SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 October 2020

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-14871	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Pluggable authentication module). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols 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. Note: This CVE is not exploitable for Solaris 11.1 and later releases, and ZFSSA 8.7 and later releases, thus the CVSS Base Score is 0.0. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2020-7127	A remote unauthenticated arbitrary code execution vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8581	An out-of-bounds read was addressed with improved input validation. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. A remote attacker may be able to leak memory.	9.8	More Details
CVE-2020-26879	Ruckus vRioT through 1.5.1.0.21 has an API backdoor that is hardcoded into validate_token.py. An unauthenticated attacker can interact with the service API by using a backdoor value as the Authorization header.	9.8	More Details
CVE-2020-27743	libtac in pam_tacplus through 1.5.1 lacks a check for a failure of RAND_bytes()/RAND_pseudo_bytes(). This could lead to use of a non-random/predictable session_id.	9.8	More Details
CVE-2020-27179	konzept-ix publiXone before 2020.015 allows attackers to take over arbitrary user accounts by crafting password-reset tokens.	9.8	More Details
CVE-2020-27183	A RemoteFunctions endpoint with missing access control in konzept-ix publiXone before 2020.015 allows attackers to disclose sensitive user information, send arbitrary e-mails, escalate the privileges of arbitrary user accounts, and have unspecified other impact.	9.8	More Details
CVE-2020-10256	An issue was discovered in beta versions of the 1Password command-line tool prior to 0.5.5 and in beta versions of the 1Password SCIM bridge prior to 0.7.3. An insecure random number generator was used to generate various keys. An attacker with access to the user's encrypted data may be able to perform brute-force calculations of encryption keys and thus succeed at decryption.	9.8	More Details
CVE-2020-11854	Arbitrary code execution vlnerability in Operation bridge Manager, Application Performance Management and Operations Bridge (containerized) vulnerability in Micro Focus products products Operation Bridge Manager, Operation Bridge (containerized) and Application Performance Management. The vulneravility affects: 1.) Operation Bridge Manager versions 2020.05, 2019.11, 2019.05, 2018.11, 2018.05, 10.63,10.62, 10.61, 10.60, 10.12, 10.11, 10.10 and all earlier versions. 2.) Operations Bridge (containerized) 2020.05, 2019.08, 2019.05, 2018.11, 2018.08, 2018.05. 2018.02 and 2017.11. 3.) Application Performance Management versions 9,51, 9.50 and 9.40 with uCMDB 10.33 CUP 3. The vulnerability could allow Arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27853	Wire before 2020-10-16 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a format string. This affects Wire AVS (Audio, Video, and Signaling) 5.3 through 6.x before 6.4, the Wire Secure Messenger application before 3.49.918 for Android, and the Wire Secure Messenger application before 3.61 for iOS. This occurs via the value parameter to sdp_media_set_lattr in peerflow/sdp.c.	9.8	More Details
CVE-2018-4296	This issue is fixed in macOS Mojave 10.14. A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks.	9.8	More Details
CVE-2019-7288	The issue was addressed with improved validation on the FaceTime server. This issue is fixed in macOS Mojave 10.14.3 Supplemental Update, iOS 12.1.4. A thorough security audit of the FaceTime service uncovered an issue with Live Photos .	9.8	More Details
CVE-2019-8547	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, watchOS 5.2, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.2. A remote attacker may be able to leak memory.	9.8	More Details
CVE-2019-8572	A null pointer dereference was addressed with improved input validation. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. A remote attacker may be able to cause arbitrary code execution.	9.8	More Details
CVE-2019-8578	A use after free issue was addressed with improved memory management. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. A remote attacker may be able to cause arbitrary code execution.	9.8	More Details
CVE-2019-8712	A memory corruption issue was addressed with improved memory handling. This issue is fixed in watchOS 6, iOS 13, tvOS 13. An application may be able to execute arbitrary code with system privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14825	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. 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 takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2019-8716	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006. An application may be able to execute arbitrary code with system privileges.	9.8	More Details
CVE-2019-8746	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15, iOS 13, iCloud for Windows 7.14, iCloud for Windows 10.7, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6, iTunes 12.10.1 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details
CVE-2019-8749	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Catalina 10.15, iOS 13, iCloud for Windows 7.14, iCloud for Windows 10.7, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6, iTunes 12.10.1 for Windows. Multiple issues in libxml2.	9.8	More Details
CVE-2019-8756	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Catalina 10.15, iOS 13, iCloud for Windows 7.14, iCloud for Windows 10.7, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6, iTunes 12.10.1 for Windows. Multiple issues in libxml2.	9.8	More Details
CVE-2019-8767	A memory consumption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15. Processing a maliciously crafted string may lead to heap corruption.	9.8	More Details
CVE-2020-12830	Addressed multiple stack buffer overflow vulnerabilities that could allow an attacker to carry out escalation of privileges through unauthorized remote code execution in Western Digital My Cloud devices before 5.04.114.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25765	Addressed remote code execution vulnerability in reg_device.php due to insufficient validation of user input.in Western Digital My Cloud Devices prior to 5.4.1140.	9.8	More Details
CVE-2020-27158	Addressed remote code execution vulnerability in cgi_api.php that allowed escalation of privileges in Western Digital My Cloud NAS devices prior to 5.04.114.	9.8	More Details
CVE-2020-27159	Addressed remote code execution vulnerability in DsdkProxy.php due to insufficient sanitization and insufficient validation of user input in Western Digital My Cloud NAS devices prior to 5.04.114	9.8	More Details
CVE-2020-27160	Addressed remote code execution vulnerability in AvailableApps.php that allowed escalation of privileges in Western Digital My Cloud NAS devices prior to 5.04.114 (issue 3 of 3).	9.8	More Details
CVE-2019-8531	A validation issue existed in Trust Anchor Management. This issue was addressed with improved validation. This issue is fixed in watchOS 5.2, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.2. An untrusted radius server certificate may be trusted.	9.8	More Details
CVE-2020-7197	SSMC3.7.0.0 is vulnerable to remote authentication bypass. HPE StoreServ Management Console (SSMC) 3.7.0.0 is an off node multiarray manager web application and remains isolated from data on the managed arrays. HPE has provided an update to HPE StoreServ Management Console (SSMC) software 3.7.0.0* Upgrade to HPE 3PAR StoreServ Management Console 3.7.1.1 or later.	9.8	More Details
CVE-2020-9866	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. A buffer overflow may result in arbitrary code execution.	9.8	More Details
CVE-2020-7124	A remote unauthorized access vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14841	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, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-27605	BigBlueButton through 2.2.28 uses Ghostscript for processing of uploaded EPS documents, and consequently may be subject to attacks related to a "schwache Sandbox."	9.8	More Details
CVE-2020-27615	The Loginizer plugin before 1.6.4 for WordPress allows SQL injection (with resultant XSS), related to loginizer_login_failed and lz_valid_ip.	9.8	More Details
CVE-2020-27619	In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK codec tests call eval() on content retrieved via HTTP.	9.8	More Details
CVE-2020-15906	tiki-login.php in Tiki before 21.2 sets the admin password to a blank value after 50 invalid login attempts.	9.8	More Details
CVE-2020-9898	This issue was addressed with improved entitlements. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A sandboxed process may be able to circumvent sandbox restrictions.	9.8	More Details
CVE-2020-14859	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, 12.2.1.4.0 and 14.1.1.0.0. 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 takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14855	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Administration). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-27664	admin/src/containers/InputModalStepperProvider/index.js in Strapi before 3.2.5 has unwanted /proxy?url= functionality.	9.8	More Details
CVE-2019-17006	In Network Security Services (NSS) before 3.46, several cryptographic primitives had missing length checks. In cases where the application calling the library did not perform a sanity check on the inputs it could result in a crash due to a buffer overflow.	9.8	More Details
CVE-2020-15683	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4.	9.8	More Details
CVE-2020-15684	Mozilla developers reported memory safety bugs present in Firefox 81. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 82.	9.8	More Details
CVE-2020-25466	A SSRF vulnerability exists in the downloadimage interface of CRMEB 3.0, which can remotely download arbitrary files on the server and remotely execute arbitrary code.	9.8	More Details
CVE-2020-25483	An arbitrary command execution vulnerability exists in the fopen() function of file writes of UCMS v1.4.8, where an attacker can gain access to the server.	9.8	More Details
CVE-2020-27678	An issue was discovered in illumos before 2020-10-22, as used in OmniOS before r151030by, r151032ay, and r151034y and SmartOS before 20201022. There is a buffer overflow in parse_user_name in lib/libpam/pam_framework.c.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14882	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, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-7750	This affects the package scratch-svg-renderer before 0.2.0-prerelease.20201019174008. The loadString function does not escape SVG properly, which can be used to inject arbitrary elements into the DOM via the _transformMeasurements function.	9.6	More Details
CVE-2020-18766	A cross-site scripting (XSS) vulnerability AntSword v2.0.7 can remotely execute system commands.	9.6	More Details
CVE-2020-15271	In lookatme (python/pypi package) versions prior to 2.3.0, the package automatically loaded the built-in "terminal" and "file_loader" extensions. Users that use lookatme to render untrusted markdown may have malicious shell commands automatically run on their system. This is fixed in version 2.3.0. As a workaround, the `lookatme/contrib/terminal.py` and `lookatme/contrib/file_loader.py` files may be manually deleted. Additionally, it is always recommended to be aware of what is being rendered with lookatme.	9.3	More Details
CVE-2020-14876	Vulnerability in the Oracle Trade Management 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 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14875	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 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2020-9868	A certificate validation issue existed when processing administrator added certificates. This issue was addressed with improved certificate validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An attacker may have been able to impersonate a trusted website using shared key material for an administrator added certificate.	9.1	More Details
CVE-2020-27195	HashiCorp Nomad and Nomad Enterprise version 0.9.0 up to 0.12.5 client file sandbox feature can be subverted using either the template or artifact stanzas. Fixed in 0.12.6, 0.11.5, and 0.10.6	9.1	More Details
CVE-2019-16127	Atmel Advanced Software Framework (ASF) 4 has an Integer Overflow.	9.1	More Details
CVE-2020-9906	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	9.1	More Details
CVE-2020-9920	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A malicious mail server may overwrite arbitrary mail files.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14805	Vulnerability in the Oracle E-Business Suite Secure Enterprise Search product of Oracle E-Business Suite (component: Search Integration Engine). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Suite Secure Enterprise Search. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Suite Secure Enterprise Search accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Suite Secure Enterprise Search accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-3456	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user.	8.8	More Details
CVE-2019-8696	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.	8.8	More Details
CVE-2019-8835	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13.3, iCloud for Windows 10.9, iOS 13.3 and iPadOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-24033	An issue was discovered in fs.com S3900 24T4S 1.7.0 and earlier. The form does not have an authentication or token authentication mechanism that allows remote attackers to forge requests on behalf of a site administrator to change all settings including deleting users, creating new users with escalated privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26878	Ruckus through 1.5.1.0.21 is affected by remote command injection. An authenticated user can submit a query to the API (/service/v1/createUser endpoint), injecting arbitrary commands that will be executed as root user via web.py.	8.8	More Details
CVE-2019-8751	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in Safari 13.0.1, iOS 13.1 and iPadOS 13.1, iCloud for Windows 10.7, iCloud for Windows 7.14, tvOS 13, watchOS 6, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8752	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in Safari 13.0.1, iOS 13.1 and iPadOS 13.1, iCloud for Windows 10.7, iCloud for Windows 7.14, tvOS 13, watchOS 6, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-7752	This affects the package systeminformation before 4.27.11. This package is vulnerable to Command Injection. The attacker can concatenate curl's parameters to overwrite Javascript files and then execute any OS commands.	8.8	More Details
