Oracle Critical Patch Update Advisory - October 2020

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third-party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to "Critical Patch Updates, Security Alerts and Bulletins" for information about Oracle Security advisories.

Starting with the October 2020 Critical Patch Update, Oracle lists updates that address vulnerabilities in third-party components which are not exploitable in the context of their inclusion in their respective Oracle product beneath the product's risk matrix. Oracle has published two versions of the October 2020 Critical Patch Update Advisory: this version of the advisory implemented the change in how non-exploitable vulnerabilities in third-party components are reported, and the "traditional" advisory follows the same format as the previous advisories. The "traditional" advisory is published at https://www.oracle.com/security-alerts/cpuoct2020traditional.html.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update security patches without delay.

This Critical Patch Update contains 403 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at October 2020 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below. The product area is shown in the Patch Availability Document column.

Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

Affected Products and Versions	Patch Availability Document
Application Performance Management (APM), versions 13.3.0.0, 13.4.0.0	Enterprise Manager
Big Data Spatial and Graph, versions prior to 3.0	Database
Enterprise Manager Base Platform, versions 13.2.1.0, 13.3.0.0, 13.4.0.0	Enterprise Manager
Enterprise Manager for Peoplesoft, version 13.4.1.1	Enterprise Manager
Enterprise Manager for Storage Management, versions 13.3.0.0, 13.4.0.0	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2362, prior to XCP3090	Systems
Fujitsu M12-1, M12-2, M12-2S Servers, versions prior to XCP3090	Systems
Hyperion Analytic Provider Services, version 11.1.2.4	Fusion Middleware
Hyperion BI+, version 11.1.2.4	Fusion Middleware
Hyperion Essbase, version 11.1.2.4	Fusion Middleware
Hyperion Infrastructure Technology, version 11.1.2.4	Fusion Middleware
Hyperion Lifecycle Management, version 11.1.2.4	Fusion Middleware
Hyperion Planning, version 11.1.2.4	Fusion Middleware
Identity Manager Connector, version 9.0	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineering Suit
Management Pack for Oracle GoldenGate, version 12.2.1.2.0	Fusion Middleware
MySQL Cluster, versions 7.3.30 and prior, 7.4.29 and prior, 7.5.19 and prior, 7.6.15 and prior, 8.0.21 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.21 and prior	MySQL
MySQL Server, versions 5.6.49 and prior, 5.7.31 and prior, 8.0.21 and prior	MySQL
MySQL Workbench, versions 8.0.21 and prior	MySQL
Oracle Access Manager, version 11.1.2.3.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Agile PLM, versions 9.3.3, 9.3.5, 9.3.6	Oracle Supply Chain Products
Oracle Agile Product Lifecycle Management for Process, version 6.2.0.0	Oracle Supply Chain Products
Oracle Application Express, versions prior to 20.2	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle Banking Corporate Lending, versions 12.3.0, 14.0.0-14.4.0	Oracle Financial Services Applications
Oracle Banking Digital Experience, versions 18.1, 18.2, 18.3, 19.1, 19.2, 20.1	Oracle Financial Services Applications
Oracle Banking Payments, versions 14.1.0-14.4.0	Oracle Financial Services Applications
Oracle Banking Platform, versions 2.4.0-2.10.0	Oracle Banking Platform
Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Communications Application Session Controller, versions 3.8m0, 3.9m0p1	Oracle Communications Application Sessi Controller
Oracle Communications Billing and Revenue Management, versions 7.5.0.23.0, 12.0.0.2.0, 12.0.0.3.0	Oracle Communications Billing and Reven Management
Oracle Communications BRM - Elastic Charging Engine, versions 11.3.0.9.0, 12.0.0.3.0	Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0.0-8.4.0.5, [IDIH] 8.0.0-8.2.2	Oracle Communications Diameter Signalir Router
Oracle Communications EAGLE Software, versions 46.6.0-46.8.2	Oracle Communications EAGLE
Oracle Communications Element Manager, versions 8.2.0-8.2.2	Oracle Communications Element Manage
Oracle Communications Evolved Communications Application Server, version 7.1	Oracle Communications Evolved Communications Application Server
Oracle Communications Messaging Server, version 8.1	Oracle Communications Messaging Serve
Oracle Communications Offline Mediation Controller, version 12.0.0.3.0	Oracle Communications Offline Mediation Controller
Oracle Communications Services Gatekeeper, version 7	Oracle Communications Services Gatekee
Oracle Communications Session Border Controller, versions 8.2-8.4	Oracle Communications Session Border Controller

