SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 July 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
CVE-2020-14701	Vulnerability in the Oracle SD-WAN Aware product of Oracle Communications Applications (component: User Interface). The supported version that is affected is 8.2. E vulnerability is in Oracle SD-WAN Aware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Sl (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14606	Vulnerability in the Oracle SD-WAN Edge product of Oracle Communications Applications (component: User Interface). Supported versions that are affected are 8.2 an the vulnerability is in Oracle SD-WAN Edge, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-6103	An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be
CVE-2020-6102	An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be
CVE-2020-6101	An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be
CVE-2020-6100	An exploitable memory corruption vulnerability exists in AMD atidxx64.dll 26.20.15019.19000 graphics driver. A specially crafted pixel shader can cause memory corrup from guest machines running virtualization environments (ie. VMware, qemu, VirtualBox etc.) in order to perform guest-to-host escape - as it was demonstrated before webassembly). This vulnerability was triggered from HYPER-V guest using RemoteFX feature leading to executing the vulnerable code on the HYPER-V host (inside o
CVE-2020-11981	An issue was found in Apache Airflow versions 1.10.10 and below. When using CeleryExecutor, if an attacker can connect to the broker (Redis, RabbitMQ) directly, it is
CVE-2020-11982	An issue was found in Apache Airflow versions 1.10.10 and below. When using CeleryExecutor, if an attack can connect to the broker (Redis, RabbitMQ) directly, it was Worker.
CVE-2020-9669	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a lack of exploit mitigations vulnerability. Successful exploitation could lead to privilege escalat
CVE-2020-0225	In a2dp_vendor_ldac_decoder_decode_packet of a2dp_vendor_ldac_decoder.cc, there is a possible out of bounds write due to a missing bounds check. This could lea AndroidVersions: Android-10Android ID: A-142546668
CVE-2020-9670	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a symlink vulnerability vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2020-9671	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have an insecure file permissions vulnerability. Successful exploitation could lead to privilege escala

CVE Number	Description
CVE-2020-9682	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a symlink vulnerability vulnerability. Successful exploitation could lead to arbitrary file system v
CVE-2020-15801	In Python 3.8.4, sys.path restrictions specified in a python38._pth file are ignored, allowing code to be loaded from arbitrary locations. The <executable-name>._pth file
CVE-2020-14001	The kramdown gem before 2.3.0 for Ruby processes the template option inside Kramdown documents by default, which allows unintended read access (such as templ is used in Jekyll, GitLab Pages, GitHub Pages, and Thredded Forum.
CVE-2020-1647	On Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, a double free vulnerability can lead to a Denial of Service (result in an extended Denial of Service (DoS). The offending HTTP message that causes this issue may originate both from the HTTP server or the client. This issue af 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S2, 19.2R2; 19.3 versions prior to 19.3R
CVE-2020-1654	On Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, processing a malformed HTTP message can lead to a Der of Service (DoS) condition. The offending HTTP message that causes this issue may originate both from the HTTP server or the HTTP client. This issue affects Junipe 18.3R1-S7, 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S2,
CVE-2020-0224	In FastKeyAccumulator::GetKeysSlow of keys.cc, there is a possible out of bounds write due to type confusion. This could lead to remote code execution when process Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147664838
CVE-2020-14497	Advantech iView, versions 5.6 and prior, contains multiple SQL injection vulnerabilities that are vulnerable to the use of an attacker-controlled string in the construction
CVE-2020-0230	There is a possible out of bounds write due to an incorrect bounds check. Product: AndroidVersions: Android SoCAndroid ID: A-156337262
CVE-2020-0231	There is a possible out of bounds write due to an incorrect bounds check. Product: AndroidVersions: Android SoCAndroid ID: A-156333727
CVE-2020-14505	Advantech iView, versions 5.6 and prior, has an improper neutralization of special elements used in a command (“command injection”) vulnerability. Successful exploita attacker may then remotely execute code.
CVE-2020-5757	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can bypass c
CVE-2020-5759	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute c
CVE-2020-7206	HP nagios plugin for iLO (nagios-plugins-hpilo v1.50 and earlier) has a php code injection vulnerability.
CVE-2020-14484	OpenClinic GA versions 5.09.02 and 5.89.05b may allow an attacker to bypass the system’s account lockout protection, which may allow brute force password attacks.
CVE-2020-14485	OpenClinic GA versions 5.09.02 and 5.89.05b may allow an attacker to bypass client-side access controls or use a crafted request to initiate a session with limited func
CVE-2020-14494	OpenClinic GA versions 5.09.02 and 5.89.05b contain an authentication mechanism within the system that does not provide sufficient complexity to protect against brut
CVE-2020-6871	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the server and execute som <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.
CVE-2020-15866	mruby through 2.1.2-rc has a heap-based buffer overflow in the mrb_yield_with_class function in vm.c because of incorrect VM stack handling. It can be triggered via th
CVE-2016-7063	A flaw was found in pritunl-client before version 1.0.1116.6. Arbitrary write to user specified path may lead to privilege escalation.

CVE Number	Description
CVE-2020-12007	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vuln version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 a
CVE-2020-12011	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mit GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior.
CVE-2020-3357	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTT device or cause the device to reload, resulting in a DoS condition.
CVE-2020-12684	XXE injection can occur in i-net Clear Reports 2019 19.0.287 (Designer), as used in i-net HelpDesk and other products, when XML input containing a reference to an e
CVE-2020-14507	Advantech iView, versions 5.6 and prior, is vulnerable to multiple path traversal vulnerabilities that could allow an attacker to create/download arbitrary files, limit systen
CVE-2020-14501	Advantech iView, versions 5.6 and prior, has an improper authentication for critical function (CWE-306) issue. Successful exploitation of this vulnerability may allow an administrator account.
CVE-2020-14503	Advantech iView, versions 5.6 and prior, has an improper input validation vulnerability. Successful exploitation of this vulnerability could allow an attacker to remotely e
CVE-2020-14511	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Ro
CVE-2020-8178	Insufficient input validation in npm package `jison` <= 0.4.18 may lead to OS command injection attacks.
CVE-2020-14625	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 ar 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 im
CVE-2020-14644	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 ar 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 im
CVE-2020-14645	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, 1 compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentia
CVE-2020-14687	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 ar 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 im
CVE-2020-3331	A vulnerability in the web-based management interface of Cisco RV110W Wireless-N VPN Firewall and Cisco RV215W Wireless-N VPN Router could allow an unauthe data by the web-based management interface. An attacker could exploit this vulnerability by sending crafted requests to a targeted device. A successful exploit could al
CVE-2020-15889	Lua 5.4.0 has a getobjname heap-based buffer over-read because youngcollection in lgc.c uses markold for an insufficient number of list members.
CVE-2020-10285	The authentication implementation on the xArm controller has very low entropy, making it vulnerable to a brute-force attack. There is no mechanism in place to mitigate
CVE-2020-14000	MIT Lifelong Kindergarten Scratch scratch-vm before 0.2.0-prerelease.20200714185213 loads extension URLs from untrusted project.json files with certain _ character getExtensionIdForOpcode in serialization/sb3.js. The use of _ is incompatible with a protection mechanism in older versions, in which URLs were split and consequentl
CVE-2020-3330	A vulnerability in the Telnet service of Cisco Small Business RV110W Wireless-N VPN Firewall Routers could allow an unauthenticated, remote attacker to take full cor could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to gain full control of an affec
CVE-2020-3323	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, rer based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the at