CVE-2020-26561	Belkin LINKSYS WRT160NL 1.0.04.002_US_20130619 devices have a stack-based buffer overflow vulnerability because of sprintf in create_dir in mini_httpd. Successful exploitation leads to arbitrary code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2020-14862	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3 - 12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2019-8846	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 13.3, iCloud for Windows 10.9, iOS 13.3 and iPadOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-7125	A remote escalation of privilege vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8773	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in Safari 13.0.1, iOS 13.1 and iPadOS 13.1, iCloud for Windows 10.7, iCloud for Windows 7.14, tvOS 13, watchOS 6, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8825	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15, iOS 13, iCloud for Windows 10.7, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, iCloud for Windows 7.14, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8844	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13.3, watchOS 6.1.1, iCloud for Windows 10.9, iOS 13.3 and iPadOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8826	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8830	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 13.3, watchOS 6.1.1, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, iOS 13.3 and iPadOS 13.3, iOS 12.4.4, watchOS 5.3.4. Processing malicious video via FaceTime may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8728	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13, iCloud for Windows 7.14, iCloud for Windows 10.7, Safari 13, tvOS 13, watchOS 6, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8734	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13, iCloud for Windows 7.14, iCloud for Windows 10.7, Safari 13, tvOS 13, watchOS 6, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8675	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14735	Vulnerability in the Scheduler 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. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Scheduler executes to compromise Scheduler. While the vulnerability is in Scheduler, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Scheduler. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.8	More Details
CVE-2020-18129	A CSRF vulnerability in Eyoucms v1.2.7 allows an attacker to add an admin account via login.php.	8.8	More Details
CVE-2019-8638	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 5.2, iCloud for Windows 7.11, iOS 12.2, iTunes 12.9.4 for Windows, Safari 12.1. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2019-8639	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 5.2, iCloud for Windows 7.11, iOS 12.2, iTunes 12.9.4 for Windows, Safari 12.1. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-9932	A memory corruption issue was addressed with improved validation. This issue is fixed in Safari 13.0.1, iOS 13.1 and iPadOS 13.1, tvOS 13. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-5651	SQL injection vulnerability in Simple Download Monitor 3.8.8 and earlier allows remote attackers to execute arbitrary SQL commands via a specially crafted URL.	8.8	More Details
CVE-2019-8840	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 11.3. Compiling with untrusted sources may lead to arbitrary code execution with user privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11853	Arbitrary code execution vulnerability affecting multiple Micro Focus products. 1.) Operation Bridge Manager affecting version: 2020.05, 2019.11, 2019.05, 2018.11, 2018.05, versions 10.6x and 10.1x and older versions. 2.) Application Performance Management affecting versions : 9.51, 9.50 and 9.40 with uCMDB 10.33 CUP 3 3.) Data Center Automation affected version 2019.11 4.) Operations Bridge (containerized) affecting versions: 2019.11, 2019.08, 2019.05, 2018.11, 2018.08, 2018.05, 2018.02, 2017.11 5.) Universal CMDB affecting version: 2020.05, 2019.11, 2019.05, 2019.02, 2018.11, 2018.08, 2018.05, 11, 10.33, 10.32, 10.31, 10.30 6.) Hybrid Cloud Management affecting version 2020.05 7.) Service Management Automation affecting version 2020.5 and 2020.02. The vulnerability could allow to execute arbitrary code.	8.8	More Details
CVE-2018-11764	Web endpoint authentication check is broken in Apache Hadoop 3.0.0-alpha4, 3.0.0-beta1, and 3.0.0. Authenticated users may impersonate any user even if no proxy user is configured.	8.8	More Details
CVE-2020-15272	In the git-tag-annotation-action (open source GitHub Action) before version 1.0.1, an attacker can execute arbitrary (*) shell commands if they can control the value of [the `tag` input] or manage to alter the value of [the `GITHUB_REF` environment variable]. The problem has been patched in version 1.0.1. If you don't use the `tag` input you are most likely safe. The `GITHUB_REF` environment variable is protected by the GitHub Actions environment so attacks from there should be impossible. If you must use the `tag` input and cannot upgrade to `> 1.0.0` make sure that the value is not controlled by another Action.	8.7	More Details
CVE-2020-3562	A vulnerability in the SSL/TLS inspection of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series firewalls could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation for certain fields of specific SSL/TLS messages. An attacker could exploit this vulnerability by sending a malformed SSL/TLS message through an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. No manual intervention is needed to recover the device after it has reloaded.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3563	A vulnerability in the packet processing functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of TCP packets to a specific port on an affected device. A successful exploit could allow the attacker to exhaust system memory, which could cause the device to reload unexpectedly. No manual intervention is needed to recover the device after it has reloaded.	8.6	More Details
CVE-2020-3571	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload.	8.6	More Details
CVE-2020-3572	A vulnerability in the SSL/TLS session handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory leak when closing SSL/TLS connections in a specific state. An attacker could exploit this vulnerability by establishing several SSL/TLS sessions and ensuring they are closed under certain conditions. A successful exploit could allow the attacker to exhaust memory resources in the affected device, which would prevent it from processing new SSL/TLS connections, resulting in a DoS. Manual intervention is required to recover an affected device.	8.6	More Details
CVE-2020-3304	A vulnerability in the web interface of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, 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 an affected device. An exploit could allow the attacker to cause a DoS condition. Note: This vulnerability applies to IP Version 4 (IPv4) and IP Version 6 (IPv6) HTTP traffic.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14824	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, 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 Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 8.6 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).	8.6	More Details
CVE-2020-3499	A vulnerability in the licensing service of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.The vulnerability is due to improper handling of system resource values by the affected system. An attacker could exploit this vulnerability by sending malicious requests to the targeted system. A successful exploit could allow the attacker to cause the affected system to become unresponsive, resulting in a DoS condition and preventing the management of dependent devices.	8.6	More Details
CVE-2020-3373	A vulnerability in the IP fragment-handling implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device. This memory leak could prevent traffic from being processed through the device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper error handling when specific failures occur during IP fragment reassembly. An attacker could exploit this vulnerability by sending crafted, fragmented IP traffic to a targeted device. A successful exploit could allow the attacker to continuously consume memory on the affected device and eventually impact traffic, resulting in a DoS condition. The device could require a manual reboot to recover from the DoS condition. Note: This vulnerability applies to both IP Version 4 (IPv4) and IP Version 6 (IPv6) traffic.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3528	A vulnerability in the OSPF Version 2 (OSPFv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation when the affected software processes certain OSPFv2 packets with Link-Local Signaling (LLS) data. An attacker could exploit this vulnerability by sending a malformed OSPFv2 packet to an affected device. A successful exploit could allow the attacker to cause an affected device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2020-3436	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to upload arbitrary-sized files to specific folders on an affected device, which could lead to an unexpected device reload. The vulnerability exists because the affected software does not efficiently handle the writing of large files to specific folders on the local file system. An attacker could exploit this vulnerability by uploading files to those specific folders. A successful exploit could allow the attacker to write a file that triggers a watchdog timeout, which would cause the device to unexpectedly reload, causing a denial of service (DoS) condition.	8.6	More Details
CVE-2020-3529	A vulnerability in the SSL VPN negotiation process for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to inefficient direct memory access (DMA) memory management during the negotiation phase of an SSL VPN connection. An attacker could exploit this vulnerability by sending a steady stream of crafted Datagram TLS (DTLS) traffic to an affected device. A successful exploit could allow the attacker to exhaust DMA memory on the device and cause a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3533	A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to restart unexpectedly. The vulnerability is due to a lack of sufficient memory management protections under heavy SNMP polling loads. An attacker could exploit this vulnerability by sending a high rate of SNMP requests to the SNMP daemon through the management interface on an affected device. A successful exploit could allow the attacker to cause the SNMP daemon process to consume a large amount of system memory over time, which could then lead to an unexpected device restart, causing a denial of service (DoS) condition. This vulnerability affects all versions of SNMP.	8.6	More Details
CVE-2020-14879	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). 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 low privileged attacker with network access via HTTP to compromise BI Publisher. While the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	8.5	More Details
CVE-2020-14880	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). 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 low privileged attacker with network access via HTTP to compromise BI Publisher. While the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	8.5	More Details
CVE-2020-27613	The installation procedure in BigBlueButton before 2.2.28 (or earlier) uses ClueCon as the FreeSWITCH password, which allows local users to achieve unintended FreeSWITCH access.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14850	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Flex Fields). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14857	Vulnerability in the Oracle Trade Management 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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14856	Vulnerability in the Oracle Trade Management 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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/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-2020-14815	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 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 Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, 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 Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14816	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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14817	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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/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-2020-14851	Vulnerability in the Oracle Trade Management 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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14819	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). The supported version that is affected is 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14808	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/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-2020-14863	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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14849	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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-3514	A vulnerability in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their Cisco FTD instance and execute commands with root privileges in the host namespace. The attacker must have valid credentials on the device.The vulnerability exists because a configuration file that is used at container startup has insufficient protections. An attacker could exploit this vulnerability by modifying a specific container configuration file on the underlying file system. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running Cisco FTD instances or the host Cisco FXOS device.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26896	Prior to 0.11.0-beta, LND (Lightning Network Daemon) had a vulnerability in its invoice database. While claiming on-chain a received HTLC output, it didn't verify that the corresponding outgoing off-chain HTLC was already settled before releasing the preimage. In the case of a hash-and-amount collision with an invoice, the preimage for an expected payment was instead released. A malicious peer could have deliberately intercepted an HTLC intended for the victim node, probed the preimage through a colluding relayed HTLC, and stolen the intercepted HTLC. The impact is a loss of funds in certain situations, and a weakening of the victim's receiver privacy.	8.2	More Details
