker can use this flaw to modify the iSCSI configuration and escalate their privileges to root.	7.8	More Details
CVE-2020-2929	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2020-2851	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2802	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: GraalVM Compiler). Supported versions that are affected are 19.3.1 and 20.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	7.7	More Details
CVE-2020-11728	An issue was discovered in DAViCal Andrew's Web Libraries (AWL) through 0.60. Session management does not use a sufficiently hard-to-guess session key. Anyone who can guess the microsecond time (and the incrementing session_id) can impersonate a session.	7.5	More Details
CVE-2019-20649	NETGEAR MR1100 devices before 12.06.08.00 are affected by disclosure of sensitive information.	7.5	More Details
CVE-2020-11968	In the web-panel in IQrouter through 3.3.1, remote attackers can read system logs because of Incorrect Access Control. Note: The vendor claims that this vulnerability can only occur on a brand-new network that, after initiating the forced initial configuration (which has a required step for setting a secure password on the system), makes this CVE invalid. This vulnerability is “true for any unconfigured release of OpenWRT, and true of many other new Linux distros prior to being configured for the first time”	7.5	More Details
CVE-2020-3162	A vulnerability in the Constrained Application Protocol (CoAP) implementation of Cisco IoT Field Network Director could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation of incoming CoAP traffic. An attacker could exploit this vulnerability by sending a malformed CoAP packet to an affected device. A successful exploit could allow the attacker to force the CoAP server to stop, interrupting communication to the IoT endpoints.	7.5	More Details
CVE-2020-11662	CA API Developer Portal 4.3.1 and earlier handles requests insecurely, which allows remote attackers to exploit a Cross-Origin Resource Sharing flaw and access sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12520	An issue was discovered in Squid through 4.7 and 5. When receiving a request, Squid checks its cache to see if it can serve up a response. It does this by making a MD5 hash of the absolute URL of the request. If found, it servers the request. The absolute URL can include the decoded UserInfo (username and password) for certain protocols. This decoded info is prepended to the domain. This allows an attacker to provide a username that has special characters to delimit the domain, and treat the rest of the URL as a path or query string. An attacker could first make a request to their domain using an encoded username, then when a request for the target domain comes in that decodes to the exact URL, it will serve the attacker's HTML instead of the real HTML. On Squid servers that also act as reverse proxies, this allows an attacker to gain access to features that only reverse proxies can use, such as ESI.	7.5	More Details
CVE-2020-10615	Triangle MicroWorks SCADA Data Gateway 3.02.0697 through 4.0.122, 2.41.0213 through 4.0.122 allows remote attackers cause a denial-of-service condition due to a lack of proper validation of the length of user-supplied data, prior to copying it to a fixed-length stack-based buffer. Authentication is not required to exploit this vulnerability.	7.5	More Details
CVE-2020-10613	Triangle MicroWorks SCADA Data Gateway 3.02.0697 through 4.0.122, 2.41.0213 through 4.0.122 allows remote attackers to disclose sensitive information due to the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. Authentication is not required to exploit this vulnerability. Only applicable to installations using DNP3 Data Sets.	7.5	More Details
CVE-2019-20654	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects WAC505 before 8.0.6.4 and WAC510 before 8.0.6.4.	7.5	More Details
CVE-2020-11792	NETGEAR R8900, R9000, RAX120, and XR700 devices before 2020-01-20 are affected by Transport Layer Security (TLS) certificate private key disclosure.	7.5	More Details
CVE-2020-2816	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20650	Certain NETGEAR devices are affected by denial of service. This affects R8900 before 1.0.5.2, R9000 before 1.0.5.2, XR500 before 2.3.2.56, and XR700 before 1.0.1.20.	7.5	More Details
CVE-2020-2828	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Web Services). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2020-11964	In IQrouter through 3.3.1, the Lua function diag_set_password in the web-panel allows remote attackers to change the root password arbitrarily. Note: The vendor claims that this vulnerability can only occur on a brand-new network that, after initiating the forced initial configuration (which has a required step for setting a secure password on the system), makes this CVE invalid. This vulnerability is “true for any unconfigured release of OpenWRT, and true of many other new Linux distros prior to being configured for the first time”	7.5	More Details
CVE-2020-2907	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20643	NETGEAR RAX40 devices before 1.0.3.64 are affected by disclosure of sensitive information.	7.5	More Details
CVE-2020-3249	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	7.5	More Details
CVE-2020-10506	The School Manage System before 2020, developed by ALLE INFORMATION CO., LTD., contains a vulnerability of Path Traversal, allowing attackers to access arbitrary files.	7.5	More Details
CVE-2020-3946	InstallBuilder AutoUpdate tool and regular installers enabling <checkForUpdates> built with versions earlier than 19.11 are vulnerable to Billion laughs attack (denial-of-service).	7.5	More Details
CVE-2020-2859	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: nVision). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2019-8961	A Denial of Service vulnerability related to stack exhaustion has been identified in FlexNet Publisher lmadmin.exe 11.16.2. Because the message reading function calls itself recursively given a certain condition in the received message, an unauthenticated remote attacker can repeatedly send messages of that type to cause a stack exhaustion condition.	7.5	More Details
CVE-2019-8960	A Denial of Service vulnerability related to command handling has been identified in FlexNet Publisher lmadmin.exe version 11.16.2. The message reading function used in lmadmin.exe can, given a certain message, call itself again and then wait for a further message. With a particular flag set in the original message, but no second message received, the function eventually return an unexpected value which leads to an exception being thrown. The end result can be process termination.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4269	IBM QRadar 7.3.0 to 7.3.3 Patch 2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-ForceID: 175845.	7.5	More Details
CVE-2020-11946	Zoho ManageEngine OpManager before 125120 allows an unauthenticated user to retrieve an API key via a servlet call.	7.5	More Details
CVE-2020-1018	An information disclosure vulnerability exists when Microsoft Dynamics Business Central/NAV on-premise does not properly hide the value of a masked field when showing the records as a chart page.The attacker who successfully exploited the vulnerability could see the information that are in a masked field.The security update addresses the vulnerability by updating the rendering engine the Windows client to properly detect masked fields and render the content as masked., aka 'Microsoft Dynamics Business Central/NAV Information Disclosure'.	7.5	More Details
CVE-2020-3177	A vulnerability in the Tool for Auto-Registered Phones Support (TAPS) of Cisco Unified Communications Manager (UCM) and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the TAPS interface of the affected device. An attacker could exploit this vulnerability by sending a crafted request to the TAPS interface. A successful exploit could allow the attacker to read arbitrary files in the system.	7.5	More Details
CVE-2020-3273	A vulnerability in the 802.11 Generic Advertisement Service (GAS) frame processing function of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS). The vulnerability is due to incomplete input validation of the 802.11 GAS frames that are processed by an affected device. An attacker could exploit this vulnerability by sending a crafted 802.11 GAS frame over the air to an access point (AP), and that frame would then be relayed to the affected WLC. Also, an attacker with Layer 3 connectivity to the WLC could exploit this vulnerability by sending a malicious 802.11 GAS payload in a Control and Provisioning of Wireless Access Points (CAPWAP) packet to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3262	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol handler of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of CAPWAP packets. An attacker could exploit this vulnerability by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to restart, resulting in a DoS condition.	7.5	More Details
CVE-2020-7484	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability with the former 'password' feature could allow a denial of service attack if the user is not following documented guidelines pertaining to dedicated TriStation connection and key-switch protection. This vulnerability was discovered and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. This feature is not present in version v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions.	7.5	More Details
CVE-2020-3932	A vulnerable SNMP in Draytek VigorAP910C cannot be disabled, which may cause information leakage.	7.5	More Details
CVE-2020-11877	airhost.exe in Zoom Client for Meetings 4.6.11 uses 3423423432325249 as the Initialization Vector (IV) for AES-256 CBC encryption. NOTE: the vendor states that this IV is used only within unreachable code	7.5	More Details
CVE-2020-11876	airhost.exe in Zoom Client for Meetings 4.6.11 uses the SHA-256 hash of 0123425234234fsdfsdr3242 for initialization of an OpenSSL EVP AES-256 CBC context. NOTE: the vendor states that this initialization only occurs within unreachable code	7.5	More Details
CVE-2020-4277	IBM TRIRIGA Application Platform 3.5.3 and 3.6.1 discloses sensitive information in error messages that could aid an attacker formulate future attacks. IBM X-Force ID: 175993.	7.5	More Details
CVE-2020-11874	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. Attackers can bypass Factory Reset Protection (FRP). The LG ID is LVE-SMP-200004 (March 2020).	7.5	More Details
CVE-2019-20771	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService allows unconfirmed configuration changes via a modified OMACP message. The LG ID is LVE-SMP-190006 (August 2019).	7.5	More Details
CVE-2020-10813	A buffer overflow vulnerability in FTPDMIN 0.96 allows attackers to crash the server via a crafted packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11872	The Cloud Functions subsystem in OpenTrace 1.0 might allow fabrication attacks by making billions of TempID requests before an AES-256-GCM key rotation occurs.	7.5	More Details
CVE-2020-11868	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.	7.5	More Details
CVE-2019-4327	"HCL AppScan Enterprise uses hard-coded credentials which can be exploited by attackers to get unauthorized access to application's encrypted files."	7.5	More Details
CVE-2017-18799	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6200v2 before 1.0.3.14, R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.1.1.20, R7000 before 1.0.7.10, R7000P/R6900P before 1.0.0.56, R7100LG before 1.0.0.30, R7900 before 1.0.1.14, R8000 before 1.0.3.22, R8500 before 1.0.2.74, and D8500 before 1.0.3.28.	7.5	More Details
CVE-2020-7486	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior.	7.5	More Details
CVE-2020-7483	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause certain data to be visible on the network when the 'password' feature is enabled. This vulnerability was discovered in and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. The 'password' feature is an additional optional check performed by TS1131 that it is connected to a specific controller. This data is sent as clear text and is visible on the network. This feature is not present in TriStation 1131 versions v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions.	7.5	More Details
CVE-2020-9280	In SilverStripe through 4.5, files uploaded via Forms to folders migrated from Silverstripe CMS 3.x may be put to the default "/Uploads" folder instead. This affects installations which allowed upload folder protection via the optional silverstripe/secureassets module under 3.x. This module is installed and enabled by default on the Common Web Platform (CWP). The vulnerability only affects files uploaded after an upgrade to 4.x.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11826	Users can lock their notes with a password in Memono version 3.8. Thus, users needs to know a password to read notes. However, these notes are stored in a database without encryption and an attacker can read the password-protected notes without having the password. Notes are stored in the ZENTITY table in the memono.sqlite database.	7.5	More Details
CVE-2020-2750	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Account Hierarchy Manager). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2019-20696	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC505 before V5.6.8.3 and WAC510 before V5.6.8.3.	7.5	More Details
CVE-2019-20695	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects SRK60 before 2.3.5.106, SRR60 before 2.3.5.106, and SRS60 before 2.3.5.106.	7.5	More Details
CVE-2019-20694	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects GS728TP before 6.0.0.48, GS728TPPv2 before 6.0.0.48, GS728TPv2 before 6.0.0.48, GS752TPP before 6.0.0.48, and GS752TPv2 before 6.0.0.48.	7.5	More Details