CVE Number	Description
CVE-2020-3144	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN R commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could explo access on the affected device.
CVE-2020-3140	A vulnerability in the web management interface of Cisco Prime License Manager (PLM) Software could allow an unauthenticated, remote attacker to gain unauthorized exploit this vulnerability by submitting a malicious request to an affected system. An exploit could allow the attacker to gain administrative-level privileges on the system
CVE-2020-15027	ConnectWise Automate through 2020.x has insufficient validation on certain authentication paths, allowing authentication bypass via a series of attempts. This was pate
CVE-2019-20914	An issue was discovered in GNU LibreDWG through 0.9.3. There is a NULL pointer dereference in the function dwg_encode_common_entity_handle_data in common_
CVE-2020-10288	IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request of username and password, however you can input whatever y
CVE-2020-10287	The IRC5 family with UAS service enabled comes by default with credentials that can be found on publicly available manuals. ABB considers this a well documented fu and consider thereby this an exposure that should be mitigated. Moreover, future deployments should consider that these defaults should be forbidden (user should be
CVE-2020-14705	Vulnerability in the Oracle GoldenGate product of Oracle GoldenGate (component: Process Management). The supported version that is affected is Prior to 19.1.0.0.0. where the Oracle GoldenGate executes to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-15123	In codecov (npm package) before version 3.7.1 the upload method has a command injection vulnerability. Clients of the codecov-node library are unlikely to be aware o the fix was incomplete. It only blocked &, and command injection is still possible using backticks instead to bypass the sanitizer. The attack surface is low in this case. F that may supply malicious input and perform command injection.
CVE-2020-14658	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 Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible d (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).
CVE-2020-14599	Vulnerability in the Oracle CRM Gateway for Mobile Devices product of Oracle E-Business Suite (component: Setup of Mobile Applications). Supported versions that ar CRM Gateway for Mobile Devices. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracl for Mobile Devices 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)
CVE-2020-14598	Vulnerability in the Oracle CRM Gateway for Mobile Devices product of Oracle E-Business Suite (component: Setup of Mobile Applications). Supported versions that ar CRM Gateway for Mobile Devices. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracl for Mobile Devices 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)
CVE-2020-14665	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Invoice). Supported versions that are affected are 12.1.1-12.1.3 and 12 Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trade Managemen 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).
CVE-2020-10284	No authentication is required to control the robot inside the network, moreso the latest available user manual shows an option that lets the user to add a password to th operator from an active session.
CVE-2020-12013	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior.
CVE-2020-12029	All versions of FactoryTalk View SE do not properly validate input of filenames within a project directory. A remote, unauthenticated attacker may be able to execute a c Before installing this patch, the patch rollup dated 06 Apr 2020 or later MUST be applied. 1066644 – Patch Roll-up for CPR9 SRx.
CVE-2020-11436	LibreHealth EMR v2.0.0 is vulnerable to XSS that results in the ability to force arbitrary actions on behalf of other users including administrators.

OTHER VULNERABILITIES

CVE Number	Description
CVE-2020-3387	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to execute code with root privileges on an affected system. The vuln crafted response to the Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to access the software and execute commands they should no
CVE-2020-15816	In Western Digital WD Discovery before 4.0.251.0, a malicious application running with standard user permissions could potentially execute code in the application's pr

CVE Number	Description
CVE-2020-9309	Silverstripe CMS through 4.5 can be susceptible to script execution from malicious upload contents under allowed file extensions (for example HTML code in a TXT file protected or draft files are allowed by default for authorised users only, but can also be enabled through custom logic as well as modules such as silverstripe/userforms prevent this issue. Sites on the Common Web Platform (CWP) use this module by default, and are not affected.
CVE-2020-3145	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sendi operating system of the affected device as a high-privilege user.
CVE-2020-5756	Grandstream GWN7000 firmware version 1.0.9.4 and below allows authenticated remote users to modify the system's crontab via undocumented API. An attacker can
CVE-2020-5758	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can execute c
CVE-2020-2228	Jenkins Gitlab Authentication Plugin 1.5 and earlier does not perform group authorization checks properly, resulting in a privilege escalation vulnerability.
CVE-2020-3146	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sendi operating system of the affected device as a high-privilege user.
CVE-2020-14066	IceWarp Email Server 12.3.0.1 allows remote attackers to upload JavaScript files that are dangerous for clients to access.
CVE-2020-9257	HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E19R2P5patch02), versions earlier than 10.1.0.126(C10E11R5P1), and versions earlier thar buffer when handling certain operations of certificate, the attacker should trick the user into installing a malicious application, successful exploit may cause code execut
CVE-2020-11978	An issue was found in Apache Airflow versions 1.10.10 and below. A remote code/command injection vulnerability was discovered in one of the example DAGs shipped executor in use). If you already have examples disabled by setting load_examples=False in the config then you are not vulnerable.
CVE-2020-3332	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A success
CVE-2020-4464	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to execute arbitrary code on a system with a specially-crafted sequer
CVE-2020-7825	A vulnerability exists that could allow the execution of operating system commands on systems running MiPlatform 2019.05.16 and earlier. An attacker could execute a
CVE-2020-8215	A buffer overflow is present in canvas version <= 1.6.9, which could lead to a Denial of Service or execution of arbitrary code when it processes a user-provided image.
CVE-2020-10286	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to prevent sudo su or sudo -i to be run gaining unre
CVE-2020-3381	A vulnerability in the web management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct directory traversal attac uploaded to an affected device. An attacker could exploit this vulnerability by uploading a crafted file to an affected system. An exploit could allow the attacker to view o
CVE-2020-7826	EyeSurfer BflyInstallerX.ocx v1.0.0.16 and earlier versions contain a vulnerability that could allow remote files to be download by setting the arguments to the vulnerabl passed to it.
CVE-2019-20912	An issue was discovered in GNU LibreDWG through 0.9.3. Crafted input will lead to a stack overflow in bits.c, possibly related to bit_read_TF.
CVE-2020-15877	An issue was discovered in LibreNMS before 1.65.1. It has insufficient access control for normal users because of "'guard' => 'admin'" instead of "'middleware' => ['can:
CVE-2020-12854	A remote code execution vulnerability was identified in SecZetta NEProfile 3.3.11. Authenticated remote adversaries can invoke code execution upon uploading a carel

CVE Number	Description
CVE-2020-11439	LibreHealth EMR v2.0.0 is affected by a Local File Inclusion issue allowing arbitrary PHP to be included and executed within the EMR application.
CVE-2020-11438	LibreHealth EMR v2.0.0 is affected by systemic CSRF.
CVE-2020-15888	Lua through 5.4.0 mishandles the interaction between stack resizes and garbage collection, leading to a heap-based buffer overflow, heap-based buffer over-read, or u
CVE-2020-14609	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Answers). Supported versions that access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical dat to some of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).
CVE-2020-14611	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.3.0 and 12 Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data service (partial DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P
CVE-2020-3358	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow
CVE-2020-3351	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is du vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in
CVE-2020-14583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 1 protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability i takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sa 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 Sco
CVE-2020-15841	Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 89, 7.1 before fix pack 17, and 7.2 before fix pack 4, does not safely test a connection to a LDAP server
CVE-2020-14664	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. Difficult to exploit vulnerability a from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerabil 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 vuln CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-1645	When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets proc the Services PIC to restart. While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PI core-dumps -rw-rw---- 1 nobody wheel 575685123 <Date> /var/tmp/pics/mspmand.core.<*>.gz This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks
CVE-2020-14596	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Address Book). Supported versions that are affected are 12.1.1-12.1.3. Easily exploit interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV
CVE-2020-14588	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 10.3.6.0.0, 12 compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all O Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).
CVE-2020-14686	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Others). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Su well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVS
CVE-2020-14690	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are af HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unaut (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).
CVE-2020-14585	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 Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significa 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
CVE-2020-14584	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). Supported versions that are affected are 12.2.1.3.0 an 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 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 (Confident
CVE-2020-14582	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: User Registration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3 attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional produc as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVS

CVE Number	Description
CVE-2020-14688	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are af Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Appl data or complete access to all Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applic (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).
CVE-2020-14580	Vulnerability in the Oracle Communications Session Border Controller product of Oracle Communications Applications (component: System Admin). Supported version compromise Oracle Communications Session Border Controller. Successful attacks require human interaction from a person other than the attacker and while the vuln vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Session Border Controller accessible data as well as ur to cause a partial denial of service (partial DOS) of Oracle Communications Session Border Controller. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availabi
CVE-2020-14628	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this 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).
CVE-2020-14723	Vulnerability in the Oracle Help Technologies product of Oracle Fusion Middleware (component: Web UIX). Supported versions that are affected are 11.1.1.9.0 and 12. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Help Technologies, attacks may significantly Help Technologies accessible data as well as unauthorized update, insert or delete access to some of Oracle Help Technologies accessible data. CVSS 3.1 Base Scor
CVE-2020-14660	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 a Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Found 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 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).
CVE-2020-12499	In PHOENIX CONTACT PLCnext Engineer version 2020.3.1 and earlier an improper path sanitation vulnerability exists on import of project files.
CVE-2020-14666	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impac Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.2 (Conf
CVE-2020-14668	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3 Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significa Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVS
CVE-2020-14669	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploita human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, attacks may significantly impact additional products. Succe well as unauthorized update, insert or delete access to some of Oracle Configurator accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). (
CVE-2020-14670	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Settings). Supported versions that are affected are 12.1.1-1 Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced C to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Ora (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).
CVE-2020-14671	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12 Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound T data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advan (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).
CVE-2020-14608	Vulnerability in the Oracle Fusion Middleware MapViewer product of Oracle Fusion Middleware (component: Tile Server). The supported version that is affected is 12.2 MapViewer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Fusion Middleware M Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).
CVE-2020-14534	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Popups). The supported version that is affected is 12.2.9. Easily ex attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impac Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1
CVE-2020-4462	IBM Sterling External Authentication Server 6.0.1, 6.0.0, 2.4.3.2, and 2.4.2 and IBM Sterling Secure Proxy 6.0.1, 6.0.0, 3.4.3, and 3.4.2 are vulnerable to an XML Exter consume memory resources. IBM X-Force ID: 181482.
CVE-2020-14595	Vulnerability in the Oracle iLearning product of Oracle iLearning (component: Assessment Manager). Supported versions that are affected are 6.1 and 6.1.1. Easily exp vulnerability can result in unauthorized access to critical data or complete access to all Oracle iLearning accessible data and unauthorized ability to cause a partial deni (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).
CVE-2020-14681	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3 Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significa Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVS
CVE-2020-14682	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impac Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.1 Base Score 8.2 (Con
CVE-2020-14565	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 11.1.2.3.0, 12.2.1.3.0 Directory. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Unified Directory, attacks may sign critical data or all Oracle Unified Directory accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Unified Di

CVE Number	Description
CVE-2020-15813	Graylog before 3.3.3 lacks SSL Certificate Validation for LDAP servers. It allows use of an external user/group database stored in LDAP. The connection configuration not implement proper certificate validation (regardless of whether the "Allow self-signed certificates" option is used). Therefore, any attacker with the ability to intercept due to the lack of certificate validation), effectively bypassing Graylog's authentication mechanism.
CVE-2020-15842	Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 90, 7.1 before fix pack 17, and 7.2 before fix pack 5, allows man-in-the-middle attackers to execute arbi
CVE-2020-14569	Vulnerability in the Oracle FLEXCUBE Investor Servicing product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are aff compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical FLEXCUBE Investor Servicing 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
CVE-2019-20915	An issue was discovered in GNU LibreDWG through 0.9.3. Crafted input will lead to a heap-based buffer over-read in bit_write_TF in bits.c.
CVE-2019-20913	An issue was discovered in GNU LibreDWG through 0.9.3. Crafted input will lead to a heap-based buffer over-read in dwg_encode_entity in common_entity_data.spec
CVE-2020-14626	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence E (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-4125	Using HCL Marketing Operations 9.1.2.4, 10.1.x, 11.1.0.x, a malicious attacker could download files from the RHEL environment by doing some modification in the link
CVE-2019-20910	An issue was discovered in GNU LibreDWG through 0.9.3. Crafted input will lead to a heap-based buffer over-read in decode_R13_R2000 in decode.c, a different vuln
CVE-2020-2968	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 explo compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may signific (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-15602	An untrusted search path remote code execution (RCE) vulnerability in the Trend Micro Secuity 2020 (v16.0.0.1146 and below) consumer family of products could allov DLL could also be loaded with the same privileges as the installer if run as Administrator. User interaction is required to exploit the vulnerbaility in that the target must o
CVE-2020-3180	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker t
CVE-2020-9672	Adobe ColdFusion 2016 update 15 and earlier versions, and ColdFusion 2018 update 9 and earlier versions have a dll search-order hijacking vulnerability. Successful
CVE-2020-0120	In notifyErrorForPendingRequests of QCamera3HWI.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of pri ID: A-149995442
CVE-2020-9688	Adobe Download Manager version 2.0.0.518 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-15009	AsusScreenXpertServicec.exe and ScreenXpertUpgradeServiceManager.exe in ScreenPad2_Upgrade_Tool.msi V1.0.3 for ASUS PCs with ScreenPad 1.0 (UX450FD path with a particular file name.
CVE-2020-0227	In onCommand of CompanionDeviceManagerService.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalatio is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-129476618
CVE-2020-0226	In createWithSurfaceParent of Client.cpp, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege in the graphics se ID: A-150226994
CVE-2020-3379	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system system. A successful exploit could allow the attacker to gain administrative privileges.
CVE-2020-15852	An issue was discovered in the Linux kernel 5.5 through 5.7.9, as used in Xen through 4.13.x for x86 PV guests. An attacker may be granted the I/O port permissions o and Xen, aka CID-cadfad870154.

CVE Number	Description
CVE-2020-9254	HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E19R2P5patch02), versions earlier than 10.1.0.126(C10E11R5P1), and versions earlier thar the attacker should trick the user into installing a malicious application, successful exploit may cause code execution.
CVE-2020-5131	SonicWall NetExtender Windows client vulnerable to arbitrary file write vulnerability, this allows attacker to overwrite a DLL and execute code with the same privilege in
CVE-2020-15722	In version 12.1.0.1004 and below of 360 Total Security,when TPI calls the browser process, there exists a local privilege escalation vulnerability. An attacker who could
CVE-2020-9673	Adobe ColdFusion 2016 update 15 and earlier versions, and ColdFusion 2018 update 9 and earlier versions have a dll search-order hijacking vulnerability. Successful e
CVE-2020-15723	In the version 12.1.0.1004 and below of 360 Total Security, when the main process of 360 Total Security calls GameChrome.exe, there exists a local privilege escalatic
CVE-2020-9650	Adobe Media Encoder versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9646	Adobe Media Encoder versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-15724	In the version 12.1.0.1005 and below of 360 Total Security, when the Gamefolde calls GameChrome.exe, there exists a local privilege escalation vulnerability. An attac
CVE-2020-3388	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root priv submitting crafted input to the CLI. The attacker must be authenticated to access the CLI. A successful exploit could allow the attacker to execute commands with root p
CVE-2020-3380	A vulnerability in the CLI of Cisco Data Center Network Manager (DCNM) could allow an authenticated, local attacker to elevate privileges to root and execute arbitrary command. An attacker could exploit this vulnerability by authenticating as the fmserver user and submitting malicious input to a specific command. A successful exploit
CVE-2020-7818	DaviewIndy 8.98.9 and earlier has a Heap-based overflow vulnerability, triggered when the user opens a malformed PDF file that is mishandled by Daview.exe. Attacke
CVE-2020-14719	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses Admin Utilities). Supported versions that are affected a Expenses. While the vulnerability is in Oracle Internet Expenses, attacks may significantly impact additional products. Successful attacks of this vulnerability can result (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N).
CVE-2020-14720	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses Admin Utilities). Supported versions that are affected a Expenses. While the vulnerability is in Oracle Internet Expenses, attacks may significantly impact additional products. Successful attacks of this vulnerability can result (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14610	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments / File Upload). The supported version that is affected i Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework access
CVE-2020-14667	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 a Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Founc 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 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).
CVE-2020-14657	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 a Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Founc 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 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).
CVE-2020-14674	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14675	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14676	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).