CVE-2020-14831	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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14833	Vulnerability in the Oracle Trade Management 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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/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-2020-14834	Vulnerability in the Oracle Trade Management 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 - 12.2.10. 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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14835	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 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-27890	The Zigbee protocol implementation on Texas Instruments CC2538 devices with Z-Stack 3.0.1 does not properly process a ZCL Write Attributes No Response message. It crashes in zclParseInWriteCmd() and does not update the specific attribute's value.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14842	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2020-14872	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2020-14784	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Mobile Service). Supported versions that are affected are 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, 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 BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/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-2020-14865	Vulnerability in the PeopleSoft Enterprise SCM eSupplier Connection product of Oracle PeopleSoft (component: eSupplier Connection). 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 eSupplier Connection. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise SCM eSupplier Connection accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise SCM eSupplier Connection accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2020-3410	A vulnerability in the Common Access Card (CAC) authentication feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass authentication and access the FMC system. The attacker must have a valid CAC to initiate the access attempt. The vulnerability is due to incorrect session invalidation during CAC authentication. An attacker could exploit this vulnerability by performing a CAC-based authentication attempt to an affected system. A successful exploit could allow the attacker to access an affected system with the privileges of a CAC-authenticated user who is currently logged in.	8.1	More Details
CVE-2020-26649	AtomXCMS 2.0 is affected by Incorrect Access Control via admin/dump.php	8.1	More Details
CVE-2020-3549	A vulnerability in the sftunnel functionality of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to obtain the device registration hash. The vulnerability is due to insufficient sftunnel negotiation protection during initial device registration. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a specific flow of the sftunnel communication between an FMC device and an FTD device. A successful exploit could allow the attacker to decrypt and modify the sftunnel communication between FMC and FTD devices, allowing the attacker to modify configuration data sent from an FMC device to an FTD device or alert data sent from an FTD device to an FMC device.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14734	Vulnerability in the Oracle Text 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 unauthenticated attacker with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2020-3550	A vulnerability in the sfmgr daemon of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to perform directory traversal and access directories outside the restricted path. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by using a relative path in specific sfmgr commands. An exploit could allow the attacker to read or write arbitrary files on an sftunnel-connected peer device.	8.1	More Details
CVE-2020-15244	In Magento (rubygems openmage/magento-lts package) before versions 19.4.8 and 20.0.4, an admin user can generate soap credentials that can be used to trigger RCE via PHP Object Injection through product attributes and a product. The issue is patched in versions 19.4.8 and 20.0.4.	8.0	More Details
CVE-2020-14878	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.0	More Details
CVE-2020-5990	NVIDIA GeForce Experience, all versions prior to 3.20.5.70, contains a vulnerability in the ShadowPlay component which may lead to local privilege escalation, code execution, denial of service or information disclosure.	7.8	More Details
CVE-2020-9749	Adobe Animate version 20.5 (and earlier) is affected by an out-of-bounds read vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24848	FruityWifi through 2.4 has an unsafe Sudo configuration [(ALL : ALL) NOPASSWD: ALL]. This allows an attacker to perform a system-level (root) local privilege escalation, allowing an attacker to gain complete persistent access to the local system.	7.8	More Details
CVE-2019-6238	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. Processing a maliciously crafted package may lead to arbitrary code execution.	7.8	More Details
CVE-2019-14717	Verifone Verix OS on VerixV Pinpad Payment Terminals with QT000530 have a Buffer Overflow via the Run system call.	7.8	More Details
CVE-2020-3915	A path handling issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to overwrite arbitrary files.	7.8	More Details
CVE-2019-8592	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15, tvOS 12.3, watchOS 5.2.1, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, iOS 12.3, iOS 13. Playing a malicious audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-3455	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots.	7.8	More Details
CVE-2020-3898	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2019-14719	Verifone MX900 series Pinpad Payment Terminals with OS 30251000 allow multiple arbitrary command injections, as demonstrated by the file manager.	7.8	More Details
CVE-2020-9853	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to determine kernel memory layout.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4452	A memory consumption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.3, Security Update 2019-001 High Sierra, Security Update 2019-001 Sierra, macOS Mojave 10.14.2, Security Update 2018-003 High Sierra, Security Update 2018-006 Sierra. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-9748	Adobe Animate version 20.5 (and earlier) is affected by a stack overflow vulnerability, which could lead to arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate.	7.8	More Details
CVE-2018-4451	This issue is fixed in macOS Mojave 10.14. A memory corruption issue was addressed with improved input validation.	7.8	More Details
CVE-2020-24418	Adobe After Effects version 17.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .aepx file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2020-5977	NVIDIA GeForce Experience, all versions prior to 3.20.5.70, contains a vulnerability in NVIDIA Web Helper NodeJS Web Server in which an uncontrolled search path is used to load a node module, which may lead to code execution, denial of service, escalation of privileges, and information disclosure.	7.8	More Details
CVE-2020-9747	Adobe Animate version 20.5 (and earlier) is affected by a double free vulnerability when parsing a crafted .fla file, which could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	7.8	More Details
CVE-2019-8509	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15. A malicious application may be able to elevate privileges.	7.8	More Details
CVE-2019-8579	An input validation issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2020-26887	FRITZ!OS before 7.21 on FRITZ!Box devices allows a bypass of a DNS Rebinding protection mechanism.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9750	Adobe Animate version 20.5 (and earlier) is affected by an out-of-bounds read vulnerability, which could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate.	7.8	More Details
CVE-2020-5978	NVIDIA GeForce Experience, all versions prior to 3.20.5.70, contains a vulnerability in its services in which a folder is created by nvcontainer.exe under normal user login with LOCAL_SYSTEM privileges which may lead to a denial of service or escalation of privileges.	7.8	More Details
CVE-2020-9331	CryptoPro CSP through 5.0.0.10004 on 32-bit platforms allows Local Privilege Escalation (by local users with the SeChangeNotifyPrivilege right) because user-mode input is mishandled during process creation. An attacker can write arbitrary data to an arbitrary location in the kernel's address space.	7.8	More Details
CVE-2019-8539	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-23864	An issue exits in IOBit Malware Fighter version 8.0.2.547. Local escalation of privileges is possible by dropping a malicious DLL file into the WindowsApps folder.	7.8	More Details
CVE-2020-6023	Check Point ZoneAlarm before version 15.8.139.18543 allows a local actor to escalate privileges while restoring files in Anti-Ransomware.	7.8	More Details
CVE-2020-11858	Code execution with escalated privileges vulnerability in Micro Focus products Operation Bridge Manager and Operation Bridge (containerized). The vulneravility affects: 1.) Operation Bridge Manager versions: 2020.05, 2019.11, 2019.05, 2018.11, 2018.05, 10.63,10.62, 10.61, 10.60, 10.12, 10.11, 10.10 and all earlier versions. 2.) Operations Bridge (containerized) versions: 2020.05, 2019.08, 2019.05, 2018.11, 2018.08, 2018.05. 2018.02 and 2017.11. The vulnerability could allow local attackers to execute code with escalated privileges.	7.8	More Details
CVE-2020-27187	An issue was discovered in KDE Partition Manager 4.1.0 before 4.2.0. The kpmcore_externalcommand helper contains a logic flaw in which the service invoking D-Bus is not properly checked. An attacker on the local machine can replace /etc/fstab, and execute mount and other partitioning related commands, while KDE Partition Manager is running. the mount command can then be used to gain full root privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4467	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.3, Security Update 2019-001 High Sierra, Security Update 2019-001 Sierra, macOS Mojave 10.14.2, Security Update 2018-003 High Sierra, Security Update 2018-006 Sierra. A malicious application may be able to elevate privileges.	7.8	More Details
CVE-2020-9873	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2019-8838	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3 and iPadOS 13.3, watchOS 6.1.1, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, tvOS 13.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9927	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8832	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3 and iPadOS 13.3, watchOS 6.1.1, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, tvOS 13.3. An application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2019-8833	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.3 and iPadOS 13.3, watchOS 6.1.1, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, tvOS 13.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8836	A memory corruption issue was addressed with improved memory handling. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9961	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8837	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. A malicious application may be able to access restricted files.	7.8	More Details
CVE-2019-14712	Verifone VerixV Pinpad Payment Terminals with QT000530 allow bypass of integrity and origin control for S1G file generation.	7.8	More Details
CVE-2020-9854	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2020-9901	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2020-9904	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8841	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.3 and iPadOS 13.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9919	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-3880	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2019-8847	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9928	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8829	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6.1, tvOS 13.2, iOS 13.2 and iPadOS 13.2. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8848	This issue was addressed with improved checks. This issue is fixed in tvOS 13.3, watchOS 6.1.1, iCloud for Windows 10.9, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, iOS 13.3 and iPadOS 13.3, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2019-8852	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9937	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9938	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-3864	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin.	7.8	More Details
CVE-2020-9940	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9980	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9984	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-3863	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. An application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-9985	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-27671	An issue was discovered in Xen through 4.14.x allowing x86 HVM and PVH guest OS users to cause a denial of service (data corruption), cause a data leak, or possibly gain privileges because coalescing of per-page IOMMU TLB flushes is mishandled.	7.8	More Details
CVE-2020-9990	A race condition was addressed with additional validation. This issue is fixed in macOS Catalina 10.15.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-3851	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2020-10721	A flaw was found in the fabric8-maven-plugin 4.0.0 and later. When using a wildfly-swarm or thorntail custom configuration, a malicious YAML configuration file on the local machine executing the maven plug-in could allow for deserialization of untrusted data resulting in arbitrary code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8831	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15, iOS 13.1 and iPadOS 13.1, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6. An application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2019-8828	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3 and iPadOS 13.3, watchOS 6.1.1, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, tvOS 13.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9880	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-9863	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9871	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9872	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-3459	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10138	Acronis Cyber Backup 12.5 and Cyber Protect 15 include an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis Cyber Backup and Cyber Protect contain a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges.	7.8	More Details
CVE-2020-9874	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9875	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9876	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2019-8706	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15, iOS 13.1 and iPadOS 13.1, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2019-8709	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6, iOS 13. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8715	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15, iOS 13. An application may be able to execute arbitrary code with system privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8718	A memory corruption issue was addressed with improved memory handling. This issue is fixed in watchOS 6, iOS 13, tvOS 13. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9877	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9879	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2019-8740	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in iOS 13.1 and iPadOS 13.1, watchOS 6, tvOS 13. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2019-8824	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9881	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-9882	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-9883	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10139	Acronis True Image 2021 includes an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis True Image contains a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges.	7.8	More Details