Affected Products and Versions	Patch Availability Document
Oracle Communications Session Report Manager, versions 8.2.0-8.2.2	Oracle Communications Session Report Manager
Oracle Communications Session Route Manager, versions 8.2.0-8.2.2	Oracle Communications Session Route Manager
Oracle Communications Unified Inventory Management, versions 7.3.0, 7.4.0	Oracle Communications Unified Inventory Management
Oracle Communications WebRTC Session Controller, version 7.2	Oracle Communications WebRTC Session Controller
Oracle Data Integrator, versions 11.1.1.9.0, 12.2.1.3.0	Fusion Middleware
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c	Database
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10	E-Business Suite
Oracle Endeca Information Discovery Integrator, version 3.2.0	Fusion Middleware
Oracle Endeca Information Discovery Studio, version 3.2.0	Fusion Middleware
Oracle Enterprise Repository, version 11.1.1.7.0	Fusion Middleware
Oracle Enterprise Session Border Controller, version 8.4	Oracle Enterprise Session Border Controlle
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.0	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Analytical Applications Reconciliation Framework, versions 8.0.6-8.0.8, 8.1.0	Oracle Financial Services Analytical Applications Reconciliation Framework
Oracle Financial Services Asset Liability Management, versions 8.0.6, 8.0.7, 8.1.0	Oracle Financial Services Asset Liability Management
Oracle Financial Services Balance Sheet Planning, version 8.0.8	Oracle Financial Services Balance Sheet Planning
Oracle Financial Services Basel Regulatory Capital Basic, versions 8.0.6-8.0.8, 8.1.0	Oracle Financial Services Basel Regulatory Capital Basic
Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, versions 8.0.6-8.0.8, 8.1.0	Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach
Oracle Financial Services Data Foundation, versions 8.0.6-8.1.0	Oracle Financial Services Data Foundatior
Oracle Financial Services Data Governance for US Regulatory Reporting, versions 8.0.6-8.0.9	Oracle Financial Services Data Governanc US Regulatory Reporting
Oracle Financial Services Data Integration Hub, versions 8.0.6, 8.0.7, 8.1.0	Oracle Financial Services Data Integration Hub

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Funds Transfer Pricing, versions 8.0.6, 8.0.7, 8.1.0	Oracle Financial Services Funds Transfer Pricing
Oracle Financial Services Hedge Management and IFRS Valuations, versions 8.0.6-8.0.8, 8.1.0	Oracle Financial Services Hedge Managen and IFRS Valuations
Oracle Financial Services Institutional Performance Analytics, versions 8.0.6, 8.0.7, 8.1.0, 8.7.0	Oracle Financial Services Institutional Performance Analytics
Oracle Financial Services Liquidity Risk Management, version 8.0.6	Oracle Financial Services Liquidity Risk Management
Oracle Financial Services Liquidity Risk Measurement and Management, versions 8.0.7, 8.0.8, 8.1.0	Oracle Financial Services Liquidity Risk Measurement and Management
Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.6-8.0.8, 8.1.0	Oracle Financial Services Loan Loss Forecasting and Provisioning
Oracle Financial Services Market Risk Measurement and Management, versions 8.0.6, 8.0.8, 8.1.0	Oracle Financial Services Market Risk Measurement and Management
Oracle Financial Services Price Creation and Discovery, versions 8.0.6, 8.0.7	Oracle Financial Services Price Creation A Discovery
Oracle Financial Services Profitability Management, versions 8.0.6, 8.0.7, 8.1.0	Oracle Financial Services Profitability Management
Oracle Financial Services Regulatory Reporting for European Banking Authority, versions 8.0.6-8.1.0	Oracle Financial Services Regulatory Reporting for European Banking Authority
Oracle Financial Services Regulatory Reporting for US Federal Reserve, versions 8.0.6-8.0.9	Oracle Financial Services Regulatory Reporting for US Federal Reserve
Oracle Financial Services Regulatory Reporting with AgileREPORTER, version 8.0.9.2.0	Oracle Financial Services Regulatory Reporting with AgileREPORTER
Oracle Financial Services Retail Customer Analytics, version 8.0.6	Oracle Financial Services Retail Customer Analytics
Oracle FLEXCUBE Core Banking, versions 5.2.0, 11.5.0-11.7.0	Oracle Financial Services Applications
Oracle FLEXCUBE Direct Banking, versions 12.0.1, 12.0.2, 12.0.3	Oracle Financial Services Applications
Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0	Oracle Financial Services Applications
Oracle FLEXCUBE Universal Banking, versions 12.3.0, 14.0.0-14.4.0	Oracle Financial Services Applications
Oracle GoldenGate Application Adapters, versions 12.3.2.1.0, 19.1.0.0.0	Fusion Middleware
Oracle GraalVM Enterprise Edition, versions 19.3.3, 20.2.0	Oracle GraalVM Enterprise Edition
Oracle Health Sciences Empirica Signal, version 9.0	Health Sciences
Oracle Healthcare Data Repository, version 7.0.1	Health Sciences