CVE Number	Description
CVE-2020-14677	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14679	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 a Technical Foundation. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracl
CVE-2020-2967	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12. compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLog
CVE-2020-14699	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14713	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14499	Advantech iView, versions 5.6 and prior, has an improper access control vulnerability. Successful exploitation of this vulnerability may allow an attacker to obtain all use
CVE-2020-15603	An invalid memory read vulnerability in a Trend Micro Secuity 2020 (v16.0.0.1302 and below) consumer family of products' driver could allow an attacker to manipulate
CVE-2020-1650	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Ju 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.
CVE-2020-15879	Bitwarden Server 1.35.1 allows SSRF because it does not consider certain IPv6 addresses (ones beginning with fc, fd, fe, or ff, and the :: address) and certain IPv4 ad
CVE-2016-7064	A flaw was found in pritunl-client before version 1.0.1116.6. A lack of signature verification leads to sensitive information leakage
CVE-2018-21036	Sails.js before v1.0.0-46 allows attackers to cause a denial of service with a single request because there is no error handler in sails-hook-sockets to handle an empty
CVE-2020-3481	A vulnerability in the EGG archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.102.0 - 0.102.3 could allow an unauthenticated, remote attacker to vulnerability by sending a crafted EGG file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial
CVE-2020-15052	An issue was discovered in Artica Proxy CE before 4.28.030.418. SQL Injection exists via the Netmask, Hostname, and Alias fields.
CVE-2020-8214	A path traversal vulnerability in servey version < 3 allows an attacker to read content of any arbitrary file.
CVE-2020-12031	In all versions of FactoryTalk View SE, after bypassing memory corruption mechanisms found in the operating system, a local, authenticated attacker may corrupt the a patch, the patch rollup dated 06 Apr 2020 or later MUST be applied. 1066644 – Patch Roll-up for CPR9 SRx.
CVE-2020-8205	The uppy npm package < 1.13.2 and < 2.0.0-alpha.5 is vulnerable to a Server-Side Request Forgery (SSRF) vulnerability, which allows an attacker to scan local or ext
CVE-2020-10605	Grundfos CIM 500 before v06.16.00 responds to unauthenticated requests for password storage files.
CVE-2020-0228	There is an improper configuration of recorder related service. Product: AndroidVersions: Android SoCAndroid ID: A-156333723

CVE Number	Description
CVE-2020-1653	On Juniper Networks Junos OS devices, a stream of TCP packets sent to the Routing Engine (RE) may cause mbuf leak which can lead to Flexible PIC Concentrator (is not related to any specific configuration and it affects Junos OS releases starting from 17.4R1. However, this issue does not affect Junos OS releases prior to 18.2R1 command provides the number of mbufs counter that are currently in use and maximum number of mbufs that can be allocated on a platform: user@host> show syster device might become inaccessible requiring a manual restart. This issue affects Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versio 18.2X75-D60, 18.2X75-D34; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, Versions of Junos OS prior to 17.4R1 are unaffected by this vulnerability.
CVE-2020-1649	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2T generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Er functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0 category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CI pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pf the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prio versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Serie 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 vulnerability.
CVE-2020-15779	A Path Traversal issue was discovered in the socket.io-file package through 2.0.31 for Node.js. The socket.io-file::createFile message uses path.join with ../ in the nam
CVE-2020-1648	On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific BGP packet can lead to a routing process daemon (RPD) crash and restart. This Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 18.2X75 versions starting from 18.2X75-D50.8, 18.2X75-D60 and later versions, prio 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved: 19.4-EVO versions prior to 19.4R2-S2-EVO; 20.1-EVO versions prior to 20.1R2-EVO. This issue does not af
CVE-2020-1646	On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific UPDATE for an EBGP peer can lead to a routing process daemon (RPD) crash a when the device is receiving and processing the BGP UPDATE for an IBGP peer. However, the offending BGP UPDATE can originally come from an EBGP peer, propa EBGP peer. Repeated receipt and processing of the same specific BGP UPDATE can result in an extended Denial of Service (DoS) condition. This issue affects: Junip 19.3R1-EVO. Other Junos OS releases are not affected.
CVE-2020-1644	On Juniper Networks Junos OS and Junos OS Evolved devices, the receipt of a specific BGP UPDATE packet causes an internal counter to be incremented incorrectly in IPv4 or IPv6 network. This issue affects: Juniper Networks Junos OS: 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S8; 17.4 versions pr D13, 18.2X75-D411.1, 18.2X75-D420.18, 18.2X75-D52.3, 18.2X75-D60; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS Evolved: any releases prior to 20.1R2-EVO. This issue does not affect Juniper Network
CVE-2020-1640	An improper use of a validation framework when processing incoming genuine BGP packets within Juniper Networks RPD (routing protocols process) daemon allows a continuously sending any of these types of formatted genuine packets, an attacker can repeatedly crash the RPD process causing a sustained Denial of Service. Authe modes of use as long as the devices are configured to support the compromised framework and a BGP path is activated or active. This issue affects: Juniper Networks S8; 17.4 versions 17.4R2-S7, 17.4R3 and later versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions 18.1R3-S7 and later versions prior to 18.1R3-S10; 18.2 version D51, 18.2X75-D60, 18.2X75-D411, 18.2X75-D420 and later versions prior to 18.2X75-D32, 18.2X75-D33, 18.2X75-D420, 18.2X75-D52, 18.2X75-D60, 18.2X75-D65, 1 18.4R2-S4, 18.4R3 and later versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S3(*2); 19.1 versions 19.1R1-S3, 19.1R2 and later versions prior to 19.1R1-S5, 19.1R2-S 19.4 versions prior to 19.4R1-S2, 19.4R2, 19.4R3; 20.1 versions prior to 20.1R1-S1, 20.1R2. This issue does not affect Junos OS prior to 16.1R1. This issue affects IP
CVE-2020-7684	This affects all versions of package rollup-plugin-serve. There is no path sanitization in readFile operation.
CVE-2020-12015	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mits ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior.
CVE-2020-12009	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsub ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior.
CVE-2020-13405	userfiles/modules/users/controller/controller.php in Microweber before 1.1.20 allows an unauthenticated user to disclose the users database via a /modules/ POST requ
CVE-2020-14649	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2019-20909	An issue was discovered in GNU LibreDWG through 0.9.3. There is a NULL pointer dereference in the function dwg_encode_LWPOLYLINE in dwg.spec.
CVE-2020-6164	In SilverStripe through 4.5.0, a specific URL path configured by default through the silverstripe/framework module can be used to disclose the fact that a domain is host context, and is not known to present a vulnerability through web-based access. As a side-effect, this preconfigured path also blocks the creation of other resources on t
CVE-2020-3369	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, remote attacker to cause a denial of servic sending crafted FTP packets through an affected device. A successful exploit could allow the attacker to make the device reboot continuously, causing a DoS condition

CVE Number	Description
CVE-2020-15890	LuaJit through 2.1.0-beta3 has an out-of-bounds read because __gc handler frame traversal is mishandled.
CVE-2020-14639	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2 Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server ac
CVE-2020-14646	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14630	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications Applications (component: File Upload). Supported versions that are Oracle Enterprise Session Border Controller. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Enterprise Session Border Controller as well as unauthorized update, ins Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:
CVE-2020-14589	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 10.3.6.0.0, 12 compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-15572	Tor before 0.4.3.6 has an out-of-bounds memory access that allows a remote denial-of-service (crash) attack against Tor instances built to use Mozilla Network Securit
CVE-2020-14647	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14642	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: CacheStore). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2 Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle C
CVE-2020-14536	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Workbench). Supported vers via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager ac
CVE-2020-14535	Vulnerability in the Oracle Commerce Service Center product of Oracle Commerce (component: Commerce Service Center). Supported versions that are affected are 1 Commerce Service Center. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Comm accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).
CVE-2020-8203	Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.
CVE-2020-14593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java S creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typica 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 co (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N).
CVE-2020-15121	In radare2 before version 4.5.0, malformed PDB file names in the PDB server path cause shell injection. To trigger the problem it's required to open the executable in ra
CVE-2020-3405	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is sto attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and
CVE-2020-12028	In all versions of FactoryTalk View SEA remote, an authenticated attacker may be able to utilize certain handlers to interact with the data on the remote endpoint since FactoryTalk View SE. Users should follow guidance found in knowledge base articles 109056 and 1126943 to set up IPSec and/or HTTPs.
CVE-2020-14724	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Utility). The supported version that is affected is 11. Easily exploitable vulnerab require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7
CVE-2020-14543	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Installation). The supported version that and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-14561	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Installation). The supported version that and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).