CVE-2019-20687	Certain NETGEAR devices are affected by denial of service. This affects D6200 before 1.1.00.34, D7000 before 1.0.1.70, JR6150 before 1.0.1.18, R6050 before 1.0.1.18, and WNR2020 before 1.1.0.62.	7.5	More Details
CVE-2019-18948	An issue was found in Arista EOS. Specific malformed ARP packets can impact the software forwarding of VxLAN packets. This issue is found in Arista's EOS VxLAN code, which can allow attackers to crash the VxlanSwFwd agent. This affects EOS 4.21.8M and below releases in the 4.21.x train, 4.22.3M and below releases in the 4.22.x train, 4.23.1F and below releases in the 4.23.x train, and all releases in 4.15, 4.16, 4.17, 4.18, 4.19, 4.20 code train.	7.5	More Details
CVE-2019-4762	IBM MQ 9.0 and 9.1 is vulnerable to a denial of service attack due to an error in the Channel processing function. IBM X-Force ID: 173625.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3651	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	7.5	More Details
CVE-2019-14022	Error occurs While extracting the ipv6_header having an invalid length due to lack of length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8096AU, MDM9205, MDM9206, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS605, QM215, Rennell, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	7.5	More Details
CVE-2019-14012	Possibility of null pointer deference as the array of video codecs from media info is referenced without null checking while processing SDP messages in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, Nicobar, QCM2150, QM215, Rennell, SC7180, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150	7.5	More Details
CVE-2020-1699	A path traversal flaw was found in the Ceph dashboard implemented in upstream versions v14.2.5, v14.2.6, v15.0.0 of Ceph storage and has been fixed in versions 14.2.7 and 15.1.0. An unauthenticated attacker could use this flaw to cause information disclosure on the host machine running the Ceph dashboard.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2911	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2020-12051	The CentralAuth extension through REL1_34 for MediaWiki allows remote attackers to obtain sensitive hidden account information via an api.php?action=query&meta=globaluserinfo&guiuser= request. In other words, the information can be retrieved via the action API even though access would be denied when simply visiting wiki/Special:CentralAuth in a web browser.	7.5	More Details
CVE-2020-0970	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0968.	7.5	More Details
CVE-2020-11828	In ColorOS (oppo mobile phone operating system, based on AOSP frameworks/native code position/services/surfaceflinger surfaceflinger.CPP), RGB is defined on the stack but uninitialized, so when the screenShot function to RGB value assignment, will not initialize the value is returned to the attackers, leading to values on the stack information leakage, the vulnerability can be used to bypass attackers ALSR.	7.5	More Details
CVE-2020-0895	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'.	7.5	More Details
CVE-2020-0969	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2958	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2020-0968	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0970.	7.5	More Details
CVE-2020-1967	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).	7.5	More Details
CVE-2020-2739	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N).	7.4	More Details
CVE-2020-7278	Exploiting incorrectly configured access control security levels vulnerability in ENS Firewall in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 and 10.6.1 April 2020 updates allows remote attackers and local users to allow or block unauthorized traffic via pre-existing rules not being handled correctly when updating to the February 2020 updates.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2785	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details
CVE-2020-2786	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2784	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details
CVE-2020-3240	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	7.3	More Details
CVE-2020-4347	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 could be subject to attacks based on privilege escalation due to inappropriate file permissions for files used by WebSphere Application Server Network Deployment. IBM X-Force ID: 178412.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2787	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details
CVE-2019-20767	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.60, D3600 before 1.0.0.75, D6000 before 1.0.0.75, R9000 before 1.0.4.26, R8900 before 1.0.4.26, R7800 before 1.0.2.52, WNDR4500v3 before 1.0.0.58, WNDR4300v2 before 1.0.0.58, WNDR4300 before 1.0.2.104, WNDR3700v4 before 1.0.2.102, and WNR2000v5 before 1.0.0.66.	7.2	More Details
CVE-2020-2798	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2020-11885	WSO2 Enterprise Integrator through 6.6.0 has an XXE vulnerability where a user (with admin console access) can use the XML validator to make unintended network invocations such as SSRF via an uploaded file.	7.2	More Details
CVE-2020-7111	A server side injection vulnerability exists which could allow an authenticated administrative user to achieve Remote Code Execution in ClearPass. Resolution: Fixed in 6.7.13, 6.8.4, 6.9.0 and higher.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2963	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2019-20659	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6400v2 before 1.0.4.84, R6700 before 1.0.2.8, R6700v3 before 1.0.4.84, R6900 before 1.0.2.8, and R7900 before 1.0.3.10.	7.2	More Details
CVE-2020-2793	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6 - 8.0.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-2964	Vulnerability in the Oracle Financial Services Data Foundation product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 - 8.0.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Data Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Data Foundation accessible data as well as unauthorized read access to a subset of Oracle Financial Services Data Foundation accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2019-14104	Slab-out-of-bounds access can occur if the context pointer is invalid due to lack of null check on pointer before accessing it in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, SC8180X, SDX55, SM8150	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0942	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0944, CVE-2020-1029.	7.1	More Details
CVE-2019-10625	Out of bound access in diag services when DCI command buffer reallocation is not done properly with required capacity in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, QCS605, Rennell, SC8180X, SDM429W, SDM710, SDX55, SM7150, SM8150	7.1	More Details
CVE-2020-2935	Vulnerability in the Oracle Financial Services Hedge Management and IFRS Valuations product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 - 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Hedge Management and IFRS Valuations. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Hedge Management and IFRS Valuations accessible data as well as unauthorized read access to a subset of Oracle Financial Services Hedge Management and IFRS Valuations accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-2936	Vulnerability in the Oracle Financial Services Balance Sheet Planning product of Oracle Financial Services Applications (component: User Interface). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Balance Sheet Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Balance Sheet Planning accessible data as well as unauthorized read access to a subset of Oracle Financial Services Balance Sheet Planning accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10623	Possible integer overflow can happen in host driver while processing user controlled string due to improper validation on data received. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCN7605, QCS605, Rennell, SC8180X, SDA845, SDM710, SDX24, SDX55, SM7150, SM8150, SM8250, SXR2130	7.1	More Details
CVE-2020-2937	Vulnerability in the Oracle Insurance Accounting Analyzer product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 - 8.0.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Insurance Accounting Analyzer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Insurance Accounting Analyzer accessible data as well as unauthorized read access to a subset of Oracle Insurance Accounting Analyzer accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-1002	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'.	7.1	More Details
CVE-2020-0936	An elevation of privilege vulnerability exists when a Windows scheduled task improperly handles file redirections, aka 'Windows Scheduled Task Elevation of Privilege Vulnerability'.	7.1	More Details
CVE-2020-2938	Vulnerability in the Oracle Financial Services Loan Loss Forecasting and Provisioning product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 - 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Loan Loss Forecasting and Provisioning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Loan Loss Forecasting and Provisioning accessible data as well as unauthorized read access to a subset of Oracle Financial Services Loan Loss Forecasting and Provisioning accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2939	Vulnerability in the Oracle Financial Services Asset Liability Management product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 and 8.0.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Asset Liability Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Asset Liability Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Asset Liability Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-2178	Jenkins Parasoft Findings Plugin 10.4.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.1	More Details
CVE-2019-10574	Lack of boundary checks for data offsets received from HLOS can lead to out-of-bound read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8016, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCM2150, QCS605, QM215, Rennell, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130	7.1	More Details
CVE-2020-8099	A vulnerability in the improper handling of junctions in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects: Bitdefender Antivirus Free versions prior to 1.0.17.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2940	Vulnerability in the Oracle Financial Services Profitability Management product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 and 8.0.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Profitability Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Profitability Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Profitability Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-2891	Vulnerability in the Oracle Financial Services Liquidity Risk Management product of Oracle Financial Services Applications (component: User Interfaces). The supported version that is affected is 8.0.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Liquidity Risk Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Liquidity Risk Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Liquidity Risk Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-2943	Vulnerability in the Oracle Financial Services Liquidity Risk Measurement and Management product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.7 and 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Liquidity Risk Measurement and Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Liquidity Risk Measurement and Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Liquidity Risk Measurement and Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2782	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Query). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L).	7.1	More Details
CVE-2020-2945	Vulnerability in the Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management product of Oracle Financial Services Applications (component: User Interfaces). Supported versions that are affected are 8.0.7 and 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2020-2941	Vulnerability in the Oracle Financial Services Funds Transfer Pricing product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6 and 8.0.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Funds Transfer Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Funds Transfer Pricing accessible data as well as unauthorized read access to a subset of Oracle Financial Services Funds Transfer Pricing accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2942	Vulnerability in the Oracle Financial Services Price Creation and Discovery product of Oracle Financial Services Applications (component: User Interface). The supported version that is affected is 8.0.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Price Creation and Discovery. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Price Creation and Discovery accessible data as well as unauthorized read access to a subset of Oracle Financial Services Price Creation and Discovery accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	7.1	More Details
CVE-2019-14070	Possible use after free issue in pcm volume controls due to race condition exist in private data used in mixer controls in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.0	More Details
CVE-2020-2914	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2913	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.0	More Details