CVE-2020-9887	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. Viewing a maliciously crafted JPEG file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9892	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-9899	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-9900	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2020-10140	Acronis True Image 2021 fails to properly set ACLs of the C:\ProgramData\Acronis directory. Because some privileged processes are executed from the C:\ProgramData\Acronis, an unprivileged user can achieve arbitrary code execution with SYSTEM privileges by placing a DLL in one of several paths within C:\ProgramData\Acronis.	7.8	More Details
CVE-2020-9973	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2019-8776	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-27670	An issue was discovered in Xen through 4.14.x allowing x86 guest OS users to cause a denial of service (data corruption), cause a data leak, or possibly gain privileges because an AMD IOMMU page-table entry can be half-updated.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1915	An out-of-bounds read in the JavaScript Interpreter in Facebook Hermes prior to commit 8cb935cd3b2321c46aa6b7ed8454d95c75a7fca0 allows attackers to cause a denial of service attack or possible further memory corruption via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	7.5	More Details
CVE-2019-17007	In Network Security Services before 3.44, a malformed Netscape Certificate Sequence can cause NSS to crash, resulting in a denial of service.	7.5	More Details
CVE-2020-25186	An XXE vulnerability exists within LeviStudioU Release Build 2019-09-21 and prior when processing parameter entities, which may allow file disclosure.	7.5	More Details
CVE-2020-9828	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A remote attacker may be able to leak sensitive user information.	7.5	More Details
CVE-2020-3554	A vulnerability in the TCP packet processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory exhaustion condition. An attacker could exploit this vulnerability by sending a high rate of crafted TCP traffic through an affected device. A successful exploit could allow the attacker to exhaust device resources, resulting in a DoS condition for traffic transiting the affected device.	7.5	More Details
CVE-2020-26566	A Denial of Service condition in Motion-Project Motion 3.2 through 4.3.1 allows remote unauthenticated users to cause a webu.c segmentation fault and kill the main process via a crafted HTTP request.	7.5	More Details
CVE-2020-9924	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6. A remote attacker may be able to cause a denial of service.	7.5	More Details
CVE-2020-15897	Arista EOS before 4.21.12M, 4.22.x before 4.22.7M, 4.23.x before 4.23.5M, and 4.24.x before 4.24.2F allows remote attackers to cause traffic loss or incorrect forwarding of traffic via a malformed link-state PDU to the IS-IS router.	7.5	More Details
CVE-2020-13100	Arista's CloudVision eXchange (CVX) server before 4.21.12M, 4.22.x before 4.22.7M, 4.23.x before 4.23.5M, and 4.24.x before 4.24.2F allows remote attackers to cause a denial of service (crash and restart) in the ControllerOob agent via a malformed control-plane packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9905	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A remote attacker may be able to cause a denial of service.	7.5	More Details
CVE-2020-27665	In Strapi before 3.2.5, there is no admin::hasPermissions restriction for CTB (aka content-type-builder) routes.	7.5	More Details
CVE-2020-24425	Dreamweaver version 20.2 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. Successful exploitation could result in a local user with permissions to write to the file system running system commands with administrator privileges.	7.5	More Details
CVE-2020-17355	Arista EOS before 4.21.12M, 4.22.x before 4.22.7M, 4.23.x before 4.23.5M, and 4.24.x before 4.24.2F allows remote attackers to cause a denial of service (restart of agents) by crafting a malformed DHCP packet which leads to an incorrect route being installed.	7.5	More Details
CVE-2020-27638	receive.c in fastd before v21 allows denial of service (assertion failure) when receiving packets with an invalid type code.	7.5	More Details
CVE-2020-27155	An issue was discovered in Octopus Deploy through 2020.4.4. If enabled, the websocket endpoint may allow an untrusted tentacle host to present itself as a trusted one.	7.5	More Details
CVE-2020-9869	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. A remote attacker may cause an unexpected application termination.	7.5	More Details
CVE-2020-15681	When multiple WASM threads had a reference to a module, and were looking up exported functions, one WASM thread could have overwritten another's entry in a shared stub table, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 82.	7.5	More Details
CVE-2019-8851	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. A Mac may not lock immediately upon wake.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14820	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, 12.2.1.4.0 and 14.1.1.0.0. 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 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2020-27888	An issue was discovered on Ubiquiti UniFi Meshing Access Point UAP-AC-M 4.3.21.11325 and UniFi Controller 6.0.28 devices. Cached credentials are not erased from an access point returning wirelessly from a disconnected state. This may provide unintended network access.	7.5	More Details
CVE-2019-8854	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in macOS Catalina 10.15, watchOS 6, iOS 13, tvOS 13. A device may be passively tracked by its Wi-Fi MAC address.	7.5	More Details
CVE-2019-8580	Source-routed IPv4 packets were disabled by default. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. Source-routed IPv4 packets may be unexpectedly accepted.	7.5	More Details
CVE-2020-7755	All versions of package dat.gui are vulnerable to Regular Expression Denial of Service (ReDoS) via specifically crafted rgb and rgba values.	7.5	More Details
CVE-2019-8640	A logic issue was addressed with improved validation. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra. A sandboxed process may be able to circumvent sandbox restrictions.	7.5	More Details
CVE-2020-27891	The Zigbee protocol implementation on Texas Instruments CC2538 devices with Z-Stack 3.0.1 does not properly process a ZCL Read Reporting Configuration Response message. It crashes in zclHandleExternal().	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14774	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 and 12.2.3 - 12.2.10. 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle CRM Technical Foundation. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2020-27892	The Zigbee protocol implementation on Texas Instruments CC2538 devices with Z-Stack 3.0.1 does not properly process a ZCL Discover Commands Received Response message or a ZCL Discover Commands Generated Response message. It crashes in zclParseInDiscCmdsRspCmd().	7.5	More Details
CVE-2020-7754	This affects the package npm-user-validate before 1.0.1. The regex that validates user emails took exponentially longer to process long input strings beginning with @ characters.	7.5	More Details
CVE-2020-23945	A SQL injection vulnerability exists in Victor CMS V1.0 in the cat_id parameter of the category.php file. This parameter can be used by sqlmap to obtain data information in the database.	7.5	More Details
CVE-2019-8633	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, iOS 12.3, tvOS 12.3, watchOS 5.3. An application may be able to read restricted memory.	7.5	More Details
CVE-2020-8579	Clustered Data ONTAP versions 9.7 through 9.7P7 are susceptible to a vulnerability which allows an attacker with access to an intercluster LIF to cause a Denial of Service (DoS).	7.5	More Details
CVE-2020-27603	BigBlueButton before 2.2.27 has an unsafe JODConverter setting in which LibreOffice document conversions can access external files.	7.5	More Details
CVE-2019-8618	A logic issue was addressed with improved restrictions. This issue is fixed in watchOS 5.2, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.2. A sandboxed process may be able to circumvent sandbox restrictions.	7.5	More Details
CVE-2019-8631	A logic issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, iOS 12.3, tvOS 12.3. Users removed from an iMessage conversation may still be able to alter state.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9774	An issue existed with Siri Suggestions access to encrypted data. The issue was fixed by limiting access to encrypted data. This issue is fixed in macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Encrypted data may be inappropriately accessed.	7.5	More Details
CVE-2019-8575	The issue was addressed with improved data deletion. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. A base station factory reset may not delete all user information.	7.5	More Details
CVE-2020-7753	All versions of package trim are vulnerable to Regular Expression Denial of Service (ReDoS) via trim().	7.5	More Details
CVE-2020-27610	The installation procedure in BigBlueButton before 2.2.28 (or earlier) exposes certain network services to external interfaces, and does not automatically set up a firewall configuration to block external access.	7.5	More Details
CVE-2018-4474	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iCloud for Windows 7.7, watchOS 5, Safari 12, iOS 12, iTunes 12.9 for Windows, tvOS 12. Unexpected interaction causes an ASSERT failure.	7.5	More Details
CVE-2020-9782	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. A remote attacker may be able to overwrite existing files.	7.5	More Details
CVE-2020-9941	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. A remote attacker may be able to unexpectedly alter application state.	7.5	More Details
CVE-2019-8573	An input validation issue was addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, iOS 12.3, watchOS 5.2.1. A remote attacker may be able to cause a system denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14864	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Installation). Supported versions that are affected are 5.5.0.0.0, 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 Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2020-27180	konzept-ix publiXone before 2020.015 allows attackers to download files by iterating over the IXCopy fileID parameter.	7.5	More Details
CVE-2020-3317	A vulnerability in the ssl_inspection component of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to crash Snort instances. The vulnerability is due to insufficient input validation in the ssl_inspection component. An attacker could exploit this vulnerability by sending a malformed TLS packet through a Cisco Adaptive Security Appliance (ASA). A successful exploit could allow the attacker to crash a Snort instance, resulting in a denial of service (DoS) condition.	7.5	More Details
CVE-2019-8564	A logic issue was addressed with improved validation. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. An attacker in a privileged network position can modify driver state.	7.5	More Details
CVE-2019-8588	A null pointer dereference was addressed with improved input validation. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. A remote attacker may be able to cause a system denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3577	A vulnerability in the ingress packet processing path of Cisco Firepower Threat Defense (FTD) Software for interfaces that are configured either as Inline Pair or in Passive mode could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation when Ethernet frames are processed. An attacker could exploit this vulnerability by sending malicious Ethernet frames through an affected device. A successful exploit could allow the attacker do either of the following: Fill the /ngfw partition on the device: A full /ngfw partition could result in administrators being unable to log in to the device (including logging in through the console port) or the device being unable to boot up correctly. Note: Manual intervention is required to recover from this situation. Customers are advised to contact the Cisco Technical Assistance Center (TAC) to help recover a device in this condition. Cause a process crash: The process crash would cause the device to reload. No manual intervention is necessary to recover the device after the reload.	7.4	More Details
CVE-2020-15240	omniauth-auth0 (rubygems) versions >= 2.3.0 and < 2.4.1 improperly validate the JWT token signature when using the `jwt_validator.verify` method. Improper validation of the JWT token signature can allow an attacker to bypass authentication and authorization. You are affected by this vulnerability if all of the following conditions apply: 1. You are using `omniauth-auth0`. 2. You are using `JWTValidator.verify` method directly OR you are not authenticating using the SDK's default Authorization Code Flow. The issue is patched in version 2.4.1.	7.4	More Details
CVE-2020-27611	BigBlueButton through 2.2.28 uses STUN/TURN resources from a third party, which may represent an unintended endpoint.	7.3	More Details
CVE-2020-17381	An issue was discovered in Ghisler Total Commander 9.51. Due to insufficient access restrictions in the default installation directory, an attacker can elevate privileges by replacing the %SYSTEMDRIVE%\totalcmd\TOTALCMD64.EXE binary.	7.3	More Details
CVE-2020-14828	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 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 takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2020-24631	A remote execution of arbitrary commands vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24632	A remote execution of arbitrary commandss vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	7.2	More Details
CVE-2020-14883	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, 12.2.1.4.0 and 14.1.1.0.0. 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 takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2020-15352	An XML external entity (XXE) vulnerability in Pulse Connect Secure (PCS) before 9.1R9 and Pulse Policy Secure (PPS) before 9.1R9 allows remote authenticated admins to conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request.	7.2	More Details
CVE-2020-9771	This issue was addressed with a new entitlement. This issue is fixed in macOS Catalina 10.15.4. A user may gain access to protected parts of the file system.	7.1	More Details
CVE-2020-9779	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	7.1	More Details
CVE-2020-14807	Vulnerability in the Oracle Hospitality Suite8 product of Oracle Hospitality Applications (component: WebConnect). Supported versions that are affected are 8.10.2 and 8.11-8.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Suite8 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8759	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15. A local user may be able to cause unexpected system termination or read kernel memory.	7.1	More Details