CVE Number	Description
CVE-2020-14697	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily 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:
CVE-2020-14696	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Layout Templates). Supported versions that are affected are 11.1.1.9.0, 12.2 Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unau BI Publisher accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).
CVE-2020-14663	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily 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:
CVE-2020-14718	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: JVMCI). Supported versions that are affected are 19.3.2 and 20.1.0. Eas Edition. Successful attacks of this vulnerability can result in takeover of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Ava
CVE-2020-8958	Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute a
CVE-2020-14678	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily 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:
CVE-2020-14571	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 Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unau BI Publisher accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).
CVE-2020-2983	Vulnerability in the Oracle Data Masking and Subsetting product of Oracle Enterprise Manager (component: Data Masking). Supported versions that are affected are 13 Masking and Subsetting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Data Masking and Su 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).
CVE-2020-2984	Vulnerability in the Oracle Configuration Manager product of Oracle Enterprise Manager (component: Discovery and collection script). The supported version that is affe Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configuration Manager accessible da (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).
CVE-2019-17637	In all versions of Eclipse Web Tools Platform through release 3.18 (2020-06), XML and DTD files referring to external entities could be exploited to send the contents of
CVE-2020-14570	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 Publisher. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access Oracle 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)
CVE-2020-14691	Vulnerability in the Oracle Financial Services Liquidity Risk Management product of Oracle Financial Services Applications (component: User Interface). The supported Financial Services Liquidity Risk Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data Services Liquidity Risk Management 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/
CVE-2020-14602	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or mod access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts).
CVE-2020-14709	Vulnerability in the Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Card). Supported versions that are affecte Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data c Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR
CVE-2020-15108	In glpi before 9.5.1, there is a SQL injection for all usages of "Clone" feature. This has been fixed in 9.5.1.
CVE-2020-2982	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Enterprise Config Management). Supported versions that are Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Enterprise Manag 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).
CVE-2020-2981	Vulnerability in the Data Store component of Oracle Berkeley DB. The supported version that is affected is Prior to 18.1.40. Difficult to exploit vulnerability allows unauth interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.1 Base Score 7.0 (Confidentiality,
CVE-2020-14552	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 11.1.1.9 WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, attacks access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:I
CVE-2020-14557	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0, 12 Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unaut 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:

CVE Number	Description
CVE-2020-15110	In jupyterhub-kubespawner before 0.12, certain usernames will be able to craft particular server names which will grant them access to the default server of other users
CVE-2020-15780	An issue was discovered in drivers/acpi/acpi_configfs.c in the Linux kernel before 5.7.7. Injection of malicious ACPI tables via configfs could be used by attackers to by
CVE-2020-0122	In the permission declaration for com.google.android.providers.gsf.permission.WRITE_GSERVICES in AndroidManifest.xml, there is a possible permissions bypass. Th AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147247775
CVE-2019-20908	An issue was discovered in drivers/firmware/efi/efi.c in the Linux kernel before 5.4. Incorrect access permissions for the efivar_ssdt ACPI variable could be used by atta
CVE-2019-12000	HPE has found a potential Remote Access Restriction Bypass in HPE MSE Msg Gw application E-LTU prior to version 3.2 when HTTPS is used between the USSD an Gateway Configuration and Operations Guide.
CVE-2020-2969	Vulnerability in the Data Pump 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 ex Successful attacks of this vulnerability can result in takeover of Data Pump. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector:
CVE-2020-14619	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.20 and prior. Easily exploitable 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
CVE-2019-20911	An issue was discovered in GNU LibreDWG through 0.9.3. Crafted input will lead to denial of service in bit_calc_CRC in bits.c, related to a for loop.
CVE-2020-15117	In Synergy before version 1.12.0, a Synergy server can be crashed by receiving a kMsgHelloBack packet with a client name length set to 0xffffffff (4294967295) if the s Server is more than 4GB.
CVE-2020-3372	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive syst attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit coul condition.
CVE-2020-14594	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Inventory Integration). The supported ve Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-5767	Cross-site request forgery in Icegram Email Subscribers & Newsletters Plugin for WordPress v4.4.8 allows a remote attacker to send forged emails by tricking legitimat
CVE-2020-14539	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prio MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Serv
CVE-2020-9101	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V5
CVE-2020-1651	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line ca broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versi 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1.
CVE-2020-1641	A Race Condition vulnerability in Juniper Networks Junos OS LLDP implementation allows an attacker to cause LLDP to crash leading to a Denial of Service (DoS). Th An indicator of compromise is to evaluate log file details for lldp with RLIMIT. Intervention should occur before 85% threshold of used KB versus maximum available KB #],lldpd) has exceeded 85% of RLIMIT_DATA: " with [] as variable data to evaluate for. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S 15.1X53-D593; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D50, 18.2X75-D420; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4F
CVE-2020-14064	IceWarp Email Server 12.3.0.1 has Incorrect Access Control for user accounts.
CVE-2020-14065	IceWarp Email Server 12.3.0.1 allows remote attackers to upload files and consume disk space.
CVE-2020-14605	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or mod (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).

CVE Number	Description
CVE-2020-15807	GNU LibreDWG before 0.11 allows NULL pointer dereferences via crafted input files.
CVE-2020-14982	A Blind SQL Injection vulnerability in Kronos WebTA 3.8.x and later before 4.0 (affecting the com.threeis.webta.H352premPayRequest servlet's SortBy parameter) allo
CVE-2020-9259	Huawei Honor V30 smartphones with versions earlier than 10.1.0.212(C00E210R5P1) have an improper authentication vulnerability. The system does not sufficiently v bottom level, successful exploit could cause information disclosure.
CVE-2020-14591	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.20 and prior. Easily explo 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 (Availab
CVE-2020-9256	Huawei Mate 30 Pro smartphones with versions earlier than 10.1.0.150(C00E136R5P3) have an improper authorization vulnerability. The system does not properly res cause a denial of audio service.
CVE-2020-14652	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, 1 Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessib and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-15873	In LibreNMS before 1.65.1, an authenticated attacker can achieve SQL Injection via the customoid.inc.php device_id POST parameter to ajax_form.php.
CVE-2020-14680	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitab 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
CVE-2020-14685	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or mod (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).
CVE-2020-14692	Vulnerability in the Oracle Financial Services Loan Loss Forecasting and Provisioning product of Oracle Financial Services Applications (component: User Interface). S compromise Oracle Financial Services Loan Loss Forecasting and Provisioning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or m 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).
CVE-2020-14655	Vulnerability in the Oracle Security Service product of Oracle Fusion Middleware (component: SSL API). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 Service. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data as w and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N).
CVE-2020-14693	Vulnerability in the Oracle Insurance Accounting Analyzer product of Oracle Financial Services Applications (component: User Interface). Supported versions that are a Insurance Accounting Analyzer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle In (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).
CVE-2020-15102	In PrestaShop Dashboard Productions before version 2.1.0, there is improper authorization which enables an attacker to change the configuration. The problem is fixed
CVE-2020-3401	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal at attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful ex
CVE-2020-3437	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to read arbitrary files on the a specific file reference on the filesystem and then accessing it through the web-based management interface. A successful exploit could allow the attacker to read arbi
CVE-2020-3385	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, adjacent attacker to cause a denial of serv vulnerability by sending crafted packets through an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS condi
CVE-2020-14491	OpenClinic GA versions 5.09.02 and 5.89.05b do not properly check permissions before executing SQL queries, which may allow a low-privilege user to access privileg
CVE-2020-14576	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. 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
CVE-2020-4466	IBM MQ for HPE NonStop 8.0.4 and 8.1.0 could allow a remote authenticated attacker could cause a denial of service due to an error within the Queue processing func