CVE-2019-11999	Potential security vulnerabilities have been identified in HPE OpenCall Media Platform (OCMP) resulting in remote arbitrary file download and cross site scripting. HPE has made the following updates available to resolve the vulnerability in the impacted versions of OCMP. * For OCMP version 4.4.X - please upgrade to OCMP 4.4.8 and then install RP806 * For OCMP 4.5.x please contact HPE Technical Support to obtain the necessary software updates.	6.9	More Details
CVE-2019-20764	NETGEAR R7800 devices before 1.0.2.52 are affected by a stack-based buffer overflow by an authenticated user.	6.8	More Details
CVE-2019-20763	NETGEAR R7800 devices before 1.0.2.52 are affected by a stack-based buffer overflow by an authenticated user.	6.8	More Details
CVE-2019-20762	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D8500 before 1.0.3.43, R8500 before 1.0.2.128, R8300 before 1.0.2.128, R8000 before 1.0.4.28, R7300DST before 1.0.0.68, R7100LG before 1.0.0.48, R6900P before 1.3.1.44, R7900P before 1.4.1.30, R8000P before 1.4.1.30, R7000P before 1.3.1.44, R7000 before 1.0.9.34, R6900 before 1.0.2.4, R6700 before 1.0.2.6, and R6400 before 1.0.1.44.	6.8	More Details
CVE-2018-21144	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DM200 before 1.0.0.52, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.16, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	6.8	More Details
CVE-2019-20740	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.109, R7300 before 1.0.0.70, R8300 before 1.0.2.130, and R8500 before 1.0.2.130.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20757	NETGEAR R7800 devices before 1.0.2.62 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2019-20745	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WAC505 before 5.0.10.2 and WAC510 before 5.0.10.2.	6.8	More Details
CVE-2019-20736	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6000 before 1.0.0.72, D6100 before 1.0.0.63, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2019-20755	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6220 before 1.0.0.46, D6400 before 1.0.0.80, D7000v2 before 1.0.0.51, D8500 before 1.0.3.42, DGN2200v1 before 1.0.0.58, DGN2200B before 1.0.0.58, JNDR3000 before 1.0.0.24, RBW30 before 2.1.4.16, R6250 before 1.0.4.26, R6300v2 before 1.0.4.28, R6400 before 1.0.1.42, R6400v2 before 1.0.2.56, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.32, R6900P before 1.3.1.44, R7100LG before 1.0.0.46, R7300DST before 1.0.0.68, R7000P before 1.3.1.44, R7900 before 1.0.2.16, R8000P before 1.4.0.10, R7900P before 1.4.0.10, R8300 before 1.0.2.122, R8500 before 1.0.2.122, R8000 before 1.0.4.18, WNDR3400v3 before 1.0.1.22, WNDR4500v2 before 1.0.0.72, WNR3500Lv2 before 1.2.0.54, WN3100RP before 1.0.0.20, and WN2500RPv2 before 1.0.1.54.	6.8	More Details
CVE-2019-20751	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.60, DM200 before 1.0.0.61, EX2700 before 1.0.1.48, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, EX6200v2 before 1.0.1.72, EX8000 before 1.0.1.180, R7800 before 1.0.2.52, R8900 before 1.0.4.26, R9000 before 1.0.4.26, WN2000RPTv3 before 1.0.1.32, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.66, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.68.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20747	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.58, D7800 before 1.0.1.40, R7500v2 before 1.0.3.34, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.3.16, RAX120 before 1.0.0.74, RBK20 before 2.3.0.22, RBR20 before 2.3.0.22, RBS20 before 2.3.0.22, RBK50 before 2.3.0.22, RBR50 before 2.3.0.22, RBS50 before 2.3.0.22, RBK40 before 2.3.0.22, RBS40 before 2.3.0.22, SRK60 before 2.2.0.64, SRR60 before 2.2.0.64, SRS60 before 2.2.0.64, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, and WNR2000v5 before 1.0.0.66.	6.8	More Details
CVE-2019-20735	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before V1.0.0.75, D6100 before V1.0.0.63, R7800 before v1.0.2.52, R8900 before v1.0.4.2, R9000 before v1.0.4.2, RBK50 before v2.3.0.32, RBR50 before v2.3.0.32, RBS50 before v2.3.0.32, WNDR3700v4 before V1.0.2.102, WNDR4300v1 before V1.0.2.104, WNDR4300v2 before v1.0.0.58, WNDR4500v3 before v1.0.0.58, WNR2000v5 before v1.0.0.68, and XR500 before V2.3.2.32.	6.8	More Details
CVE-2019-20748	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.44, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBS40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, and RBS50 before 2.3.0.32.	6.8	More Details
CVE-2019-20754	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects DGN2200 before 1.0.0.58, DGN2200B before 1.0.0.58, D8500 before 1.0.3.42, D7000v2 before 1.0.0.51, D6400 before 1.0.0.80, D6220 before 1.0.0.44, EX7000 before 1.0.0.66, EX6200 before 1.0.3.88, EX6150 before 1.0.0.42, EX7500 before 1.0.0.46, JNDR3000 before 1.0.0.24, R8000 before 1.0.4.18, R8500 before 1.0.2.122, R8300 before 1.0.2.122, R7900P before 1.4.0.10, R8000P before 1.4.0.10, R7900 before 1.0.2.16, R7000P before 1.3.1.44, R7300DST before 1.0.0.68, R7100LG before 1.0.0.46, R6900P before 1.3.1.44, R7000 before 1.0.9.32, R6900 before 1.0.1.46, R6700 before 1.0.1.46, R6400v2 before 1.0.2.56, R6400 before 1.0.1.42, R6300v2 before 1.0.4.28, R6250 before 1.0.4.26, WNDR4500v2 before 1.0.0.72, and WNR3500Lv2 before 1.2.0.54.	6.8	More Details
CVE-2019-20765	NETGEAR R7800 devices before 1.0.2.52 are affected by a stack-based buffer overflow by an authenticated user.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20726	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.63, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2019-20727	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6100 before 1.0.0.63, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2019-20766	NETGEAR R7800 devices before 1.0.2.52 are affected by a stack-based buffer overflow by an authenticated user.	6.8	More Details
CVE-2019-20719	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.48, D6400 before 1.0.0.82, D7000v2 before 1.0.0.52, D8500 before 1.0.3.43, R6250 before 1.0.4.34, R6400 before 1.0.1.44, R6400v2 before 1.0.2.62, R7000P before 1.4.1.30, R7100LG before 1.0.0.48, R7300DST before 1.0.0.68, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, and R8500 before 1.0.2.128.	6.8	More Details
CVE-2019-20688	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.63, EX2700 before 1.0.1.48, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, EX6200v2 before 1.0.1.72, EX6400 before 1.0.2.136, EX7300 before 1.0.2.136, EX8000 before 1.0.1.180, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WN2000RPTv3 before 1.0.1.32, WN3000RPv2 before 1.0.0.68, WN3100RPv2 before 1.0.0.60, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20712	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7000v2 before 1.0.0.53, D8500 before 1.0.3.44, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.109, R6250 before 1.0.4.34, R6300v2 before 1.0.4.32, R6400 before 1.0.1.46, R6400v2 before 1.0.2.62, R6700 before 1.0.2.6, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R7000 before 1.0.9.60, R7000P before 1.3.1.64, R7100LG before 1.0.0.52, R7300DST before 1.0.0.70, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, R8500 before 1.0.2.128, WNDR3400v3 before 1.0.1.24, and WNR3500Lv2 before 1.2.0.56.	6.8	More Details
CVE-2019-20689	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6000 before 1.0.0.75, D6100 before 1.0.0.63, EX2700 before 1.0.1.48, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, EX6200v2 before 1.0.1.72, EX6400 before 1.0.2.136, EX7300 before 1.0.2.136, EX8000 before 1.0.1.180, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WN2000RPTv3 before 1.0.1.32, WN3000RPv2 before 1.0.0.68, WN3100RPv2 before 1.0.0.60, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2020-0917	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0918.	6.8	More Details
CVE-2019-20713	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D8500 before 1.0.3.44, R6250 before 1.0.4.34, R6300v2 before 1.0.4.32, R6400 before 1.0.1.46, R6700 before 1.0.2.6, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7100LG before 1.0.0.50, R7300DST before 1.0.0.70, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, and R8500 before 1.0.2.128.	6.8	More Details
CVE-2019-20716	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects DGN2200v4 before 1.0.0.110 and DGND2200Bv4 before 1.0.0.109.	6.8	More Details
CVE-2018-21146	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21145	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	6.8	More Details
CVE-2020-0918	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0917.	6.8	More Details
CVE-2019-20718	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6220 before 1.0.0.48, D6400 before 1.0.0.82, D7000v2 before 1.0.0.52, D8500 before 1.0.3.43, R6250 before 1.0.4.34, R6400 before 1.0.1.44, R6400v2 before 1.0.2.62, R7100LG before 1.0.0.48, R7300DST before 1.0.0.68, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, and R8500 before 1.0.2.128.	6.8	More Details
CVE-2018-21148	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	6.8	More Details
CVE-2019-20722	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, DM200 before 1.0.0.58, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, RBS40 before 2.3.0.28, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2019-20725	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.63, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20724	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.63, D7800 before 1.0.1.44, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, RBS40 before 2.3.0.28, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2019-20723	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.63, DM200 before 1.0.0.58, EX2700 before 1.0.1.48, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, EX6200v2 before 1.0.1.72, EX6400 before 1.0.2.136, EX7300 before 1.0.2.136, EX8000 before 1.0.1.180, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WN2000RPTv3 before 1.0.1.32, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.60, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.68, and XR500 before 2.3.2.32.	6.8	More Details
CVE-2018-21147	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	6.8	More Details
CVE-2020-7277	Protection mechanism failure in all processes in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 Update allows local users to stop certain McAfee ENS processes, reducing the protection offered.	6.8	More Details
CVE-2019-20785	An issue was discovered on LG mobile devices with Android OS 8.0 and 8.1 software for the DTAG carrier. RILD in the radio layer uses an uninitialized variable. The LG ID is LVE-SMP-180013 (January 2019).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20700	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.44, D6400 before 1.0.0.78, D7000v2 before 1.0.0.51, D8500 before 1.0.3.42, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.110, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R7900 before 1.0.2.10, R8000 before 1.0.4.12, R8300 before 1.0.2.122, R8500 before 1.0.2.122, R6900P before 1.3.1.64, R7000P before 1.3.1.64, R7100LG before 1.0.0.46, R7300DST before 1.0.0.68, R7900P before 1.3.0.10, R8000P before 1.3.0.10, WN2500RPv2 before 1.0.1.54, WNDR3400v3 before 1.0.1.22, and WNR3500Lv2 before 1.2.0.54.	6.7	More Details
CVE-2019-20732	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6220 before 1.0.0.40, D7000v2 before 1.0.0.74, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.102, DGND2200Bv4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.20, R6300v2 before 1.0.4.24, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.26, R6900P before 1.3.0.20, R7000P before 1.3.0.20, R7100LG before 1.0.0.40, R7300DST before 1.0.0.62, R7900 before 1.0.2.10, R8000 before 1.0.4.12, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.106, R8500 before 1.0.2.106, WN2500RPv2 before 1.0.1.54, WNDR3400v3 before 1.0.1.18, and WNR3500Lv2 before 1.2.0.48.	6.7	More Details
CVE-2019-20737	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.44, D6400 before 1.0.0.78, D7000v2 before 1.0.0.51, D8500 before 1.0.3.42, DGN2200v4 before 1.0.0.106, DGND2200Bv4 before 1.0.0.106, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6400 before 1.0.1.42, R6700 before 1.0.1.46, R6700v3 before 1.0.2.52, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, WNDR3400v3 before 1.0.1.24, and WNR3500Lv2 before 1.2.0.54.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18793	NETGEAR R7800 devices before 1.0.2.36 are affected by command injection.	6.7	More Details
CVE-2019-20733	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.44, D6400 before 1.0.0.78, D7000v2 before 1.0.0.51, D8500 before 1.0.3.42, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.110, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R6900P before 1.3.1.64, R7000P before 1.3.1.64, R7100LG before 1.0.0.46, R7300DST before 1.0.0.68, R7900 before 1.0.2.10, R8000 before 1.0.4.12, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, WNDR3400v3 before 1.0.1.22, and WNR3500Lv2 before 1.2.0.54.	6.7	More Details
CVE-2017-18804	Certain NETGEAR devices are affected by command injection. This affects R7800 before 1.0.2.16 and R9000 before 1.0.2.4.	6.7	More Details
CVE-2020-0076	In get_auth_result of the FPC IRIS TrustZone app, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146056878	6.7	More Details
CVE-2017-18805	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and WNDAP360 before 3.7.4.0.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20692	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.44, D6400 before 1.0.0.78, D7000v2 before 1.0.0.51, D8500 before 1.0.3.42, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.109, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R6900P before 1.3.1.44, R7000P before 1.3.1.44, R7100LG before 1.0.0.46, R7300DST before 1.0.0.68, R7900 before 1.0.2.10, R8000 before 1.0.4.12, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, WNDR3400v3 before 1.0.1.22, and WNR3500Lv2 before 1.2.0.54.	6.7	More Details