Affected Products and Versions	Patch Availability Document
Oracle Healthcare Foundation, versions 7.1.1, 7.2.0, 7.2.1, 7.3.0	Health Sciences
Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1	Oracle Hospitality Guest Access
Oracle Hospitality Materials Control, version 18.1	Oracle Hospitality Materials Control
Oracle Hospitality OPERA 5 Property Services, versions 5.5, 5.6	Oracle Hospitality OPERA 5 Property Servi
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle Hospitality RES 3700, version 5.7	Oracle Hospitality RES
Oracle Hospitality Simphony, versions 18.1, 18.2, 19.1.0-19.1.2	Oracle Hospitality Simphony
Oracle Hospitality Suite8, versions 8.10.2, 8.11-8.14	Oracle Hospitality Suite8
Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Insurance Accounting Analyzer, version 8.0.9	Oracle Insurance Accounting Analyzer
Oracle Insurance Allocation Manager for Enterprise Profitability, versions 8.0.8, 8.1.0	Oracle Insurance Allocation Manager for Enterprise Profitability
Oracle Insurance Data Foundation, versions 8.0.6-8.1.0	Oracle Insurance Data Foundation
Oracle Insurance Insbridge Rating and Underwriting, versions 5.0.0.0-5.6.0.0, 5.6.1.0	Oracle Insurance Applications
Oracle Insurance Policy Administration J2EE, versions 10.2.0.37, 10.2.4.12, 11.0.2.25, 11.1.0.15, 11.2.0.26, 11.2.2.0	Oracle Insurance Applications
Oracle Insurance Rules Palette, versions 10.2.0.37, 10.2.4.12, 11.0.2.25, 11.1.0.15, 11.2.0.26	Oracle Insurance Applications
Oracle Java SE, versions 7u271, 8u261, 11.0.8, 15	Java SE
Oracle Java SE Embedded, version 8u261	Java SE
Oracle JDeveloper, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Outside In Technology, versions 8.5.4, 8.5.5	Fusion Middleware
Oracle Policy Automation, versions 12.2.0-12.2.20	Oracle Policy Automation
Oracle Policy Automation Connector for Siebel, version 10.4.6	Oracle Policy Automation
Oracle Policy Automation for Mobile Devices, versions 12.2.0-12.2.20	Oracle Policy Automation
Oracle REST Data Services, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c, [Standalone ORDS] prior to 20.2.1	Database
Oracle Retail Advanced Inventory Planning, version 14.1	Retail Applications