CVE Number	Description
CVE-2020-14711	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can re Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-0305	In cdev_get of char_dev.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges nee
CVE-2020-14721	Vulnerability in the Oracle Enterprise Communications Broker product of Oracle Communications Applications (component: WebGUI). Supported versions that are affe Communications Broker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Enterprise Communication unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Communications Broker. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity a
CVE-2020-15700	An issue was discovered in Joomla! through 3.9.19. A missing token check in the ajax_install endpoint of com_installer causes a CSRF vulnerability.
CVE-2020-15695	An issue was discovered in Joomla! through 3.9.19. A missing token check in the remove request section of com_privacy causes a CSRF vulnerability.
CVE-2020-14662	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized update, insert or delete a of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Fi (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2020-15716	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the Preferences.php script. A remote attacker could exploit this vulnerab
CVE-2020-14638	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2 Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, a access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Ba
CVE-2020-14640	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2 Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, a access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Ba
CVE-2020-14613	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: Advanced User Interface). Supported versions that are affected are 12.2 WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks r some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 6
CVE-2020-15717	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the Search.inc.php script. A remote attacker could exploit this vulnerabil
CVE-2020-15696	An issue was discovered in Joomla! through 3.9.19. Lack of input filtering and escaping allows XSS attacks in mod_random_image.
CVE-2020-15718	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the PrintSchedules.php script. A remote attacker could exploit this vulne
CVE-2020-14572	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.(WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score (
CVE-2020-14063	A stored Cross-Site Scripting (XSS) vulnerability in the TC Custom JavaScript plugin before 1.2.2 for WordPress allows unauthenticated remote attackers to inject arbit
CVE-2020-14601	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and wh Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastruct 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).
CVE-2020-14607	Vulnerability in the Oracle Fusion Middleware MapViewer product of Oracle Fusion Middleware (component: Tile Server). Supported versions that are affected are 12.2 Middleware MapViewer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Fusion Middleware M delete access to some of Oracle Fusion Middleware MapViewer accessible data as well as unauthorized read access to a subset of Oracle Fusion Middleware MapVie (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14637	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2 Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, a access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Ba

CVE Number	Description
CVE-2020-14563	Vulnerability in the Oracle Enterprise Communications Broker product of Oracle Communications Applications (component: WebGUI). Supported versions that are affe Enterprise Communications Broker. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterpris update, insert or delete access to some of Oracle Enterprise Communications Broker accessible data as well as unauthorized read access to a subset of Oracle Enterp (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14636	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2 Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, a access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Ba
CVE-2020-2562	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Investor Module). Supported versions that are affecte HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability i unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primaver (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14592	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Rich Text Editor). Supported versions that are affected are 8.56, 8.57 PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, at to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data.
CVE-2020-14528	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected a to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Pr unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primaver (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-7680	docsify prior to 4.11.4 is susceptible to Cross-site Scripting (XSS). Docsify.js uses fragment identifiers (parameters after # sign) to load resources from server-side .md JavaScript/HTML inside docsify page.
CVE-2020-15053	An issue was discovered in Artica Proxy CE before 4.28.030.418. Reflected XSS exists via these search fields: real time request, System Events, Proxy Events, Proxy
CVE-2020-14627	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. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may sig PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1
CVE-2020-9485	An issue was found in Apache Airflow versions 1.10.10 and below. A stored XSS vulnerability was discovered in the Chart pages of the the "classic" UI.
CVE-2020-15803	Zabbix before 3.0.32rc1, 4.x before 4.0.22rc1, 4.1.x through 4.4.x before 4.4.10rc1, and 5.x before 5.0.2rc1 allows stored XSS in the URL Widget.
CVE-2020-15051	An issue was discovered in Artica Proxy before 4.30.000000. Stored XSS exists via the Server Domain Name, Your Email Address, Group Name, MYSQL Server, Data
CVE-2020-6872	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which wil <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.
CVE-2020-14615	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and wh Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastruct 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).
CVE-2020-9496	XML-RPC request are vulnerable to unsafe deserialization and Cross-Site Scripting issues in Apache OFBiz 17.12.03
CVE-2020-13932	In Apache ActiveMQ Artemis 2.5.0 to 2.13.0, a specially crafted MQTT packet which has an XSS payload as client-id or topic name can exploit this vulnerability. The XS section.
CVE-2020-12432	The WOPI API integration for Vereign Collabora CODE through 4.2.2 does not properly restrict delivery of JavaScript to a victim's browser, and lacks proper MIME type token, which can be accomplished if the attacker is able to upload a .docx or .odt file. The associated API endpoints for exploitation are /wopi/files and /wopi/getAccess
CVE-2020-4095	"BigFix Platform is storing clear text credentials within the system's memory. An attacker who is able to gain administrative privileges can use a program to create a me be applied to all BigFix deployments, limiting administrative access."
CVE-2020-14703	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this 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).

CVE Number	Description
CVE-2020-14704	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this 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).
CVE-2020-14629	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this 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).
CVE-2020-14928	evolution-data-server (eds) through 3.36.3 has a STARTTLS buffering issue that affects SMTP and POP3. When a server sends a "begin TLS" response, eds reads ad
CVE-2020-15586	Go before 1.13.13 and 1.14.x before 1.14.5 has a data race in some net/http servers, as demonstrated by the httputil.ReverseProxy Handler, because it reads a reques
CVE-2020-3150	A vulnerability in the web-based management interface of Cisco Small Business RV110W and RV215W Series Routers could allow an unauthenticated, remote attacke of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web-based management interface of the router, but only after any va which should be restricted.
CVE-2020-14618	Vulnerability in the Primavera Unifier product of Oracle Construction and Engineering (component: Mobile App). The supported version that is affected is Prior to 20.6. I 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 com accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N).
CVE-2019-19326	Silverstripe CMS sites through 4.4.4 which have opted into HTTP Cache Headers on responses served by the framework's HTTP layer can be vulnerable to web cache unexpected responses to other consumers of this cached response. Most other headers associated with web cache poisoning are already disabled through request hos
CVE-2020-14549	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Server). Supported versions that are affected a to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnera unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impa
CVE-2020-14527	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected a to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnera unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impa
CVE-2020-14706	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versi with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person othe Enterprise Project Portfolio Management accessible data as well as unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio I (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N).
CVE-2020-14530	Vulnerability in the Oracle Security Service product of Oracle Fusion Middleware (component: None). The supported version that is affected is 11.1.1.9.0. Difficult to ex this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data. CVSS 3.1 Base Score 5.9 (Confide
CVE-2020-4527	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the Secure flag for the session cookie in TLS mode information. IBM X-Force ID: 182631.
CVE-2020-14531	Vulnerability in the Siebel UI Framework product of Oracle Siebel CRM (component: SWSE Server). Supported versions that are affected are 20.6 and prior. Difficult to 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 ac accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N).
CVE-2020-3370	A vulnerability in URL filtering of Cisco Content Security Management Appliance (SMA) could allow an unauthenticated, remote attacker to bypass URL filtering on an a HTTP request to an affected device. A successful exploit could allow the attacker to redirect users to malicious sites.
CVE-2020-14722	Vulnerability in the Oracle Enterprise Communications Broker product of Oracle Communications Applications (component: WebGUI). Supported versions that are affe Communications Broker. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Commur insert or delete access to some of Oracle Enterprise Communications Broker accessible data as well as unauthorized read access to a subset of Oracle Enterprise Cor Communications Broker. CVSS 3.1 Base Score 5.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:L)
CVE-2020-15118	In Wagtail before versions 2.7.4 and 2.9.3, when a form page type is made available to Wagtail editors through the `wagtail.contrib.forms` app, and the page template is unescaped in the page. Allowing HTML within help text is an intentional design decision by Django; however, as a matter of policy Wagtail does not allow editors to inse functionality should therefore not have been made available to editor-level users. The vulnerability is not exploitable by an ordinary site visitor without access to the Wa versions, help text will be escaped to prevent the inclusion of HTML tags. Site owners who wish to re-enable the use of HTML within help text (and are willing to accept owners who are unable to upgrade to the new versions can secure their form page templates by rendering forms field-by-field as per Django's documentation, but omitt
CVE-2020-14617	Vulnerability in the Primavera Unifier product of Oracle Construction and Engineering (component: Platform, Mobile App). Supported versions that are affected are 16.1 HTTPS to compromise Primavera Unifier. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability ca (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).
CVE-2020-15366	An issue was discovered in ajv.validate() in Ajv (aka Another JSON Schema Validator) 6.12.2. A carefully crafted JSON schema could be provided that allows executio denial of service, not execution of code.)