CVE-2019-20731	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000v2 before 1.0.0.74, D8500 before 1.0.3.39, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.20, R6300v2 before 1.0.4.18, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.46, R7000 before 1.0.9.26, R6900P before 1.3.0.20, R7000P before 1.3.0.20, R7100LG before 1.0.0.34, R7300DST before 1.0.0.62, R8000 before 1.0.4.12, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, WN2500RPv2 before 1.0.1.54, and WNDR3400v3 before 1.0.1.18.	6.7	More Details
CVE-2017-18806	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and WNDAP360 before 3.7.4.0.	6.7	More Details
CVE-2017-18841	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.46, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.46, and D7000 before 1.0.1.50.	6.7	More Details
CVE-2017-18801	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.50, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.48, and D7000 before 1.0.1.50.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18795	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.28 and D6100 before 1.0.0.50_0.0.50.	6.7	More Details
CVE-2017-18846	Certain NETGEAR devices are affected by a stack-based buffer overflow. This affects R6250 before 1.0.4.12, R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	6.7	More Details
CVE-2019-20651	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WAC505 before 8.2.1.16 and WAC510 before 8.2.1.16.	6.7	More Details
CVE-2020-6992	A local privilege escalation vulnerability has been identified in the GE Digital CIMPLICITY HMI/SCADA product v10.0 and prior. If exploited, this vulnerability could allow an adversary to modify the system, leading to the arbitrary execution of code. This vulnerability is only exploitable if an attacker has access to an authenticated session. GE Digital CIMPLICITY v11.0, released January 2020, contains mitigation for this local privilege escalation vulnerability. GE Digital recommends all users upgrade to GE CIMPLICITY v11.0 or newer.	6.7	More Details
CVE-2019-20728	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6400 before 1.0.0.74, D7000v2 before 1.0.0.74, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.102, DGND2200Bv4 before 1.0.0.102, DM200 before 1.0.0.52, JNDR3000 before 1.0.0.22, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBW30 before 2.1.2.6, R6250 before 1.0.4.26, R6300v2 before 1.0.4.24, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R7000 before 1.0.9.26, R6900P before 1.3.0.20, R7000P before 1.3.0.20, R7100LG before 1.0.0.40, R7300DST before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.2.10, R8000 before 1.0.4.12, R7900P before 1.3.0.10, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3400v3 before 1.0.1.18, WNDR3700v4 before 1.0.2.96, WNDR4300v1 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, WNR2000v5 before 1.0.0.64, and WNR3500Lv2 before 1.2.0.48.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7273	Accessing functionality not properly constrained by ACLs vulnerability in the autorun start-up protection in McAfee Endpoint Security (ENS) for Windows Prior to 10.7.0 April 2020 Update allows local users to delete or rename programs in the autorun key via manipulation of some parameters.	6.7	More Details
CVE-2017-18802	Certain NETGEAR devices are affected by command injection. This affects R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before 1.0.3.16, R7800 before 1.0.2.32, EX6200v2 before 1.0.1.50, and D7800 before 1.0.1.22.	6.7	More Details
CVE-2017-18796	Certain NETGEAR devices are affected by command injection. This affects R6400 before 1.0.1.24, R6700 before 1.0.1.26, R6900 before 1.0.1.28, R7000 before 1.0.9.10, R7000P before 1.0.1.16, R6900P before 1.0.1.16, and R7800 before 1.0.2.36.	6.7	More Details
CVE-2017-18851	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D8500 through 1.0.3.28, R6400 through 1.0.1.22, R6400v2 through 1.0.2.18, R8300 through 1.0.2.94, R8500 through 1.0.2.94, and R6100 through 1.0.1.12.	6.7	More Details
CVE-2020-7274	Privilege escalation vulnerability in McTray.exe in McAfee Endpoint Security (ENS) for Windows Prior to 10.7.0 April 2020 Update allows local users to spawn unrelated processes with elevated privileges via the system administrator granting McTray.exe elevated privileges (by default it runs with the current user's privileges).	6.6	More Details
CVE-2020-7259	Exploitation of Privilege/Trust vulnerability in file in McAfee Endpoint Security (ENS) Prior to 10.7.0 February 2020 Update allows local users to bypass local security protection via a carefully crafted input file	6.6	More Details
CVE-2019-20717	Certain NETGEAR devices are affected by denial of service. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D7800 before 1.0.1.44, EX2700 before 1.0.1.52, EX6200v2 before 1.0.1.74, EX8000 before 1.0.1.180, R7500v2 before 1.0.3.38, R7800 before 1.0.2.58, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, RBS40 before 2.3.0.28, SRK60 before 2.2.1.210, SRR60 before 2.2.1.210, SRS60 before 2.2.1.210, WN2000RPTv3 before 1.0.1.34, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.60, WNDR4300v2 before 1.0.0.58, and WNDR4500v3 before 1.0.0.58.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3252	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2020-11007	In Shopizer before version 2.11.0, using API or Controller based versions negative quantity is not adequately validated hence creating incorrect shopping cart and order total. This vulnerability makes it possible to create a negative total in the shopping cart. This has been patched in version 2.11.0.	6.5	More Details
CVE-2020-11660	CA API Developer Portal 4.3.1 and earlier contains an access control flaw that allows privileged users to view restricted sensitive information.	6.5	More Details
CVE-2020-2951	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2594	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Project Manager). Supported versions that are affected are 16.2.0.0 - 16.2.19.3, 17.12.0.0 - 17.12.17.0, 18.8.0.0 - 18.8.18.0, 19.12.1.0 - 19.12.3.0 and 20.1.0.0 - 20.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Primavera P6 Enterprise Project Portfolio Management. CVSS 3.0 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).	6.5	More Details
CVE-2020-2952	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data as well as unauthorized read access to a subset of Oracle HTTP Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2020-3261	A vulnerability in the web-based management interface of Cisco Mobility Express Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user with an active session on an affected device to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions, including modifying the configuration, with the privilege level of the user.	6.5	More Details
CVE-2019-20698	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC505 before 8.0.5.5 and WAC510 before 8.0.5.5.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2780	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2020-5268	In Saml2 Authentication Services for ASP.NET versions before 1.0.2, and between 2.0.0 and 2.6.0, there is a vulnerability in how tokens are validated in some cases. Saml2 tokens are usually used as bearer tokens - a caller that presents a token is assumed to be the subject of the token. There is also support in the Saml2 protocol for issuing tokens that is tied to a subject through other means, e.g. holder-of-key where possession of a private key must be proved. The Sustainsys.Saml2 library incorrectly treats all incoming tokens as bearer tokens, even though they have another subject confirmation method specified. This could be used by an attacker that could get access to Saml2 tokens with another subject confirmation method than bearer. The attacker could then use such a token to create a log in session. This vulnerability is patched in versions 1.0.2 and 2.7.0.	6.5	More Details
CVE-2020-2790	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 5.7.28 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2020-3260	A vulnerability in Cisco Aironet Series Access Points Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to the improper processing of client packets that are sent to an affected access point (AP). An attacker could exploit this vulnerability by sending a large number of sustained client packets to the affected AP. A successful exploit could allow the attacker to cause the affected AP to crash, resulting in a DoS condition.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11880	An issue was discovered in KDE KMail before 19.12.3. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make KMail attach local files to a composed email message without showing a warning to the user, as demonstrated by an attach=.bash_history value.	6.5	More Details
CVE-2018-21140	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	6.5	More Details
CVE-2020-11879	An issue was discovered in GNOME Evolution before 3.35.91. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make Evolution attach local files or directories to a composed email message without showing a warning to the user, as demonstrated by an attach=. value.	6.5	More Details
CVE-2020-7083	An intager overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	6.5	More Details
CVE-2020-5293	In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there are improper access controls on product page with combinations, attachments and specific prices. The problem is fixed in 1.7.6.5.	6.5	More Details
CVE-2020-0576	Buffer overflow in Intel(R) Modular Server MFS2600KISPP Compute Module may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-0558	Improper buffer restrictions in kernel mode driver for Intel(R) PROSet/Wireless WiFi products before version 21.70 on Windows 10 may allow an unprivileged user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-2910	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20652	NETGEAR WAC505 devices before 8.2.1.16 are affected by disclosure of sensitive information.	6.5	More Details
CVE-2019-20653	Certain NETGEAR devices are affected by denial of service. This affects WAC505 before 8.0.6.4 and WAC510 before 8.0.6.4.	6.5	More Details
CVE-2018-21143	NETGEAR GS810EMX devices before 1.0.0.5 are affected by disclosure of sensitive information.	6.5	More Details
CVE-2019-20658	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects FS728TLP before 1.0.1.26, GS105Ev2 before 1.6.0.4, GS105PE before 1.6.0.4, GS108Ev3 before 2.06.08, GS108PEv3 before 2.06.08, GS110EMX before 1.0.1.4, GS116Ev2 before 2.6.0.35, GS408EPP before 1.0.0.15, GS808E before 1.7.0.7, GS810EMX before 1.7.1.1, GS908E before 1.7.0.3, GSS108E before 1.6.0.4, GSS108EPP before 1.0.0.15, GSS116E before 1.6.0.9, JGS516PE before 2.6.0.35, JGS524Ev2 before 2.6.0.35, JGS524PE before 2.6.0.35, XS512EM before 1.0.1.1, XS708Ev2 before 1.6.0.23, XS716E before 1.6.0.23, and XS724EM before 1.0.1.1.	6.5	More Details
CVE-2020-0952	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.	6.5	More Details
CVE-2019-20638	NETGEAR MR1100 devices before 12.06.08.00 are affected by disclosure of administrative credentials.	6.5	More Details
CVE-2020-2906	Vulnerability in the PeopleSoft Enterprise SCM Purchasing product of Oracle PeopleSoft (component: Supplier Change). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM Purchasing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise SCM Purchasing accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2020-0993	A denial of service vulnerability exists in Windows DNS when it fails to properly handle queries, aka 'Windows DNS Denial of Service Vulnerability'.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20741	NETGEAR WAC510 devices before 5.0.10.2 are affected by disclosure of sensitive information.	6.5	More Details
CVE-2019-12001	A remote session reuse vulnerability leading to access restriction bypass was discovered in HPE MSA 2040 SAN Storage; HPE MSA 1040 SAN Storage; HPE MSA 1050 SAN Storage; HPE MSA 2042 SAN Storage; HPE MSA 2050 SAN Storage; HPE MSA 2052 SAN Storage version(s): GL225P001 and earlier; GL225P001 and earlier; VE270R001-01 and earlier; GL225P001 and earlier; VL270R001-01 and earlier; VL270R001-01 and earlier.	6.4	More Details
CVE-2020-2737	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.4	More Details
CVE-2020-7276	Authentication bypass vulnerability in MfeUpgradeTool in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 Update allows administrator users to access policy settings via running this tool.	6.4	More Details
CVE-2020-2799	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: GraalVM Compiler). Supported versions that are affected are 19.3.1 and 20.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 6.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2795	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Information Manager Console). Supported versions that are affected are 8.6.0-8.6.2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Knowledge executes to compromise Oracle Knowledge. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Knowledge. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details
CVE-2020-2768	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.3.28 and prior, 7.4.27 and prior, 7.5.17 and prior, 7.6.13 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Cluster as well as unauthorized update, insert or delete access to some of MySQL Cluster accessible data. CVSS 3.0 Base Score 6.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H).	6.3	More Details