CVE-2020-14780	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	7.1	More Details
CVE-2020-14843	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 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 Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L).	7.1	More Details
CVE-2020-9929	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to cause unexpected system termination or read kernel memory.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14766	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Administration). 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 low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	7.1	More Details
CVE-2020-3855	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. A malicious application may be able to overwrite arbitrary files.	7.1	More Details
CVE-2020-9994	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to overwrite arbitrary files.	7.1	More Details
CVE-2020-15238	Blueman is a GTK+ Bluetooth Manager. In Blueman before 2.1.4, the DhcpClient method of the D-Bus interface to blueman-mechanism is prone to an argument injection vulnerability. The impact highly depends on the system configuration. If Polkit-1 is disabled and for versions lower than 2.0.6, any local user can possibly exploit this. If Polkit-1 is enabled for version 2.0.6 and later, a possible attacker needs to be allowed to use the `org.blueman.dhcp.client` action. That is limited to users in the wheel group in the shipped rules file that do have the privileges anyway. On systems with ISC DHCP client (dhclient), attackers can pass arguments to `ip link` with the interface name that can e.g. be used to bring down an interface or add an arbitrary XDP/BPF program. On systems with dhcpcd and without ISC DHCP client, attackers can even run arbitrary scripts by passing `-c/path/to/script` as an interface name. Patches are included in 2.1.4 and master that change the DhcpClient D-Bus method(s) to accept BlueZ network object paths instead of network interface names. A backport to 2.0(.8) is also available. As a workaround, make sure that Polkit-1-support is enabled and limit privileges for the `org.blueman.dhcp.client` action to users that are able to run arbitrary commands as root anyway in /usr/share/polkit-1/rules.d/blueman.rules.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4428	A lock screen issue allowed access to the share function on a locked device. This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 12.1.1. A local attacker may be able to share items from the lock screen.	7.1	More Details
CVE-2020-9908	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to cause unexpected system termination or read kernel memory.	7.1	More Details
CVE-2019-14711	Verifone MX900 series Pinpad Payment Terminals with OS 30251000 have a race condition for RBAC bypass.	7.0	More Details
CVE-2020-9796	A race condition was addressed with improved state handling. This issue is fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges.	7.0	More Details
CVE-2020-24422	Adobe Creative Cloud Desktop Application version 5.2 (and earlier) and 2.1 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-24424	Adobe Premiere Pro version 14.4 (and earlier) is affected by an uncontrolled search path element that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-27672	An issue was discovered in Xen through 4.14.x allowing x86 guest OS users to cause a host OS denial of service, achieve data corruption, or possibly gain privileges by exploiting a race condition that leads to a use-after-free involving 2MiB and 1GiB superpages.	7.0	More Details
CVE-2020-9921	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. A malicious application may be able to execute arbitrary code with system privileges.	7.0	More Details
CVE-2020-24419	Adobe After Effects version 17.1.1 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24420	Adobe Photoshop for Windows version 21.2.1 (and earlier) is affected by an uncontrolled search path element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-27216	In Eclipse Jetty versions 1.0 thru 9.4.32.v20200930, 10.0.0.alpha1 thru 10.0.0.beta2, and 11.0.0.alpha1 thru 11.0.0.beta2O, on Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory. If the attacker wins the race then they will have read and write permission to the subdirectory used to unpack web applications, including their WEB-INF/lib jar files and JSP files. If any code is ever executed out of this temporary directory, this can lead to a local privilege escalation vulnerability.	7.0	More Details
CVE-2020-24423	Adobe Media Encoder version 14.4 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-14858	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Logging). Supported versions that are affected are 5.5 and 5.6. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 6.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.8	More Details
CVE-2019-16129	Microchip CryptoAuthentication Library CryptoAuthLib prior to 20191122 has a Buffer Overflow (issue 2 of 2).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14757	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). The supported version that is affected is 12.2.1.3.0. Difficult to exploit 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 creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).	6.8	More Details
CVE-2019-16128	Microchip CryptoAuthentication Library CryptoAuthLib prior to 20191122 has a Buffer Overflow (issue 1 of 2).	6.8	More Details
CVE-2020-3555	A vulnerability in the SIP inspection process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a crash and reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a watchdog timeout and crash during the cleanup of threads that are associated with a SIP connection that is being deleted from the connection list. An attacker could exploit this vulnerability by sending a high rate of crafted SIP traffic through an affected device. A successful exploit could allow the attacker to cause a watchdog timeout and crash, resulting in a crash and reload of the affected device.	6.8	More Details
CVE-2019-14715	Verifone Pinpad Payment Terminals allow undocumented physical access to the system via an SBI bootloader memory write operation.	6.8	More Details
CVE-2020-9810	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.5. A person with physical access to a Mac may be able to bypass Login Window.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3458	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots.	6.7	More Details
CVE-2019-8525	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, watchOS 5.2, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.2. An application may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2019-14718	Verifone MX900 series Pinpad Payment Terminals with OS 30251000 have Insecure Permissions, with resultant svc_netcontrol arbitrary command injection and privilege escalation.	6.7	More Details
CVE-2019-8528	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 5.2, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.2. An application may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2019-8534	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. A malicious application may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2019-8569	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. An application may be able to execute arbitrary code with system privileges.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3457	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	6.7	More Details
CVE-2019-14716	Verifone VerixV Pinpad Payment Terminals with QT000530 have an undocumented physical access mode (aka VerixV shell.out).	6.6	More Details
CVE-2020-27607	In BigBlueButton before 2.2.28 (or earlier), the client-side Mute button only signifies that the server should stop accepting audio data from the client. It does not directly configure the client to stop sending audio data to the server, and thus a modified server could store the audio data and/or transmit it to one or more meeting participants or other third parties.	6.5	More Details
CVE-2020-27604	BigBlueButton before 2.3 does not implement LibreOffice sandboxing. This might make it easier for remote authenticated users to read the API shared secret in the bigbluebutton.properties file. With the API shared secret, an attacker can (for example) use api/join to join an arbitrary meeting regardless of its guestPolicy setting.	6.5	More Details
CVE-2020-25820	BigBlueButton before 2.2.7 allows remote authenticated users to read local files and conduct SSRF attacks via an uploaded Office document that has a crafted URL in an ODF xlink field.	6.5	More Details
CVE-2020-27181	A hardcoded AES key in CipherUtils.java in the Java applet of konzept-ix publiXone before 2020.015 allows attackers to craft password-reset tokens or decrypt server-side configuration files.	6.5	More Details
CVE-2019-8664	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, watchOS 5.2.1. Processing a maliciously crafted message may lead to a denial of service.	6.5	More Details
CVE-2019-7291	A denial of service issue was addressed with improved memory handling. This issue is fixed in AirPort Base Station Firmware Update 7.8.1, AirPort Base Station Firmware Update 7.9.1. An attacker in a privileged position may be able to perform a denial of service attack.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14769	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2020-25034	eMPS prior to eMPS 9.0 FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection attacks via the sort, sort_by, search{URL], or search[attachment] parameter to the email search feature.	6.5	More Details
CVE-2020-14887	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3.0 and 14.0.0-14.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2020-14765	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14890	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.1, 12.0.2 and 12.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2018-4444	A logic issue was addressed with improved state management. This issue is fixed in Safari 12.0.2, iOS 12.1.1, tvOS 12.1.1, iTunes 12.9.2 for Windows. Processing maliciously crafted web content may disclose sensitive user information.	6.5	More Details
CVE-2020-14761	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Oracle Diagnostics Interfaces). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2019-8901	This issue was addressed by verifying host keys when connecting to a previously-known SSH server. This issue is fixed in iOS 13.1 and iPadOS 13.1. An attacker in a privileged network position may be able to intercept SSH traffic from the “Run script over SSH” action.	6.5	More Details
CVE-2018-18508	In Network Security Services (NSS) before 3.36.7 and before 3.41.1, a malformed signature can cause a crash due to a null dereference, resulting in a Denial of Service.	6.5	More Details
CVE-2020-7196	The HPE BlueData EPIC Software Platform version 4.0 and HPE Ezmeral Container Platform 5.0 use an insecure method of handling sensitive Kerberos passwords that is susceptible to unauthorized interception and/or retrieval. Specifically, they display the kdc_admin_password in the source file of the url "/bdswebui/assignusers/".	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14896	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Core). Supported versions that are affected are 14.1.0-14.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Payments accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2020-15682	When a link to an external protocol was clicked, a prompt was presented that allowed the user to choose what application to open it in. An attacker could induce that prompt to be associated with an origin they didn't control, resulting in a spoofing attack. This was fixed by changing external protocol prompts to be tab-modal while also ensuring they could not be incorrectly associated with a different origin. This vulnerability affects Firefox < 82.	6.5	More Details
CVE-2020-14744	Vulnerability in the Oracle REST Data Services product of Oracle REST Data Services (component: General). Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c; Standalone ORDS: prior to 20.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle REST Data Services accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2020-14894	Vulnerability in the Oracle Banking Corporate Lending product of Oracle Financial Services Applications (component: Core). Supported versions that are affected are 12.3.0 and 14.0.0-14.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14877	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Logging). Supported versions that are affected are 5.5 and 5.6. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality OPERA 5 Property Services accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2020-14775	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2020-14800	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2020-14836	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14830	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2019-8612	A logic issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, tvOS 12.3, watchOS 5.2.1, macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, iOS 12.3. An attacker in a privileged network position can modify driver state.	6.5	More Details
CVE-2020-14846	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2020-14827	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2019-8645	An issue existed in the handling of encrypted Mail. This issue was addressed with improved isolation of MIME in Mail. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. An attacker in a privileged network position may be able to intercept the contents of S/MIME-encrypted e-mail.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14823	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.2.3 - 12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Technical Foundation accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2019-8736	An input validation issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15. An attacker in a privileged network position may be able to leak sensitive user information.	6.5	More Details
CVE-2020-27646	Biscom Secure File Transfer (SFT) before 5.1.1082 and 6.x before 6.0.1011 allows user credential theft.	6.5	More Details
CVE-2019-8737	A denial of service issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15. An attacker in a privileged position may be able to perform a denial of service attack.	6.5	More Details
CVE-2019-8754	A cross-origin issue existed with "iframe" elements. This was addressed with improved tracking of security origins. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006. A malicious HTML document may be able to render iframes with sensitive user information.	6.5	More Details
CVE-2019-8570	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.1.3, iCloud for Windows 7.10, iTunes 12.9.3 for Windows, Safari 12.0.3, tvOS 12.1.2. Processing maliciously crafted web content may disclose sensitive user information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14795	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2020-3998	VMware Horizon Client for Windows (5.x prior to 5.5.0) contains an information disclosure vulnerability. A malicious attacker with local privileges on the machine where Horizon Client for Windows is installed may be able to retrieve hashed credentials if the client crashes.	6.5	More Details