CVE Number	Description
CVE-2020-1652	OpenNMS is accessible via port 9443
CVE-2020-14537	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Packaging Scripts). The supported version that is affected is 11. Easily exploitable vulnerabil require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Suc Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:N/I:N/A:H).
CVE-2020-1643	Execution of the "show ospf interface extensive" or "show ospf interface detail" CLI commands on a Juniper Networks device running Junos OS may cause the routing executing the same CLI commands, a local attacker can repeatedly crash the RPD process causing a sustained Denial of Service. Note: Only systems utilizing ARM pr this issue. The processor architecture can be displayed via the 'uname -a' command. For example: ARM (vulnerable): % uname -a l awk '{print $NF}' arm PowerPC (no -a l awk '{print $NF}' i386 This issue affects Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D100; 14.1X53 versions prior to 14.1X53-D140, 14.1X53-D 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S2, 17.4R3; 18.1 versi
CVE-2020-9255	Huawei Honor 10 smartphones with versions earlier than 10.0.0.178(C00E178R1P4) have a denial of service vulnerability. Certain service in the system does not suffic cause a denial of service condition.
CVE-2020-14651	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exp 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, ins (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-9649	Adobe Media Encoder versions 14.2 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2020-0107	In getUiccCardsInfo of PhoneInterfaceManager.java, there is a possible permissions bypass due to improper input validation. This could lead to local information disclo ID: A-146570216
CVE-2020-14643	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exp 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, ins (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-9227	Huawei Smart Phones Moana-AL00B with versions earlier than 10.1.0.166 have a missing initialization of resource vulnerability. An attacker tricks the user into installin exceptions.
CVE-2019-4090	"HCL Campaign is vulnerable to cross-site scripting when a user provides XSS scripts in Campaign Description field."
CVE-2020-5765	Nessus 8.10.0 and earlier were found to contain a Stored XSS vulnerability due to improper validation of input during scan configuration. An authenticated, remote atta mechanisms to correct this issue in Nessus 8.11.0.
CVE-2019-4091	"HCL Marketing Platform is vulnerable to cross-site scripting during addition of new users and also while searching for users in Dashboard, potentially giving an attacke
CVE-2020-3406	A vulnerability in the web-based management interface of the Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execu
CVE-2020-14529	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Investor Module). Supported versions that are affecte HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability i unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-3468	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct SQL injection at queries. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit c
CVE-2020-4104	HCL BigFix WebUI is vulnerable to stored cross-site scripting (XSS) within the Apps->Software module. An attacker can use XSS to send a malicious script to an unsus id=kb_article&sysparm_article=KB0080855&sys_kb_id=971d99ed1b8ed01c086dcbfc0a4bcb6a.
CVE-2020-11983	An issue was found in Apache Airflow versions 1.10.10 and below. It was discovered that many of the admin management screens in the new/RBAC UI handled escap
CVE-2020-5769	Insufficient output sanitization in Teltonika firmware TRB2_R_00.02.02 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks l
CVE-2020-2222	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the job name in the 'Keep this build forever' badge tooltip, resulting in a stored cross-site scripting v

CVE Number	Description
CVE-2020-2226	Jenkins Matrix Authorization Strategy Plugin 2.6.1 and earlier does not escape user names shown in the configuration, resulting in a stored cross-site scripting vulnerab
CVE-2020-2221	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the upstream job's display name shown as part of a build cause, resulting in a stored cross-site scri
CVE-2020-2966	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.(WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized WebLogic Server 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).
CVE-2020-2513	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2019-4747	IBM Team Concert (RTC) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intende
CVE-2019-4748	IBM Jazz Team Server based Applications are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus a
CVE-2020-2227	Jenkins Deployer Framework Plugin 1.2 and earlier does not escape the URL displayed in the build home page, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2973	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2020-2225	Jenkins Matrix Project Plugin 1.16 and earlier does not escape the axis names shown in tooltips on the overview page of builds with multiple axes, resulting in a stored
CVE-2020-2224	Jenkins Matrix Project Plugin 1.16 and earlier does not escape the node names shown in tooltips on the overview page of builds with a single axis, resulting in a stored
CVE-2020-2223	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape correctly the 'href' attribute of links to downstream jobs displayed in the build console page, resultin
CVE-2020-14587	Vulnerability in the PeopleSoft Enterprise FIN Expenses product of Oracle PeopleSoft (component: Expenses). The supported version that is affected is 9.2. Easily exp attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise FIN Expenses accessible data as well as unauth impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2974	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2020-2972	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2020-2220	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the agent name in the build time trend page, resulting in a stored cross-site scripting vulnerability.
CVE-2020-9311	In SilverStripe through 4.5, malicious users with a valid Silverstripe CMS login (usually CMS access) can craft profile information which can lead to XSS for other users
CVE-2020-2975	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2020-14710	Vulnerability in the Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Security). Supported versions that are affe Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Customer Ma Segmentation Foundation 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:

CVE Number	Description
CVE-2020-14653	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versi attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in una unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrit
CVE-2020-2976	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2020-14612	Vulnerability in the PeopleSoft Enterprise HRMS product of Oracle PeopleSoft (component: Time and Labor). The supported version that is affected is 9.2. Easily explo this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read acces (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2971	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly 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 (Confid
CVE-2020-14550	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Ba
CVE-2020-5130	SonicOS SSLVPN LDAP login request allows remote attackers to cause external service interaction (DNS) due to improper validation of the request. This vulnerability i
CVE-2020-15497	jcore/portal/ajaxPortal.jsp in Jalios JCMS 10.0.2 build-20200224104759 allows XSS via the types parameter. Note: It is asserted that this vulnerability is not present in t
CVE-2020-14648	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14558	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. 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
CVE-2020-15698	An issue was discovered in Joomla! through 3.9.19. Inadequate filtering on the system information screen could expose Redis or proxy credentials
CVE-2020-14673	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14621	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0 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 Jav without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Ve
CVE-2020-14700	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14698	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14695	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14694	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-15699	An issue was discovered in Joomla! through 3.9.19. Missing validation checks on the usergroups table object can result in a broken site configuration.
CVE-2020-14604	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

CVE Number	Description
CVE-2020-1655	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2T generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(/fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: majo /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: f /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: f /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: f causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3 prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reasse
CVE-2020-14635	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Logging). Supported versions that are affected are 12.2.5-12.2.9. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.1 Base Score 5
CVE-2020-14650	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-14603	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14562	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically 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 co (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-13923	IDOR vulnerability in the order processing feature from ecommerce component of Apache OFBiz before 17.12.04
CVE-2019-17639	In Eclipse OpenJ9 prior to version 0.21 on Power platforms, calling the System.arraycopy method with a length longer than the length of the source or destination array whatever value happens to be in the return register at that time to be used as if it matches the method's declared return type.
CVE-2020-3197	A vulnerability in the API subsystem of Cisco Meetings App could allow an unauthenticated, remote attacker to retain and reuse the Traversal Using Relay NAT (TURN credentials. An attacker could exploit this vulnerability by intercepting the legitimate traffic that is generated by an affected system. An exploit could allow the attacker to server. The attacker would not be able to take control of the TURN server unless the same credentials were used in multiple systems.
CVE-2020-7696	This affects all versions of package react-native-fast-image. When an image with source={{uri: "...", headers: { host: "somehost.com", authorization: "..." }} is loaded, all
CVE-2020-15107	In openenclave before 0.10.0, enclaves that use x87 FPU operations are vulnerable to tampering by a malicious host application. By violating the Linux System V Appli Depending on the FPU control configuration of the enclave app and whether the operations are used in secret-dependent execution paths, this vulnerability may also b their applications against the patched libraries to be protected from this vulnerability.
CVE-2020-14039	In Go before 1.13.13 and 1.14.x before 1.14.5, Certificate.Verify may lack a check on the VerifyOptions.KeyUsages EKU requirements (if VerifyOptions.Roots equals ni
CVE-2020-6165	SilverStripe 4.5.0 allows attackers to read certain records that should not have been placed into a result set. This affects silverstripe/recipe-cms. The automatic permiss pagination), resulting in records that should have failed a permission check being added to the final result set. GraphQL endpoints are configured by default (e.g., for as limited permissions (e.g., where viewing records exposed through admin/graphql requires administrator permissions). However, if custom GraphQL endpoints have bee This vulnerability only applies to reading records; it does not allow unauthorised changing of records.
CVE-2020-14707	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can re (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H).
CVE-2020-14712	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 an to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can re (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N).
CVE-2020-14545	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Utility). The supported version that is affected is 11. Difficult to exploit vulnerab require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification acc CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:L).
CVE-2020-14575	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vu 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
CVE-2020-14632	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable 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