CVE-2020-11010	In Tortoise ORM before versions 0.15.23 and 0.16.6, various forms of SQL injection have been found for MySQL and when filtering or doing mass-updates on char/text fields. SQLite & PostgreSQL are only affected when filtering with contains, starts_with, or ends_with filters (and their case-insensitive counterparts).	6.3	More Details
CVE-2020-2955	Vulnerability in the Oracle FLEXCUBE Core Banking product of Oracle Financial Services Applications (component: Transaction Processing). The supported version that is affected is 4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Core Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Core Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Core Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Core Banking. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4271	IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow an authenticated user to send a specially crafted command which would be executed as a lower privileged user. IBM X-ForceID: 175897.	6.3	More Details
CVE-2020-4294	IBM QRadar 7.3.0 to 7.3.3 Patch 2 is vulnerable to Server Side Request Forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 176404.	6.3	More Details
CVE-2017-18798	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, D7000 before 1.0.1.50, and D1500 before 1.0.0.25.	6.2	More Details
CVE-2017-18836	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	6.2	More Details
CVE-2017-18797	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400 before 1.0.1.24, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	6.2	More Details
CVE-2017-18790	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	6.2	More Details
CVE-2017-18840	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	6.2	More Details
CVE-2017-18803	NETGEAR R7800 devices before 1.0.2.30 are affected by incorrect configuration of security settings.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2868	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Diagnostic Framework). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-9445	Zulip Server before 2.1.3 allows XSS via the modal_link feature in the Markdown functionality.	6.1	More Details
CVE-2019-4644	IBM Maximo Asset Management 7.6 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: 170880.	6.1	More Details
CVE-2020-5729	In OpenMRS 2.9 and prior, the UI Framework Error Page reflects arbitrary, user-supplied input back to the browser, which can result in XSS. Any page that is able to trigger a UI Framework Error is susceptible to this issue.	6.1	More Details
CVE-2020-11944	Abe (aka bitcoin-abe) through 0.7.2, and 0.8pre, allows XSS in __call__ in abe.py because the PATH_INFO environment variable is mishandled during a PageNotFound exception.	6.1	More Details
CVE-2020-9444	Zulip Server before 2.1.3 allows reverse tabnabbing via the Markdown functionality.	6.1	More Details
CVE-2020-5728	OpenMRS 2.9 and prior copies "Referrer" header values into an html element named "redirectUrl" within many webpages (such as login.htm). There is insufficient validation for this parameter, which allows for the possibility of cross-site scripting.	6.1	More Details
CVE-2019-19394	Northern.tech CFEngine Enterprise before 3.10.7, 3.11.x and 3.12.x before 3.12.3, 3.13.x, and 3.14.x allows XSS. This is fixed in 3.10.7, 3.12.3, and 3.15.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1050	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-1049.	6.1	More Details
CVE-2020-2751	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-5730	In OpenMRS 2.9 and prior, the sessionLocation parameter for the login page is vulnerable to cross-site scripting.	6.1	More Details
CVE-2017-18800	Certain NETGEAR devices are affected by reflected XSS. This affects R6700v2 before 1.1.0.42 and R6800 before 1.1.0.42.	6.1	More Details
CVE-2020-2954	Vulnerability in the PeopleSoft Enterprise HRMS product of Oracle PeopleSoft (component: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HRMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2920	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). Supported versions that are affected are 9.3.3, 9.3.5 and 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2019-20756	Certain NETGEAR devices are affected by reflected XSS. This affects EX7000 before 1.0.0.64, EX6200 before 1.0.3.86, EX6150 before 1.0.0.38, EX6130 before 1.0.0.22, EX6120 before 1.0.0.40, EX6100 before 1.0.2.22, EX6000 before 1.0.0.30, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, R8300 before 1.0.2.94, R7300DST before 1.0.0.62, R7000P before 1.3.0.20, R6900P before 1.3.0.20, R6400 before 1.0.1.32, R6300v2 before 1.0.4.24, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.18, and WN2500RPv2 before 1.0.1.52.	6.1	More Details
CVE-2020-11663	CA API Developer Portal 4.3.1 and earlier handles 404 requests in an insecure manner, which allows attackers to perform open redirect attacks.	6.1	More Details
CVE-2020-5733	In OpenMRS 2.9 and prior, the export functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows the export of potentially sensitive information.	6.1	More Details
CVE-2017-18833	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	6.1	More Details
CVE-2020-7261	Buffer Overflow via Environment Variables vulnerability in AMSI component in McAfee Endpoint Security (ENS) Prior to 10.7.0 February 2020 Update allows local users to disable Endpoint Security via a carefully crafted user input.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2811	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-5732	In OpenMRS 2.9 and prior, he import functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows unauthenticated users to use a feature typically restricted to administrators.	6.1	More Details
CVE-2017-18834	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	6.1	More Details
CVE-2020-11887	svg2png 4.1.1 allows XSS with resultant SSRF via JavaScript inside an SVG document.	6.1	More Details
CVE-2020-11665	CA API Developer Portal 4.3.1 and earlier handles loginRedirect page redirects in an insecure manner, which allows attackers to perform open redirect attacks.	6.1	More Details
CVE-2020-11664	CA API Developer Portal 4.3.1 and earlier handles homeRedirect page redirects in an insecure manner, which allows attackers to perform open redirect attacks.	6.1	More Details
CVE-2020-5731	In OpenMRS 2.9 and prior, the app parameter for the ActiveVisit's page is vulnerable to cross-site scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18835	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	6.1	More Details
CVE-2020-11888	python-markdown2 through 2.3.8 allows XSS because element names are mishandled unless a \w+ match succeeds. For example, an attack might use elementname@ or elementname- with an onclick attribute.	6.1	More Details
CVE-2020-11930	The GTranslate plugin before 2.8.52 for WordPress has Reflected XSS via a crafted link. This requires use of the hreflang tags feature within a sub-domain or sub-directory paid option.	6.1	More Details
CVE-2020-3954	Open Redirect vulnerability exists in VMware vRealize Log Insight prior to 8.1.0 due to improper Input validation.	6.1	More Details
CVE-2020-11791	NETGEAR JGS516PE devices before 2.6.0.43 are affected by reflected XSS.	6.1	More Details
CVE-2020-2797	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Process Scheduler). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2741	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-2743	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-2894	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2019-20676	Certain NETGEAR devices are affected by lack of access control at the function level. This affects FS728TLP before 1.0.1.26, GS105Ev2 before 1.6.0.4, GS105PE before 1.6.0.4, GS108Ev3 before 2.06.08, GS108PEv3 before 2.06.08, GS110EMX before 1.0.1.4, GS116Ev2 before 2.6.0.35, GS408EPP before 1.0.0.15, GS724TPv2 before 1.1.1.29, GS808E before 1.7.0.7, GS810EMX before 1.7.1.1, GS908E before 1.7.0.3, GSS108E before 1.6.0.4, GSS108EPP before 1.0.0.15, GSS116E before 1.6.0.9, JGS516PE before 2.6.0.35, JGS524Ev2 before 2.6.0.35, JGS524PE before 2.6.0.35, XS512EM before 1.0.1.1, XS708Ev2 before 1.6.0.23, XS716E before 1.6.0.23, and XS724EM before 1.0.1.1.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2946	Vulnerability in the Application Performance Management product of Oracle Enterprise Manager (component: EM Request Monitoring). Supported versions that are affected are 12.1.0.5, 13.2.0.0 and 13.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Application Performance Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Application Performance Management accessible data as well as unauthorized update, insert or delete access to some of Application Performance Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Application Performance Management. CVSS 3.0 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L).	6.0	More Details
CVE-2019-4594	IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-ForceID: 167810.	5.9	More Details
CVE-2020-2524	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: InQuira Search). Supported versions that are affected are 8.6.0-8.6.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Knowledge. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details
CVE-2019-12521	An issue was discovered in Squid through 4.7. When Squid is parsing ESI, it keeps the ESI elements in ESIContext. ESIContext contains a buffer for holding a stack of ESIElements. When a new ESIElement is parsed, it is added via addStackElement. addStackElement has a check for the number of elements in this buffer, but it's off by 1, leading to a Heap Overflow of 1 element. The overflow is within the same structure so it can't affect adjacent memory blocks, and thus just leads to a crash while processing.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2932	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Information Manager Console). Supported versions that are affected are 8.6.0-8.6.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Knowledge. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details
CVE-2020-2804	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details
CVE-2019-20647	NETGEAR RAX40 devices before 1.0.3.64 are affected by denial of service.	5.7	More Details
CVE-2020-0794	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.	5.5	More Details
CVE-2020-0899	An elevation of privilege vulnerability exists when Microsoft Visual Studio updater service improperly handles file permissions, aka 'Microsoft Visual Studio Elevation of Privilege Vulnerability'.	5.5	More Details
CVE-2020-0900	An elevation of privilege vulnerability exists when the Visual Studio Extension Installer Service improperly handles file operations, aka 'Visual Studio Extension Installer Service Elevation of Privilege Vulnerability'.	5.5	More Details
CVE-2019-2056	There is a possible disclosure of RAM using a shared crypto key due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140879284	5.5	More Details
CVE-2020-0699	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0962.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20784	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (MTK chipsets) software. Interaction of GPS with 911 emergency calls is mishandled. The LG ID is LVE-SMP-180012 (January 2019).	5.5	More Details
CVE-2019-20779	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A TrustZone trusted application can crash via crafted input. The LG ID is LVE-SMP-190003 (May 2019).	5.5	More Details
CVE-2019-20776	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. A TZ trusted application can crash via crafted input. The LG ID is LVE-SMP-190005 (July 2019).	5.5	More Details
CVE-2019-20775	An issue was discovered on LG mobile devices with Android OS 9.0 (Qualcomm SDM450, SDM845, SM6150, and SM8150 chipsets) software. Weak encryption leads to local information disclosure. The LG ID is LVE-SMP-190010 (August 2019).	5.5	More Details
CVE-2019-20774	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A system service allows local retrieval of the user's password. The LG ID is LVE-SMP-190009 (August 2019).	5.5	More Details
CVE-2020-7084	A NULL pointer dereference vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	5.5	More Details
CVE-2019-14007	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, Rennell, SA6155P, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	5.5	More Details
CVE-2020-1016	An information disclosure vulnerability exists when the Windows Push Notification Service improperly handles objects in memory, aka 'Windows Push Notification Service Information Disclosure Vulnerability'.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0937	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0939, CVE-2020-0945, CVE-2020-0946, CVE-2020-0947.	5.5	More Details
CVE-2020-0962	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0699.	5.5	More Details
CVE-2020-9070	Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure.	5.5	More Details
CVE-2020-10637	Eaton HMiSoft VU3 (HMIVU3 runtime not impacted), Version 3.00.23 and prior, however, the HMIVU runtimes are not impacted by these issues. A specially crafted input file could trigger an out-of-bounds read when loaded by the affected product.	5.5	More Details
CVE-2020-0947	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0937, CVE-2020-0939, CVE-2020-0945, CVE-2020-0946.	5.5	More Details
CVE-2019-10523	Target specific data is being sent to remote server and leads to information exposure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6574AU, QCS605, Rennell, SDA660, SDM429W, SDM439, SDM450, SDM710, SDM845, SM7150, SM8150, SM8250, SXR2130	5.5	More Details