CVE-2020-14897	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.1, 12.0.2 and 12.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2020-9939	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to load unsigned kernel extensions.	6.4	More Details
CVE-2020-14778	Vulnerability in the PeopleSoft Enterprise HCM Global Payroll Core product of Oracle PeopleSoft (component: Security). 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 Global Payroll Core. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Global Payroll Core accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Global Payroll Core accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise HCM Global Payroll Core. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/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-2019-8855	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to access restricted files.	6.3	More Details
CVE-2019-8753	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15, watchOS 6, iOS 13, tvOS 13. Processing maliciously crafted web content may lead to a cross site scripting attack.	6.1	More Details
CVE-2020-26161	In Octopus Deploy through 2020.4.2, an attacker could redirect users to an external site via a modified HTTP Host header.	6.1	More Details
CVE-2020-25470	AntSword 2.1.8.1 contains a cross-site scripting (XSS) vulnerability in the View Site funtion. When viewing an added site, an XSS payload can be injected in cookies view which can lead to remote code execution.	6.1	More Details
CVE-2019-8762	A validation issue was addressed with improved logic. This issue is fixed in Safari 13.0.1, iOS 13.1 and iPadOS 13.1, iCloud for Windows 10.7, tvOS 13, iCloud for Windows 7.14, iTunes 12.10.1 for Windows. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2019-8771	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in Safari 13.0.1, iOS 13. Maliciously crafted web content may violate iframe sandboxing policy.	6.1	More Details
CVE-2020-27182	Multiple cross-site scripting (XSS) vulnerabilities in konzept-ix publiXone before 2020.015 allow remote attackers to inject arbitrary JavaScript or HTML via appletError.jsp, job_jacket_detail.jsp, ixedit/editor_component.jsp, or the login form.	6.1	More Details
CVE-2020-16140	The search functionality of the Greenmart theme 2.4.2 for WordPress is vulnerable to XSS.	6.1	More Details
CVE-2020-3515	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5650	Cross-site scripting vulnerability in Simple Download Monitor 3.8.8 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-27642	A cross-site scripting (XSS) vulnerability exists in the 'merge account' functionality in admins.js in BigBlueButton Greenlight 2.7.6.	6.1	More Details
CVE-2020-27344	The cm-download-manager plugin before 2.8.0 for WordPress allows XSS.	6.1	More Details
CVE-2020-3599	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2020-3583	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3582	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	6.1	More Details
CVE-2020-3581	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	6.1	More Details
CVE-2020-3580	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14788	Vulnerability in the Oracle Communications Diameter Signaling Router (DSR) product of Oracle Communications (component: User Interface). Supported versions that are affected are 8.0.0.0-8.4.0.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Diameter Signaling Router (DSR). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Diameter Signaling Router (DSR), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Diameter Signaling Router (DSR) accessible data as well as unauthorized read access to a subset of Oracle Communications Diameter Signaling Router (DSR) accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-14854	Vulnerability in the Hyperion Infrastructure Technology product of Oracle Hyperion (component: UI and Visualization). 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 Infrastructure Technology. 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 Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	6.1	More Details
CVE-2020-3553	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17454	WSO2 API Manager 3.1.0 and earlier has reflected XSS on the "publisher" component's admin interface. More precisely, it is possible to inject an XSS payload into the owner POST parameter, which does not filter user inputs. By putting an XSS payload in place of a valid Owner Name, a modal box appears that writes an error message concatenated to the injected payload (without any form of data encoding). This can also be exploited via CSRF.	6.1	More Details
CVE-2020-27620	The Cosmos Skin for MediaWiki through 1.35.0 has stored XSS because MediaWiki messages were not being properly escaped. This is related to wfMessage and Html::rawElement, as demonstrated by CosmosSocialProfile::getUserGroups.	6.1	More Details
CVE-2020-14802	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). 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 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-14832	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). 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 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/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-2020-27608	In BigBlueButton before 2.2.28 (or earlier), uploaded presentations are sent to clients without a Content-Type header, which allows XSS, as demonstrated by a .png file extension for an HTML document.	6.1	More Details
CVE-2020-14813	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Grids). 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 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-14801	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). 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 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-14889	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14885	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-7751	pathval before version 1.1.1 is vulnerable to prototype pollution.	6.0	More Details
CVE-2020-14881	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-14884	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-13327	An issue has been discovered in GitLab Runner affecting all versions starting from 13.4.0 before 13.4.2, all versions starting from 13.3.0 before 13.3.7, all versions starting from 13.2.0 before 13.2.10. Insecure Runner Configuration in Kubernetes Environments	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14886	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2020-14753	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Installation). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Reporting and Analytics, 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 Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N).	5.9	More Details
CVE-2020-15265	In Tensorflow before version 2.4.0, an attacker can pass an invalid `axis` value to `tf.quantization.quantize_and_dequantize`. This results in accessing a dimension outside the rank of the input tensor in the C++ kernel implementation. However, dim_size only does a DCHECK to validate the argument and then uses it to access the corresponding element of an array. Since in normal builds, `DCHECK`-like macros are no-ops, this results in segfault and access out of bounds of the array. The issue is patched in eccb7ec454e6617738554a255d77f08e60ee0808 and TensorFlow 2.4.0 will be released containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved.	5.9	More Details
CVE-2020-7126	A remote server-side request forgery (ssrf) vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15274	In Wiki.js before version 2.5.162, an XSS payload can be injected in a page title and executed via the search results. While the title is properly escaped in both the navigation links and the actual page title, it is not the case in the search results. Commit a57d9af34c15adbf460dde6553d964efddf433de fixes this vulnerability (version 2.5.162) by properly escaping the text content displayed in the search results.	5.8	More Details
CVE-2020-3299	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload.	5.8	More Details
CVE-2020-3565	A vulnerability in the TCP Intercept functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured Access Control Policies (including Geolocation) and Service Polices on an affected system. The vulnerability exists because TCP Intercept is invoked when the embryonic connection limit is reached, which can cause the underlying detection engine to process the packet incorrectly. An attacker could exploit this vulnerability by sending a crafted stream of traffic that matches a policy on which TCP Intercept is configured. A successful exploit could allow the attacker to match on an incorrect policy, which could allow the traffic to be forwarded when it should be dropped. In addition, the traffic could incorrectly be dropped.	5.8	More Details
CVE-2020-14758	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:L).	5.6	More Details
CVE-2019-14713	Verifone MX900 series Pinpad Payment Terminals with OS 30251000 allow installation of unsigned packages.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21269	checkpath in OpenRC through 0.42.1 might allow local users to take ownership of arbitrary files because a non-terminal path component can be a symlink.	5.5	More Details
CVE-2020-3352	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to access hidden commands. The vulnerability is due to the presence of undocumented configuration commands. An attacker could exploit this vulnerability by performing specific steps that make the hidden commands accessible. A successful exploit could allow the attacker to make configuration changes to various sections of an affected device that should not be exposed to CLI access.	5.5	More Details
CVE-2020-9982	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in Apple Music 3.4.0 for Android. A malicious application may be able to leak a user's credentials.	5.5	More Details
CVE-2020-14754	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2019-8532	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in watchOS 5.2, iOS 12.2. A malicious application may be able to access restricted files.	5.5	More Details
CVE-2019-8839	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. An attacker in a privileged position may be able to perform a denial of service attack.	5.5	More Details
CVE-2020-6022	Check Point ZoneAlarm before version 15.8.139.18543 allows a local actor to delete arbitrary files while restoring files in Anti-Ransomware.	5.5	More Details
CVE-2019-8744	A memory corruption issue existed in the handling of IPv6 packets. This issue was addressed with improved memory management. This issue is fixed in macOS Catalina 10.15, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6, iOS 13. A malicious application may be able to determine kernel memory layout.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8656	This was addressed with additional checks by Gatekeeper on files mounted through a network share. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. Extracting a zip file containing a symbolic link to an endpoint in an NFS mount that is attacker controlled may bypass Gatekeeper.	5.5	More Details
CVE-2018-4339	This issue was addressed with a new entitlement. This issue is fixed in iOS 12.1. A local user may be able to read a persistent device identifier.	5.5	More Details
CVE-2020-24421	Adobe InDesign version 15.1.2 (and earlier) is affected by a NULL pointer dereference bug that occurs when handling a malformed .indd file. The impact is limited to causing a denial-of-service of the client application. User interaction is required to exploit this issue.	5.5	More Details
CVE-2018-4390	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan, watchOS 4.3, iOS 12.1. Processing a maliciously crafted text message may lead to UI spoofing.	5.5	More Details
CVE-2018-4391	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan, watchOS 4.3, iOS 12.1. Processing a maliciously crafted text message may lead to UI spoofing.	5.5	More Details
CVE-2020-14892	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2018-4433	A configuration issue was addressed with additional restrictions. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, watchOS 5, iOS 12, tvOS 12, macOS Mojave 10.14. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2020-3996	Velero (prior to 1.4.3 and 1.5.2) in some instances doesn't properly manage volume identifiers which may result in information leakage to unauthorized users.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4448	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.1.1, watchOS 5.1.2, macOS Mojave 10.14.2, Security Update 2018-003 High Sierra, Security Update 2018-006 Sierra, tvOS 12.1.1. A local user may be able to read kernel memory.	5.5	More Details
CVE-2019-8708	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15, iOS 13. A local user may be able to check for the existence of arbitrary files.	5.5	More Details
CVE-2019-8668	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.4, tvOS 12.4, watchOS 5.3. Processing a maliciously crafted image may lead to a denial of service.	5.5	More Details
CVE-2018-4468	This issue was addressed by removing additional entitlements. This issue is fixed in macOS Mojave 10.14.1, Security Update 2018-002 High Sierra, Security Update 2018-005 Sierra. A malicious application may be able to access restricted files.	5.5	More Details
CVE-2020-27673	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. Guest OS users can cause a denial of service (host OS hang) via a high rate of events to dom0, aka CID-e99502f76271.	5.5	More Details
CVE-2018-4381	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in tvOS 12.1, iOS 12.1. Processing a maliciously crafted message may lead to a denial of service.	5.5	More Details
CVE-2020-9902	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2019-8761	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, macOS Catalina 10.15. Parsing a maliciously crafted text file may lead to disclosure of user information.	5.5	More Details
CVE-2020-9997	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6, watchOS 6.2.8. A malicious application may disclose restricted memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8582	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iCloud for Windows 7.12, tvOS 12.3, iTunes 12.9.5 for Windows, macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra, iOS 12.3. Processing a maliciously crafted font may result in the disclosure of process memory.	5.5	More Details
CVE-2019-8538	A denial of service issue was addressed with improved validation. This issue is fixed in watchOS 5.2, macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra, iOS 12.2. Processing a maliciously crafted vcf file may lead to a denial of service.	5.5	More Details