CVE Number	Description
CVE-2020-14641	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exp this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality ir
CVE-2020-14540	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. 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
CVE-2020-14568	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnera 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
CVE-2020-5768	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in Icegram Email Subscribers & Newsletters Plugin for WordPress v4.4.8 allow
CVE-2020-14624	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.20 and prior. Easily exploitable v 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
CVE-2020-14631	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Audit). Supported versions that are affected are 8.0.20 and prior. Easily exp 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 (Availab
CVE-2020-14622	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, 1 Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server acc
CVE-2020-3450	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an authenticated, remote attacker with administrative cre attacker could exploit this vulnerability by authenticating to the web-based management interface and sending malicious requests to an affected system. A successful e vulnerability, an attacker would need valid administrative credentials.
CVE-2020-14586	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily 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
CVE-2020-14623	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnera 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
CVE-2020-14567	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and 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 Ba
CVE-2020-14702	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily 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
CVE-2020-14620	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vu 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
CVE-2020-14597	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitab 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
CVE-2020-14656	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.20 and prior. Easily exploitable 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
CVE-2020-14614	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitab 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
CVE-2020-14547	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and 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 Ba
CVE-2020-14654	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitab 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

CVE Number	Description
CVE-2020-3442	The DuoConnect client enables users to establish SSH connections to hosts protected by a DNG instance. When a user initiates an SSH connection to a DNG-protecte contents of the '-relay' argument. If the '-relay' is set to a URL beginning with "http://", then the browser will initially attempt to load the URL over an insecure HTTP conr headers to enforce this). After successfully authenticating to a DNG, DuoConnect stores an authentication token in a local system cache, so users do not have to comp which defaults to 8 hours. If a user running DuoConnect already has a valid token, then instead of opening a web browser, DuoConnect directly contacts the DNG, agai begins with "http://", then this request will be sent over an insecure connection, and could be exposed to an attacker who is sniffing the traffic on the same network. The by that given relay host. The DNG provides network-level access only to the protected SSH servers. It does not interact with the independent SSH authentication and e
CVE-2020-3349	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to condu 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 customized l information.
CVE-2020-3348	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to condu 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 customized l information.
CVE-2020-14556	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 a 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 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 e such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-14555	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 Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact a 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).
CVE-2020-14554	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 Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, att 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:
CVE-2020-4316	IBM Publishing Engine 6.0.6, 6.0.6.1, and 7.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie valu can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 177354.
CVE-2020-14574	Vulnerability in the Oracle Communications Interactive Session Recorder product of Oracle Communications Applications (component: FACE). Supported versions that Communications Interactive Session Recorder executes to compromise Oracle Communications Interactive Session Recorder. Successful attacks of this vulnerability c well as unauthorized update, insert or delete access to some of Oracle Communications Interactive Session Recorder accessible data. CVSS 3.1 Base Score 4.7 (Con
CVE-2020-14717	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are af Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Appl delete access to some of Oracle Common Applications accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/
CVE-2020-14716	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are af Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Appl delete access to some of Oracle Common Applications accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/
CVE-2020-14659	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 a Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Founc delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/
CVE-2020-14532	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11 Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, att to some of Oracle Commerce Platform 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)
CVE-2020-14661	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 a Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Founc delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/
CVE-2020-2977	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or d Express accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).
CVE-2020-4100	"HCL Verse for Android was found to employ dynamic code loading. This mechanism allows a developer to specify which components of the application should not be l dynamically loaded components are only loaded as they are specifically requested. While this can have a positive impact on performance, or grant additional functional
CVE-2020-14715	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete
CVE-2020-14714	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete
CVE-2020-11437	LibreHealth EMR v2.0.0 is affected by SQL injection allowing low-privilege authenticated users to enumerate the database.

CVE Number	Description
CVE-2020-14566	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected a to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnera Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-14553	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 5.7.30 and prior and 8.0.20 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 4.3
CVE-2020-14684	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Suppo compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Succe Applications Infrastructure accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-3378	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of a exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in s
CVE-2020-14551	Vulnerability in the Oracle AutoVue product of Oracle Supply Chain (component: Security). The supported version that is affected is 21.0. Easily exploitable vulnerabilit unauthorized update, insert or delete access to some of Oracle AutoVue accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N
CVE-2020-3345	A vulnerability in certain web pages of Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to modify a web pag vulnerability by persuading a user to follow a crafted link that is designed to pass HTML code into an affected parameter. A successful exploit could allow the attacker t further client-side attacks.
CVE-2020-12027	All versions of FactoryTalk View SE disclose the hostnames and file paths for certain files within the system. A remote, authenticated attacker may be able to leverage Users should follow guidance found in knowledge base articles 109056 and 1126943 to set up IPSec and/or HTTPs.
CVE-2020-14559	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.6.48 and prior, 5.7.3 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 Ba
CVE-2020-14708	Vulnerability in the Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Segment). Supported versions that are aff Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Cus (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-4361	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information by disclosing private IP addresses in HTTP responses. IBM X-Force ID: 17876
CVE-2020-7292	Inappropriate Encoding for output context vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows a remote attacker to cause MWG to return an ambiguous r
CVE-2020-15697	An issue was discovered in Joomla! through 3.9.19. Internal read-only fields in the User table class could be modified by users.
CVE-2020-14600	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or d (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-14544	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Data, Domain & Function Security). The supported version that is Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS
CVE-2020-13788	Harbor prior to 2.0.1 allows SSRF with this limitation: an attacker with the ability to edit projects can scan ports of hosts accessible on the Harbor server's intranet.
CVE-2020-15111	In Fiber before version 1.12.6, the filename that is given in c.Attachment() (https://docs.gofiber.io/ctx#attachment) is not escaped, and therefore vulnerable for a CRLF i name of the downloaded file, redirect to another site, change the authorization header, etc. A possible workaround is to serialize the input before passing it to ctx.Attach
CVE-2020-14560	Vulnerability in the Oracle Hyperion BI+ product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.1.2.4. Difficult to exp 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 (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N).
CVE-2020-14546	Vulnerability in the Hyperion Financial Close Management product of Oracle Hyperion (component: Close Manager). The supported version that is affected is 11.1.2.4. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N).
CVE-2020-2978	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19 compromise Oracle Database - Enterprise Edition. While the vulnerability is in Oracle Database - Enterprise Edition, attacks may significantly impact additional product accessible data. CVSS 3.1 Base Score 4.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:N).

CVE Number	Description
CVE-2020-14577	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.(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 a 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 appli (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14578	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u25 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 J 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 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14579	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u25 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 J 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 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14573	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vu vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This 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 E
CVE-2020-14581	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14. 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 a 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 appli (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14533	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11 Commerce Platform. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthoriz Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 3.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/
CVE-2020-1776	When an agent user is renamed or set to invalid the session belonging to the user is keept active. The session can not be used to access ticket data in the case the ag
CVE-2020-14548	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerab vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 3.4 (Confiden
CVE-2020-15859	QEMU 4.2.0 has a use-after-free in hw/net/e1000e_core.c because a guest OS user can trigger an e1000e packet with the data's address set to the e1000e's MMIO ac
CVE-2020-9102	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper manage include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudI CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00S V200R019C00SPC800
CVE-2020-14542	Vulnerability in the Oracle Solaris product of Oracle Systems (component: libsuri). The supported version that is affected is 11. Easily exploitable vulnerability allows lov vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (C
CVE-2020-14564	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Environment Mgmt Console). Supported versions that are affected ar Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools
CVE-2020-14590	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Page Request). Supported versions that are affected are 12.1.3 an Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Ba
CVE-2020-14634	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnera vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (C
CVE-2020-14633	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnera 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
CVE-2020-14616	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics access
CVE-2020-9252	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versio traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafte
CVE-2020-14541	Vulnerability in the Hyperion Financial Close Management product of Oracle Hyperion (component: Close Manager). The supported version that is affected is 11.1.2.4. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or d (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).

CVE Number	Description
CVE-2015-5238	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2015-3796. Reason: This candidate is a reservation duplicate of CVE-2015-3796. Note to prevent accidental usage