CVE-2020-0939	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0937, CVE-2020-0945, CVE-2020-0946, CVE-2020-0947.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14075	Null pointer dereference issue in radio interface layer due to lack of null check in sapmodule destructor in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS605, Rennell, Saipan, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR2130	5.5	More Details
CVE-2019-10483	Side channel issue in QTEE due to usage of non-time-constant comparison function such as memcmp or strcmp in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8016, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	5.5	More Details
CVE-2017-18823	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	5.5	More Details
CVE-2017-18847	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	5.5	More Details
CVE-2020-0955	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure in CPU Memory Access'.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10608	Information disclosure issue occurs as there is no binding between the secure keypad session and the secure display session that allows user to take control of the REE to stop the secure keypad session and read the keypad input. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, MSM8905, MSM8909	5.5	More Details
CVE-2020-4338	IBM MQ 9.1.4 could allow a local attacker to obtain sensitive information by inclusion of sensitive data within runmqras data. IBM X-Force ID: 177937.	5.5	More Details
CVE-2020-0821	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1007.	5.5	More Details
CVE-2020-2760	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2020-1007	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0821.	5.5	More Details
CVE-2020-1005	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0982, CVE-2020-0987.	5.5	More Details
CVE-2020-0935	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links, aka 'OneDrive for Windows Elevation of Privilege Vulnerability'.	5.5	More Details
CVE-2020-5721	MikroTik WinBox 3.22 and below stores the user's cleartext password in the settings.cfg.viw configuration file when the Keep Password field is set and no Master Password is set. Keep Password is set by default and, by default Master Password is not set. An attacker with access to the configuration file can extract a username and password to gain access to the router.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0945	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0937, CVE-2020-0939, CVE-2020-0946, CVE-2020-0947.	5.5	More Details
CVE-2020-0946	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0937, CVE-2020-0939, CVE-2020-0945, CVE-2020-0947.	5.5	More Details
CVE-2020-0987	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0982, CVE-2020-1005.	5.5	More Details
CVE-2020-0982	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0987, CVE-2020-1005.	5.5	More Details
CVE-2019-20738	Certain NETGEAR devices are affected by stored XSS. This affects D6100 before 1.0.0.58, D7800 before 1.0.1.34, JNR1010v2 before 1.1.0.50, JWNR2010v5 before 1.1.0.50, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6100 before 1.0.1.16, R6120 before 1.0.0.40, R6700v2 before 1.2.0.14, R6800 before 1.2.0.14, R6900v2 before 1.2.0.14, R7500v2 before 1.0.3.26, R7800 before 1.0.2.46, R9000 before 1.0.4.2, WN3000RPv2 before 1.0.0.52, WN3000RPv3 before 1.0.2.78, WNDR3700v4 before 1.0.2.102, WNDR3700v5 before 1.1.0.54, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.50, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.50, and WNR2050 before 1.1.0.50. NOTE: this may be a result of an incomplete fix for CVE-2017-18866.	5.4	More Details
CVE-2020-0954	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0973, CVE-2020-0978.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5737	Stored XSS in Tenable.Sc before 5.14.0 could allow an authenticated remote attacker to craft a request to execute arbitrary script code in a user's browser session. Updated input validation techniques have been implemented to correct this issue.	5.4	More Details
CVE-2020-2747	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: SSO Engine). Supported versions that are affected are 11.1.2.3.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-0930	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details
CVE-2020-4268	IBM QRadar 7.3.0 to 7.3.3 Patch 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-ForceID: 175841.	5.4	More Details
CVE-2020-0923	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details
CVE-2020-10935	Zulip Server before 2.1.3 allows XSS via a Markdown link, with resultant account takeover.	5.4	More Details
CVE-2019-19390	The Search parameter of the Software Catalogue section of Matrix42 Workspace Management 9.1.2.2765 and below accepts unfiltered parameters that lead to multiple reflected XSS issues.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4274	IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow an authenticated user to access data and perform unauthorized actions due to inadequate permission checks. IBM X-ForceID: 175980.	5.4	More Details
CVE-2020-0972	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-0975, CVE-2020-0976, CVE-2020-0977.	5.4	More Details
CVE-2020-0973	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0978.	5.4	More Details
CVE-2020-1049	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-1050.	5.4	More Details
CVE-2019-19500	Matrix42 Workspace Management 9.1.2.2765 and below allows stored XSS via unfiltered description parameters, as demonstrated by the comment field of a special order for individual software.	5.4	More Details
CVE-2019-4446	IBM Maximo Asset Management 7.6 could allow an authenticated user perform actions they are not authorized to by modifying request parameters. IBM X-Force ID: 163490.	5.4	More Details
CVE-2019-4749	IBM Maximo Asset Management 7.6 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: 173308.	5.4	More Details
CVE-2020-0975	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-0972, CVE-2020-0976, CVE-2020-0977.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0976	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-0972, CVE-2020-0975, CVE-2020-0977.	5.4	More Details
CVE-2020-0977	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-0972, CVE-2020-0975, CVE-2020-0976.	5.4	More Details
CVE-2020-0924	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details
CVE-2020-0978	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973.	5.4	More Details
CVE-2020-0925	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details
CVE-2020-11823	In Dolibarr 10.0.6, if USER_LOGIN_FAILED is active, there is a stored XSS vulnerability on the admin tools --> audit page. This may lead to stealing of the admin account.	5.4	More Details
CVE-2020-0926	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0927, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0927	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0930, CVE-2020-0933, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details
CVE-2019-20693	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects WAC505 before 8.0.6.4 and WAC510 before 8.0.6.4.	5.4	More Details
CVE-2020-2744	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Security). Supported versions that are affected are 6.3.7, 6.4.2 and 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-0933	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0923, CVE-2020-0924, CVE-2020-0925, CVE-2020-0926, CVE-2020-0927, CVE-2020-0930, CVE-2020-0954, CVE-2020-0973, CVE-2020-0978.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2706	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Project Manager). Supported versions that are affected are 16.2.0.0 - 16.2.19.3, 17.12.0.0 - 17.12.17.0, 18.8.0.0 - 18.8.18.0, 19.12.1.0 - 19.12.3.0 and 20.1.0.0 - 20.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-11814	A Host Header Injection vulnerability in qdPM 9.1 may allow an attacker to spoof a particular header and redirect users to malicious websites.	5.4	More Details
CVE-2020-11813	In Rukovoditel 2.5.2, there is a stored XSS vulnerability on the configuration page via the copyright text input. Thus, an attacker can inject a malicious script to steal all users' valuable data. This copyright text is on every page so this attack vector can be very dangerous.	5.4	More Details
CVE-2020-2781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2783	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2020-1803	Huawei smartphones Honor V20 with versions earlier than 10.0.0.179(C636E3R4P3),versions earlier than 10.0.0.180(C185E3R3P3),versions earlier than 10.0.0.180(C432E10R3P4) have an information disclosure vulnerability. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure.	5.3	More Details
CVE-2020-2865	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: Installation). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Configurator accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-2866	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments / File Upload). Supported versions that are affected are 12.2.5-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2888	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Partners). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Marketing accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-2753	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Workflow accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2020-2887	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2020-2766	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2830	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2020-2889	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-2949	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Caching, CacheStore, Invocation). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Coherence accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-11883	In Divante vue-storefront-api through 1.11.1 and storefront-api through 1.0-rc.1, as used in VueStorefront PWA, unexpected HTTP requests lead to an exception that discloses the error stack trace, with absolute file paths and Node.js module names.	5.3	More Details
CVE-2020-11891	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized editing of usergroups.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2864	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Accounts). Supported versions that are affected are 12.1.3 and 12.2.5-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iSupplier Portal accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-2775	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-11890	An issue was discovered in Joomla! before 3.9.17. Improper input validations in the usergroup table class could lead to a broken ACL configuration.	5.3	More Details
CVE-2020-11889	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized deletion of usergroups.	5.3	More Details
CVE-2020-2806	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.28 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.3	More Details
CVE-2020-2752	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20759	NETGEAR R9000 devices before 1.0.4.26 are affected by stored XSS.	5.2	More Details
CVE-2019-20742	NETGEAR WAC510 devices before 8.0.1.3 are affected by stored XSS.	5.2	More Details
CVE-2019-20743	NETGEAR WAC510 devices before 8.0.1.3 are affected by stored XSS.	5.2	More Details
CVE-2020-1751	An out-of-bounds write vulnerability was found in glibc before 2.31 when handling signal trampolines on PowerPC. Specifically, the backtrace function did not properly check the array bounds when storing the frame address, resulting in a denial of service or potential code execution. The highest threat from this vulnerability is to system availability.	5.1	More Details
CVE-2020-2934	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.19 and prior and 5.1.48 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L).	5.0	More Details
CVE-2020-2912	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Self-Service). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. While the vulnerability is in PeopleSoft Enterprise CS Campus Community, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.0 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2928	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2896	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2924	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2897	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2829	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Management Services). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2020-2761	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2893	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2898	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). The supported version that is affected is 8.0.19. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2901	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-7113	A vulnerability was found when an attacker, while communicating with the ClearPass management interface, is able to intercept and change parameters in the HTTP packets resulting in the compromise of some of ClearPass' service accounts. Resolution: Fixed in 6.7.10, 6.8.1, 6.9.0 and higher.	4.9	More Details
CVE-2020-2903	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2925	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2895	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2923	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2892	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2762	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2763	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2765	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2779	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2774	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2770	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2904	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2812	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2853	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-2814	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.47 and prior, 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2759	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2017-18811	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18812	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18813	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18816	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18839	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details