CVE-2020-9361	CryptoPro CSP through 5.0.0.10004 on 64-bit platforms allows local users with the SeChangeNotifyPrivilege right to cause denial of service because user-mode input is mishandled during process creation.	5.5	More Details
CVE-2019-8850	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15, iOS 13.1 and iPadOS 13.1, tvOS 13, macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, watchOS 6. Processing a maliciously crafted audio file may disclose restricted memory.	5.5	More Details
CVE-2019-8853	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. An application may be able to read restricted memory.	5.5	More Details
CVE-2020-14760	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.31 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 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2020-9772	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A sandboxed process may be able to circumvent sandbox restrictions.	5.5	More Details
CVE-2020-9979	A trust issue was addressed by removing a legacy API. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0. An attacker may be able to misuse a trust relationship to download malicious content.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8790	This issue was addresses by updating incorrect URLSession file descriptors management logic to match Swift 5.0. This issue is fixed in Swift 5.1.1 for Ubuntu. Incorrect management of file descriptors in URLSession could lead to inadvertent data disclosure.	5.5	More Details
CVE-2020-3918	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A local user may be able to view sensitive user information.	5.5	More Details
CVE-2019-8774	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in iOS 13.1 and iPadOS 13.1, macOS Catalina 10.15. Parsing a maliciously crafted iBooks file may lead to a persistent denial-of-service.	5.5	More Details
CVE-2017-18925	opentmpfiles through 0.3.1 allows local users to take ownership of arbitrary files because d entries are mishandled and allow a symlink attack.	5.5	More Details
CVE-2019-8780	The issue was addressed with improved permissions logic. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2020-14787	Vulnerability in the Oracle Communications Diameter Signaling Router (DSR) product of Oracle Communications (component: User Interface). Supported versions that are affected are 8.0.0.0-8.4.0.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Diameter Signaling Router (DSR). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Diameter Signaling Router (DSR), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Diameter Signaling Router (DSR) accessible data as well as unauthorized read access to a subset of Oracle Communications Diameter Signaling Router (DSR) accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-27666	Strapi before 3.2.5 has stored XSS in the wysiwyg editor's preview feature.	5.4	More Details
CVE-2020-3997	VMware Horizon Server (7.x prior to 7.10.3 or 7.13.0) contains a Cross Site Scripting (XSS) vulnerability. Successful exploitation of this issue may allow an attacker to inject malicious script which will be executed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27388	Multiple Stored Cross Site Scripting (XSS) vulnerabilities exist in the YOURLS Admin Panel, Versions 1.5 - 1.7.10. An authenticated user must modify a PHP plugin with a malicious payload and upload it, resulting in multiple stored XSS issues.	5.4	More Details
CVE-2020-9860	A custom URL scheme handling issue was addressed with improved input validation. This issue is fixed in Safari 13.0.5. Processing a maliciously crafted URL may lead to arbitrary javascript code execution.	5.4	More Details
CVE-2018-8062	A cross-site scripting (XSS) vulnerability on Comtrend AR-5387un devices with A731-410JAZ-C04_R02.A2pD035g.d23i firmware allows remote attackers to inject arbitrary web script or HTML via the Service Description parameter while creating a WAN service.	5.4	More Details
CVE-2020-14895	Vulnerability in the Oracle Utilities Framework product of Oracle Utilities Applications (component: System Wide). Supported versions that are affected are 2.2.0.0.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0 - 4.3.0.6.0, 4.4.0.0.0 and 4.4.0.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Utilities Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Utilities Framework accessible data as well as unauthorized read access to a subset of Oracle Utilities Framework accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2020-14763	Vulnerability in the Oracle Application Express Quick Poll component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Quick Poll. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Quick Poll, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Quick Poll accessible data as well as unauthorized read access to a subset of Oracle Application Express Quick Poll accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14900	Vulnerability in the Oracle Application Express Group Calendar component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Group Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Group Calendar, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Group Calendar accessible data as well as unauthorized read access to a subset of Oracle Application Express Group Calendar accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-6876	A ZTE product is impacted by an XSS vulnerability. The vulnerability is caused by the lack of correct verification of client data in the WEB module. By inserting malicious scripts into the web module, a remote attacker could trigger an XSS attack when the user browses the web page. Then the attacker could use the vulnerability to steal user cookies or destroy the page structure. This affects: eVDC ZXCLOUD-iROSV6.03.04	5.4	More Details
CVE-2020-14762	Vulnerability in the Oracle Application Express component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-27533	A Cross Site Scripting (XSS) issue was discovered in the search feature of DedeCMS v.5.8 that allows malicious users to inject code into web pages, and other users will be affected when viewing web pages.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14810	Vulnerability in the Oracle Hospitality Suite8 product of Oracle Hospitality Applications (component: WebConnect). Supported versions that are affected are 8.10.2 and 8.11-8.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. 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 Hospitality Suite8 accessible data as well as unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2020-14898	Vulnerability in the Oracle Application Express Packaged Apps component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Packaged Apps. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Packaged Apps, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Packaged Apps accessible data as well as unauthorized read access to a subset of Oracle Application Express Packaged Apps accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-14899	Vulnerability in the Oracle Application Express Data Reporter component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Data Reporter. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Data Reporter, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Data Reporter accessible data as well as unauthorized read access to a subset of Oracle Application Express Data Reporter accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14826	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: SQL Extensions). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-3852	A logic issue was addressed with improved validation. This issue is fixed in Safari 13.0.5. A URL scheme may be incorrectly ignored when determining multimedia permission for a website.	5.3	More Details
CVE-2020-6648	A cleartext storage of sensitive information vulnerability in FortiOS command line interface in versions 6.2.4 and earlier and FortiProxy 2.0.0, 1.2.9 and earlier may allow an authenticated attacker to obtain sensitive information such as users passwords by connecting to FortiGate CLI and executing the "diag sys ha checksum show" command.	5.3	More Details
CVE-2020-14811	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: AMP EBS Integration). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-14806	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 of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/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-2020-14803	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 11.0.8 and 15. Easily exploitable 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 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 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2019-8858	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006. A user who shares their screen may not be able to end screen sharing.	5.3	More Details
CVE-2019-8796	A logic issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.1, Security Update 2019-001, and Security Update 2019-006, iOS 12.4.3, watchOS 6.1, iOS 13.2 and iPadOS 13.2. AirDrop transfers may be unexpectedly accepted while in Everyone mode.	5.3	More Details
CVE-2020-14783	Vulnerability in the Oracle Hospitality RES 3700 product of Oracle Food and Beverage Applications (component: CAL). The supported version that is affected is 5.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Hospitality RES 3700. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality RES 3700 accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-15680	If a valid external protocol handler was referenced in an image tag, the resulting broken image size could be distinguished from a broken image size of a non-existent protocol handler. This allowed an attacker to successfully probe whether an external protocol handler was registered. This vulnerability affects Firefox < 82.	5.3	More Details
CVE-2020-26895	Prior to 0.10.0-beta, LND (Lightning Network Daemon) would have accepted a counterparty high-S signature and broadcast tx-relay invalid local commitment/HTLC transactions. This can be exploited by any peer with an open channel regardless of the victim situation (e.g., routing node, payment-receiver, or payment-sender). The impact is a loss of funds in certain situations.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3585	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device	5.3	More Details
CVE-2020-27674	An issue was discovered in Xen through 4.14.x allowing x86 PV guest OS users to gain guest OS privileges by modifying kernel memory contents, because invalidation of TLB entries is mishandled during use of an INVLPG-like attack technique.	5.3	More Details
CVE-2020-27606	BigBlueButton before 2.2.28 (or earlier) does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	5.3	More Details
CVE-2020-9787	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. Some websites may not have appeared in Safari Preferences.	5.3	More Details
CVE-2020-26650	AtomXCMS 2.0 is affected by Arbitrary File Read via admin/dump.php	5.3	More Details
CVE-2020-27609	BigBlueButton through 2.2.28 records a video meeting despite the deactivation of video recording in the user interface. This may result in data storage beyond what is authorized for a specific meeting topic or participant.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3557	A vulnerability in the host input API daemon of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper certificate validation. An attacker could exploit this vulnerability by sending a crafted data stream to the host input daemon of the affected device. A successful exploit could allow the attacker to cause the host input daemon to restart. The attacker could use repeated attacks to cause the daemon to continuously reload, creating a DoS condition for the API.	5.3	More Details
CVE-2020-3564	A vulnerability in the FTP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass FTP inspection. The vulnerability is due to ineffective flow tracking of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device. A successful exploit could allow the attacker to bypass FTP inspection and successfully complete FTP connections.	5.3	More Details
CVE-2020-3578	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access rule and access parts of the WebVPN portal that are supposed to be blocked. The vulnerability is due to insufficient validation of URLs when portal access rules are configured. An attacker could exploit this vulnerability by accessing certain URLs on the affected device.	5.3	More Details
CVE-2020-15002	OX App Suite through 7.10.3 allows SSRF via the the /ajax/messaging/message message API.	5.0	More Details
CVE-2020-14790	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14804	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14799	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.20 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14794	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14793	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14789	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14861	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14809	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14786	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14785	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14777	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14776	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14773	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14741	Vulnerability in the Database Filesystem component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Resource, Create Table, Create View, Create Procedure, Dbfs_role privilege with network access via Oracle Net to compromise Database Filesystem. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Database Filesystem. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14672	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14901	Vulnerability in the RDBMS Security component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having Analyze Any privilege with network access via Oracle Net to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all RDBMS Security accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2020-14848	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14844	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14829	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14839	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14870	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14837	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14868	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14869	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14821	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14852	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14845	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14888	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14814	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14891	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14812	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14893	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-14866	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2020-15004	OX App Suite through 7.10.3 allows stats/diagnostic?param= XSS.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3561	A vulnerability in the Clientless SSL VPN (WebVPN) of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to inject arbitrary HTTP headers in the responses of the affected system. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to conduct a CRLF injection attack, adding arbitrary HTTP headers in the responses of the system and redirecting the user to arbitrary websites.	4.7	More Details