CVE-2017-18814	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18815	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18821	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18820	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18810	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18831	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details
CVE-2017-18828	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details
CVE-2017-18827	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details
CVE-2017-18807	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details
CVE-2017-18825	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details
CVE-2017-18809	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18832	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	4.8	More Details
CVE-2019-20639	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2020-11785	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20674	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20672	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20671	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20670	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2020-11783	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2553	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Information Manager Console). Supported versions that are affected are 8.6.0-8.6.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge accessible data as well as unauthorized read access to a subset of Oracle Knowledge accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2019-20668	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20667	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20666	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20665	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20664	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2767	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2019-20661	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20660	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2020-5346	RSA Authentication Manager versions prior to 8.4 P11 contain a stored cross-site scripting vulnerability in the Security Console. A malicious RSA Authentication Manager Security Console administrator with advanced privileges could exploit this vulnerability to store arbitrary HTML or JavaScript code through the Security Console web interface. When other Security Console administrators open the affected page, the injected scripts could potentially be executed in their browser.	4.8	More Details
CVE-2020-3953	Cross Site Scripting (XSS) vulnerability exists in VMware vRealize Log Insight prior to 8.1.0 due to improper Input validation.	4.8	More Details
CVE-2020-11787	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2800	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2020-2899	Vulnerability in the PeopleSoft Enterprise SCM Purchasing product of Oracle PeopleSoft (component: Purchasing). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM Purchasing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM Purchasing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM Purchasing accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM Purchasing accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	4.8	More Details
CVE-2019-4654	IBM QRadar 7.3.0 to 7.3.3 Patch 2 does not validate, or incorrectly validates, a certificate which could allow an attacker to spoof a trusted entity by using a man-in-the-middle (MITM) attack. IBM X-ForceID: 170965.	4.8	More Details
CVE-2020-11779	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11780	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20645	NETGEAR RAX40 devices before 1.0.3.62 are affected by stored XSS.	4.8	More Details
CVE-2020-11781	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20644	NETGEAR RAX40 devices before 1.0.3.62 are affected by stored XSS.	4.8	More Details
CVE-2020-11786	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11782	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11784	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20673	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20669	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20675	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7110	ClearPass is vulnerable to Stored Cross Site Scripting by allowing a malicious administrator, or a compromised administrator account, to save malicious scripts within ClearPass that could be executed resulting in a privilege escalation attack. Resolution: Fixed in 6.7.13, 6.8.4, 6.9.0 and higher.	4.8	More Details
CVE-2020-7275	Accessing, modifying or executing executable files vulnerability in the uninstaller in McAfee Endpoint Security (ENS) for Windows Prior to 10.7.0 April 2020 Update allows local users to execute arbitrary code via a carefully crafted input file.	4.8	More Details
CVE-2020-11768	Certain NETGEAR devices are affected by Stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11769	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11771	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11772	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20752	Certain NETGEAR devices are affected by stored XSS. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D7800 before 1.0.1.44, DM200 before 1.0.0.58, R7800 before 1.0.2.58, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBS40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.60, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.68.	4.8	More Details
CVE-2020-11773	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20750	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.47, EX6150v2 before 1.0.1.76, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WN2000RPTv3 before 1.0.1.32, WN3000RPv3 before 1.0.2.70, and WN3100RPv2 before 1.0.0.66.	4.8	More Details
CVE-2019-20677	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20746	Certain NETGEAR devices are affected by reflected XSS. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D7800 before 1.0.1.44, DM200 before 1.0.0.58, R7800 before 1.0.2.58, R8900 before 1.0.4.12, R9000 before 1.0.4.8, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBS40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.60, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.68.	4.8	More Details
CVE-2020-11774	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20749	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.47, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WN2000RPTv3 before 1.0.1.32, WN3000RPv3 before 1.0.2.70, and WN3100RPv2 before 1.0.0.66.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11775	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20720	Certain NETGEAR devices are affected by stored XSS. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D7800 before 1.0.1.47, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WN2000RPTv3 before 1.0.1.32, WN3000RPv3 before 1.0.2.70, and WN3100RPv2 before 1.0.0.66.	4.8	More Details
CVE-2020-11776	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2019-20678	Certain NETGEAR devices are affected by stored XSS. This affects RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK20 before 2.3.5.26, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK40 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.8	More Details
CVE-2019-20721	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.47, EX2700 before 1.0.1.48, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, EX6200v2 before 1.0.1.72, EX6400 before 1.0.2.136, EX7300 before 1.0.2.136, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WN2000RPTv3 before 1.0.1.32, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.66, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.66, XR450 before 2.3.2.32, and XR500 before 2.3.2.32.	4.8	More Details
CVE-2020-11778	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details
CVE-2020-11777	Certain NETGEAR devices are affected by Stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20714	Certain NETGEAR devices are affected by stored XSS. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D7800 before 1.0.1.44, DM200 before 1.0.0.58, R7500v2 before 1.0.3.40, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.22, RBR20 before 2.3.0.22, RBS20 before 2.3.0.22, RBK50 before 2.3.0.22, RBR50 before 2.3.0.22, RBS50 before 2.3.0.22, RBS40 before 2.3.0.22, WN3000RPv2 before 1.0.0.68, WN3000RPv3 before 1.0.2.70, WN3100RPv2 before 1.0.0.60, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.68.	4.8	More Details
CVE-2019-20715	Certain NETGEAR devices are affected by stored XSS. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6100 before 1.0.0.63, D7800 before 1.0.1.47, DM200 before 1.0.0.61, R7500v2 before 1.0.3.40, R7800 before 1.0.2.60, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, and RBS50 before 2.3.0.32.	4.8	More Details
CVE-2020-10932	An issue was discovered in Arm Mbed TLS before 2.16.6 and 2.7.x before 2.7.15. An attacker that can get precise enough side-channel measurements can recover the long-term ECDSA private key by (1) reconstructing the projective coordinate of the result of scalar multiplication by exploiting side channels in the conversion to affine coordinates; (2) using an attack described by Naccache, Smart, and Stern in 2003 to recover a few bits of the ephemeral scalar from those projective coordinates via several measurements; and (3) using a lattice attack to get from there to the long-term ECDSA private key used for the signatures. Typically an attacker would have sufficient access when attacking an SGX enclave and controlling the untrusted OS.	4.7	More Details
CVE-2020-10951	Western Digital My Cloud Home and ibi devices before 2.2.0 allow clickjacking on sign-in pages.	4.7	More Details
CVE-2020-0568	Race condition in the Intel(R) Driver and Support Assistant before version 20.1.5 may allow an authenticated user to potentially enable denial of service via local access.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2886	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2020-2875	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.14 and prior and 5.1.48 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Connectors, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N).	4.7	More Details
CVE-2020-2862	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N).	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2810	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2020-2789	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2020-0943	An authentication bypass vulnerability exists in Microsoft YourPhoneCompanion application for Android, in the way the application processes notifications generated by work profiles.This could allow an unauthenticated attacker to view notifications, aka 'Microsoft YourPhone Application for Android Authentication Bypass Vulnerability'.	4.6	More Details
CVE-2020-2514	Vulnerability in the Oracle Application Express component of Oracle Database Server. The supported version that is affected is Prior to 19.2. Easily exploitable vulnerability allows low privileged attacker having End User Role privilege with network access via HTTPS to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Express. CVSS 3.0 Base Score 4.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2740	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 11.1.2.3.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.0 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	4.6	More Details
CVE-2019-12522	An issue was discovered in Squid through 4.7. When Squid is run as root, it spawns its child processes as a lesser user, by default the user nobody. This is done via the leave_suid call. leave_suid leaves the Saved UID as 0. This makes it trivial for an attacker who has compromised the child process to escalate their privileges back to root.	4.5	More Details
CVE-2018-21141	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	4.5	More Details
CVE-2019-20744	NETGEAR WAC510 devices before 5.0.10.2 are affected by disclosure of sensitive information.	4.5	More Details
CVE-2020-2921	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2930	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2020-2926	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2020-0077	In authorize_enroll of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146055840	4.4	More Details
CVE-2020-0075	In set_shared_key of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146057864	4.4	More Details
CVE-2019-20729	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JNDR3000 before 1.0.0.22, R6250 before 1.0.4.26, R6300v2 before 1.0.4.22, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R7000 before 1.0.9.28, R6900P before 1.3.1.26, R7000P before 1.3.1.26, R7300DST before 1.0.0.62, R7900 before 1.0.2.16, R8000 before 1.0.4.18, R7900P before 1.4.1.42, R8000P before 1.4.1.42, R8300 before 1.0.2.116, R8500 before 1.0.2.116, WNDR3400v3 before 1.0.1.18, WNDR4500v2 before 1.0.0.68, and WNR3500Lv2 before 1.2.0.48.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0068	In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: Android. Versions: Android kernel. Android ID: A-139354541	4.4	More Details
CVE-2020-5266	In the ps_link module for PrestaShop before version 3.1.0, there is a stored XSS when you create or edit a link list block with the title field. The problem is fixed in 3.1.0	4.4	More Details
CVE-2020-0067	In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: Android. Versions: Android kernel. Android ID: A-120551147.	4.4	More Details
CVE-2020-5264	In PrestaShop before version 1.7.6.5, there is a reflected XSS while running the security compromised page. It allows anyone to execute arbitrary action. The problem is patched in the 1.7.6.5.	4.4	More Details
CVE-2020-5265	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminAttributesGroups page. The problem is patched in 1.7.6.5.	4.4	More Details
CVE-2020-2869	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2020-11659	CA API Developer Portal 4.3.1 and earlier contains an access control flaw that allows privileged users to perform a restricted user administration action.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2522	Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Information Manager Console). Supported versions that are affected are 8.6.0-8.6.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2020-2738	Vulnerability in the Siebel UI Framework product of Oracle Siebel CRM (component: EAI, SWSE). Supported versions that are affected are 20.2 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel UI Framework accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2019-20663	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.3	More Details
CVE-2020-2745	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Federation). Supported versions that are affected are 11.1.2.3.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Access Manager. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2019-20662	Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.	4.3	More Details
CVE-2020-2177	Jenkins Copr Plugin 0.3 and earlier stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	4.3	More Details
CVE-2020-4260	IBM UrbanCode Deploy (UCD) 7.0.5 could allow a user with special permissions to obtain sensitive information via generic processes. IBM X-Force ID: 175639.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-4593	IBM QRadar 7.3.0 to 7.3.3 Patch 2 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-ForceID: 167743.	4.3	More Details
CVE-2019-7306	Byobu Apport hook may disclose sensitive information since it automatically uploads the local user's .screenrc which may contain private hostnames, usernames and passwords. This issue affects: byobu	4.3	More Details
CVE-2020-2947	Vulnerability in the PeopleSoft Enterprise HCM Absence Management product of Oracle PeopleSoft (component: Absence Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Absence Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Absence Management accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2017-18808	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	4.2	More Details
CVE-2020-2777	Vulnerability in the Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Hyperion Financial Management accessible data. CVSS 3.0 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N).	4.2	More Details
CVE-2020-5288	"In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there is improper access controls on product attributes page. The problem is fixed in 1.7.6.5.	4.1	More Details
CVE-2020-5287	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is improper access control on customers search. The problem is fixed in 1.7.6.5.	4.1	More Details
CVE-2020-5286	In PrestaShop between versions 1.7.4.0 and 1.7.6.5, there is a reflected XSS when uploading a wrong file. The problem is fixed in 1.7.6.5	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5276	In PrestaShop between versions 1.7.1.0 and 1.7.6.5, there is a reflected XSS on AdminCarts page with `cartBox` parameter The problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-5273	In PrestaShop module ps_linklist versions before 3.1.0, there is a stored XSS when using custom URLs. The problem is fixed in version 3.1.0	4.1	More Details
CVE-2020-5294	PrestaShop module ps_facetedsearch versions before 2.1.0 has a reflected XSS with social networks fields The problem is fixed in 2.1.0	4.1	More Details
CVE-2020-2772	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: Absence Recording, Maintenance). Supported versions that are affected are 12.2.6-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Human Resources, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Human Resources accessible data. CVSS 3.0 Base Score 4.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N).	4.1	More Details
CVE-2020-5285	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is a reflected XSS with `back` parameter. The problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-5279	In PrestaShop between versions 1.5.0.0 and 1.7.6.5, there are improper access control since the the version 1.5.0.0 for legacy controllers. - admin-dev/index.php/configure/shop/customer-preferences/ - admin-dev/index.php/improve/international/translations/ - admin-dev/index.php/improve/international/geolocation/ - admin-dev/index.php/improve/international/localization - admin-dev/index.php/configure/advanced/performance - admin-dev/index.php/sell/orders/delivery-slips/ - admin-dev/index.php?controller=AdminStatuses The problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-5272	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is a reflected XSS on Search page with `alias` and `search` parameters. The problem is patched in 1.7.6.5	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5278	In PrestaShop between versions 1.5.4.0 and 1.7.6.5, there is a reflected XSS on Exception page The problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-5271	In PrestaShop between versions 1.6.0.0 and 1.7.6.5, there is a reflected XSS with `date_from` and `date_to` parameters in the dashboard page This problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-5270	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is an open redirection when using back parameter. The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-5269	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminFeatures page by using the `id_feature` parameter. The problem is fixed in 1.7.6.5	4.1	More Details
CVE-2020-11008	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where _some_ credential is leaked (but the attacker cannot control which one). Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently published Git versions can cause Git to send a "blank" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching _any_ URL, and will return some unspecified stored password, leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to `git clone`. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The root of the problem is in Git itself, which should not be feeding blank input to helpers. However, the ability to exploit the vulnerability in practice depends on which helpers are in use. Credential helpers which are known to trigger the vulnerability: - Git's "store" helper - Git's "cache" helper - the "osxkeychain" helper that ships in Git's "contrib" directory Credential helpers which are known to be safe even with vulnerable versions of Git: - Git Credential Manager for Windows Any helper not in this list should be assumed to trigger the vulnerability.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7255	Privilege escalation vulnerability in the administrative user interface in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows local users to gain elevated privileges via ENS not checking user permissions when editing configuration in the ENS client interface. Administrators can lock the ENS client interface through ePO to prevent users being able to edit the configuration.	3.9	More Details
CVE-2020-2778	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2020-2773	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2754	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2020-2755	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2756	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2020-2757	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2020-2764	Vulnerability in the Java SE product of Oracle Java SE (component: Advanced Management Console). The supported version that is affected is Java Advanced Management Console: 2.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2922	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2020-2900	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Tools). Supported versions that are affected are 19.3.1 and 20.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N).	3.7	More Details
CVE-2019-20648	NETGEAR RN42400 devices before 6.10.2 are affected by incorrect configuration of security settings.	3.5	More Details
CVE-2017-18824	Certain NETGEAR devices are affected by directory traversal. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	3.3	More Details
CVE-2017-18819	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2748	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
CVE-2020-11767	Istio through 1.5.1 and Envoy through 1.14.1 have a data-leak issue. If there is a TCP connection (negotiated with SNI over HTTPS) to *.example.com, a request for a domain concurrently configured explicitly (e.g., abc.example.com) is sent to the server(s) listening behind *.example.com. The outcome should instead be 421 Misdirected Request. Imagine a shared caching forward proxy re-using an HTTP/2 connection for a large subnet with many users. If a victim is interacting with abc.example.com, and a server (for abc.example.com) recycles the TCP connection to the forward proxy, the victim's browser may suddenly start sending sensitive data to a *.example.com server. This occurs because the forward proxy between the victim and the origin server reuses connections (which obeys the specification), but neither Istio nor Envoy corrects this by sending a 421 error. Similarly, this behavior voids the security model browsers have put in place between domains.	3.1	More Details
CVE-2020-5301	SimpleSAMLphp versions before 1.18.6 contain an information disclosure vulnerability. The module controller in `SimpleSAML\Module` that processes requests for pages hosted by modules, has code to identify paths ending with `.php` and process those as PHP code. If no other suitable way of handling the given path exists it presents the file to the browser. The check to identify paths ending with `.php` does not account for uppercase letters. If someone requests a path ending with e.g. `.PHP` and the server is serving the code from a case-insensitive file system, such as on Windows, the processing of the PHP code does not occur, and the source code is instead presented to the browser. An attacker may use this issue to gain access to the source code in third-party modules that is meant to be private, or even sensitive. However, the attack surface is considered small, as the attack will only work when SimpleSAMLphp serves such content from a file system that is not case-sensitive, such as on Windows. This issue is fixed in version 1.18.6.	3.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2909	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 2.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	2.8	More Details
CVE-2020-2749	Vulnerability in the Oracle Solaris product of Oracle Systems (component: SMF command svcbundle). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.0 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:N/I:L/A:N).	2.5	More Details
CVE-2020-2771	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Whodo). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.0 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N).	2.5	More Details
CVE-2020-2734	Vulnerability in the RDBMS/Optimizer component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Execute on DBMS_SQLTUNE privilege with network access via Oracle Net to compromise RDBMS/Optimizer. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS/Optimizer accessible data. CVSS 3.0 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2769	Vulnerability in the Hyperion Financial Reporting product of Oracle Hyperion (component: Web Based Report Designer). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Hyperion Financial Reporting accessible data. CVSS 3.0 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).	2.4	More Details
CVE-2020-2933	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 5.1.48 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.2	More Details
CVE-2020-10707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-11612. Reason: This candidate is a reservation duplicate of CVE-2020-11612. Notes: All CVE users should reference CVE-2020-11612 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-7612	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-2019-11285	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-2019-10148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-12779. Reason: This candidate is a reservation duplicate of CVE-2019-12779. Notes: All CVE users should reference CVE- CVE-2019-12779 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10178	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-11637. Reason: This candidate is a reservation duplicate of CVE-2020-11637. Notes: All CVE users should reference CVE-2020-11637 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-8842	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-2020-11747	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-8497. Reason: This candidate is a reservation duplicate of CVE-2020-8497. Notes: All CVE users should reference CVE-2020-8497 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details