CVE-2020-27675	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. drivers/xen/events/events_base.c allows event-channel removal during the event-handling loop (a race condition). This can cause a use-after-free or NULL pointer dereference, as demonstrated by a dom0 crash via events for an in-reconfiguration paravirtualized device, aka CID-073d0552ead5.	4.7	More Details
CVE-2020-3558	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting an HTTP request from a user. A successful exploit could allow the attacker to modify the HTTP request to cause the interface to redirect the user to a specific, malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	4.7	More Details
CVE-2020-14822	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14840	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2020-14746	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Popup windows). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. 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 update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2020-14853	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: NDBCluster Plugin). Supported versions that are affected are 8.0.21 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 update, insert or delete access to some of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/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-2020-14867	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2020-14873	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.21 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 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2019-8827	The HTTP referrer header may be used to leak browsing history. The issue was resolved by downgrading all third party referrers to their origin. This issue is fixed in Safari 13.0.3, iTunes 12.10.2 for Windows, iCloud for Windows 10.9.2, tvOS 13.2, iOS 13.2 and iPadOS 13.2, iCloud for Windows 7.15. Visiting a maliciously crafted website may reveal the sites a user has visited.	4.3	More Details
CVE-2020-15003	OX App Suite through 7.10.3 allows Information Exposure because a user can obtain the IP address and User-Agent string of a different user (via the session API during shared Drive access).	4.3	More Details
CVE-2019-8898	An information disclosure issue existed in the handling of the Storage Access API. This issue was addressed with improved logic. This issue is fixed in iOS 13.3 and iPadOS 13.3, tvOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows. Visiting a maliciously crafted website may reveal sites a user has visited.	4.3	More Details
CVE-2020-9857	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5, Security Update 2020-003 Mojave, Security Update 2020-003 High Sierra. A malicious website may be able to exfiltrate autofilled data in Safari.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14768	Vulnerability in the Hyperion Analytic Provider Services product of Oracle Hyperion (component: Smart View Provider). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Hyperion Analytic Provider Services executes to compromise Hyperion Analytic Provider Services. 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 Hyperion Analytic Provider Services accessible data as well as unauthorized read access to a subset of Hyperion Analytic Provider Services accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion Analytic Provider Services. CVSS 3.1 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L).	4.3	More Details
CVE-2020-14745	Vulnerability in the Oracle REST Data Services product of Oracle REST Data Services (component: General). Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c; Standalone ORDS: prior to 20.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle REST Data Services accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2020-27612	Greenlight in BigBlueButton through 2.2.28 places usernames in room URLs, which may represent an unintended information leak to users in a room, or an information leak to outsiders if any user publishes a screenshot of a browser window.	4.3	More Details
CVE-2019-8834	A configuration issue was addressed with additional restrictions. This issue is fixed in tvOS 13.3, watchOS 6.1.1, iCloud for Windows 10.9, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra, iOS 13.3 and iPadOS 13.3, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. An attacker in a privileged network position may be able to bypass HSTS for a limited number of specific top-level domains previously not in the HSTS preload list.	4.3	More Details
CVE-2020-24847	A Cross-Site Request Forgery (CSRF) vulnerability is identified in FruityWifi through 2.4. Due to a lack of CSRF protection in page_config_adv.php, an unauthenticated attacker can lure the victim to visit his website by social engineering or another attack vector. Due to this issue, an unauthenticated attacker can change the newSSID and hostapd_wpa_passphrase.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14838	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2020-9935	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6. A user may be unexpectedly logged in to another user’s account.	4.3	More Details
CVE-2020-15270	Parse Server (npm package parse-server) broadcasts events to all clients without checking if the session token is valid. This allows clients with expired sessions to still receive subscription objects. It is not possible to create subscription objects with invalid session tokens. The issue is not patched.	4.3	More Details
CVE-2020-27621	The FileImporter extension in MediaWiki through 1.35.0 was not properly attributing various user actions to a specific user's IP address. Instead, for various actions, it would report the IP address of an internal Wikimedia Foundation server by omitting X-Forwarded-For data. This resulted in an inability to properly audit and attribute various user actions performed via the FileImporter extension.	4.3	More Details
CVE-2020-14764	Vulnerability in the Hyperion Planning product of Oracle Hyperion (component: Application Development Framework). 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 Planning. 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 Planning accessible data. CVSS 3.1 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N).	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14752	Vulnerability in the Hyperion Lifecycle Management product of Oracle Hyperion (component: Shared Services). 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 Lifecycle 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 Lifecycle Management accessible data. CVSS 3.1 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N).	4.2	More Details
CVE-2020-14767	Vulnerability in the Hyperion BI+ product of Oracle Hyperion (component: IQR-Foundation service). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion BI+ accessible data. CVSS 3.1 Base Score 4.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N).	4.2	More Details
CVE-2020-14772	Vulnerability in the Hyperion Lifecycle Management product of Oracle Hyperion (component: Shared Services). 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 Lifecycle 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 Lifecycle Management accessible data. CVSS 3.1 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N).	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14792	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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: 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 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).	4.2	More Details
CVE-2020-14736	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create Public Synonym privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Vault accessible data as well as unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	3.8	More Details
CVE-2020-14797	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15266	In Tensorflow before version 2.4.0, when the `boxes` argument of `tf.image.crop_and_resize` has a very large value, the CPU kernel implementation receives it as a C++ `nan` floating point value. Attempting to operate on this is undefined behavior which later produces a segmentation fault. The issue is patched in eccb7ec454e6617738554a255d77f08e60ee0808 and TensorFlow 2.4.0 will be released containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved.	3.7	More Details
CVE-2020-14779	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2020-14781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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 read access to a subset of Java SE, Java SE Embedded 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 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/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-2020-14782	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2019-8856	An API issue existed in the handling of outgoing phone calls initiated with Siri. This issue was addressed with improved state handling. This issue is fixed in iOS 13.3 and iPadOS 13.3, watchOS 6.1.1, macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. Calls made using Siri may be initiated using the wrong cellular plan on devices with two active plans.	3.3	More Details
CVE-2019-8857	The issue was addressed with improved validation when an iCloud Link is created. This issue is fixed in iOS 13.3 and iPadOS 13.3. Live Photo audio and video data may be shared via iCloud links even if Live Photo is disabled in the Share Sheet carousel.	3.3	More Details
CVE-2020-9786	This issue was addressed with improved checks This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra. An application may be able to trigger a sysdiagnose.	3.3	More Details
CVE-2019-8842	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. In certain configurations, a remote attacker may be able to submit arbitrary print jobs.	3.3	More Details
CVE-2020-27560	ImageMagick 7.0.10-34 allows Division by Zero in OptimizeLayerFrames in MagickCore/layer.c, which may cause a denial of service.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8642	An issue existed in the handling of S-MIME certificates. This issue was addressed with improved validation of S-MIME certificates. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. Processing a maliciously crafted mail message may lead to S/MIME signature spoofing.	3.3	More Details
CVE-2019-8809	A validation issue was addressed with improved logic. This issue is fixed in macOS Catalina 10.15, iOS 13.1 and iPadOS 13.1, tvOS 13, watchOS 6, iOS 13. A local app may be able to read a persistent account identifier.	3.3	More Details
CVE-2020-9986	A file access issue existed with certain home folder files. This was addressed with improved access restrictions. This issue is fixed in macOS Catalina 10.15.7. A malicious application may be able to read sensitive location information.	3.3	More Details
CVE-2020-8956	Pulse Secure Desktop Client 9.0Rx before 9.0R5 and 9.1Rx before 9.1R4 on Windows reveals users' passwords if Save Settings is enabled.	3.3	More Details
CVE-2020-7020	Elasticsearch versions before 6.8.13 and 7.9.2 contain a document disclosure flaw when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries. This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.	3.1	More Details
CVE-2020-14732	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Promotions). The supported version that is affected is 19.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14731	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Segment). Supported versions that are affected are 18.0 and 19.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	3.1	More Details
CVE-2020-14796	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. 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 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	3.1	More Details
CVE-2020-14798	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. 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 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14743	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 Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	3.1	More Details
CVE-2020-14818	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with network access via SSH 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 3.1 Base Score 3.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:L/A:N).	3.0	More Details
CVE-2020-14740	Vulnerability in the SQL Developer Install component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Client Computer User Account privilege with logon to the infrastructure where SQL Developer Install executes to compromise SQL Developer Install. 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 SQL Developer Install accessible data. CVSS 3.1 Base Score 2.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).	2.8	More Details
CVE-2020-14860	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.21 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14742	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. Easily exploitable vulnerability allows high privileged attacker having SYSDBA level account privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2020-14847	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 high privileged 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 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.7	More Details
CVE-2020-14759	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). 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 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:N/I:L/A:N).	2.5	More Details
CVE-2019-8799	This issue was resolved by replacing device names with a random identifier. This issue is fixed in iOS 13.1 and iPadOS 13.1, macOS Catalina 10.15, watchOS 6, tvOS 13. An attacker in physical proximity may be able to passively observe device names in AWDL communications.	2.4	More Details
CVE-2019-8777	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra. A local attacker may be able to view contacts from the lock screen.	2.4	More Details
CVE-2019-8732	The issue was addressed with improved data deletion. This issue is fixed in iOS 13. Deleted calls remained visible on the device.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14771	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.2	More Details
CVE-2020-14791	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.2	More Details
CVE-2020-14770	Vulnerability in the Hyperion BI+ product of Oracle Hyperion (component: IQR-Foundation service). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Hyperion BI+. 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 BI+ accessible data. CVSS 3.1 Base Score 2.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N).	2.0	More Details
CVE-2018-21266	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-21267	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-26156	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