Affected Products and Versions	Patch Availability Document
Oracle Retail Assortment Planning, versions 15.0.3.0, 16.0.3.0	Retail Applications
Oracle Retail Back Office, versions 14.0, 14.1	Retail Applications
Oracle Retail Bulk Data Integration, versions 15.0.3.0, 16.0.3.0	Retail Applications
Oracle Retail Central Office, versions 14.0, 14.1	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 18.0, 19.0	Retail Applications
Oracle Retail Integration Bus, versions 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Order Broker, versions 15.0, 16.0, 18.0, 19.0, 19.1, 19.2, 19.3	Retail Applications
Oracle Retail Point-of-Service, versions 14.0, 14.1	Retail Applications
Oracle Retail Predictive Application Server, versions 14.1.3.0, 15.0.3.0, 16.0.3.0	Retail Applications
Oracle Retail Price Management, versions 14.0.4, 14.1.3.0, 15.0.3.0, 16.0.3.0	Retail Applications
Oracle Retail Returns Management, versions 14.0, 14.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Xstore Point of Service, versions 15.0.3, 16.0.5, 17.0.3, 18.0.2, 19.0.1	Retail Applications
Oracle Solaris, versions 10, 11	Systems
Oracle TimesTen In-Memory Database, versions prior to 11.2.2.8.49, prior to 18.1.3.1.0, prior to 18.1.4.1.0	Database
Oracle Transportation Management, version 6.3.7	Oracle Supply Chain Products
Oracle Utilities Framework, versions 2.2.0.0.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.16	Virtualization
Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
PeopleSoft Enterprise HCM Global Payroll Core, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft

Affected Products and Versions	Patch Availability Document
PeopleSoft Enterprise SCM eSupplier Connection, version 9.2	PeopleSoft
Primavera Gateway, versions 16.2.0-16.2.11, 17.12.0-17.12.8	Oracle Construction and Engineering Suit
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12	Oracle Construction and Engineering Suit
Siebel Applications, versions 20.7, 20.8	Siebel

Note:

- Vulnerabilities affecting either Oracle Database or Oracle Fusion Middleware may affect Oracle Fusion Applications, so Oracle customers should refer to Oracle Fusion Applications Critical Patch Update Knowledge Document, My Oracle Support Note 1967316.1 for information on patches to be applied to Fusion Application environments.
- Vulnerabilities affecting Oracle Solaris may affect Oracle ZFSSA so Oracle customers should refer to the Oracle and Sun Systems Product Suite Critical Patch Update Knowledge Document, My Oracle Support Note 2160904.1 for information on minimum revisions of security patches required to resolve ZFSSA issues published in Critical Patch Updates and Solaris Third Party bulletins.
- Solaris Third Party Bulletins are used to announce security patches for third party software distributed with Oracle Solaris. Solaris 10 customers should refer to the latest patch-sets which contain critical security fixes and detailed in Systems Patch Availability Document. Please see Reference Index of CVE IDs and Solaris Patches (My Oracle Support Note 1448883.1) for more information.
- Users running Java SE with a browser can download the latest release from https://java.com. Users on the Windows and Mac OS X platforms can also use automatic updates to get the latest release.

Risk Matrix Content

Risk matrices list only security vulnerabilities that are newly addressed by the patches associated with this advisory. Risk matrices for previous security patches can be found in previous Critical Patch Update advisories and Alerts. An English text version of the risk matrices provided in this document is here.

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. Each vulnerability is identified by a CVE# which is its unique identifier. A vulnerability that affects multiple products will appear with the same CVE# in all risk matrices. A CVE# shown in *italics* indicates that this vulnerability impacts a different product, but also has impact on the product where the italicized CVE# is listed.

Security vulnerabilities are scored using CVSS version 3.1 (see Oracle CVSS Scoring for an explanation of how Oracle applies CVSS version 3.1).

Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update. Oracle does not disclose detailed information about this security analysis to customers, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see Oracle vulnerability disclosure policies.

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply Critical Patch Update security patches as soon as possible. Until you apply the Critical Patch Update patches, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

Oracle strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Critical Patch Update Supported Products and Versions

Patches released through the Critical Patch Update program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the Lifetime Support Policy. Oracle recommends that customers plan product upgrades to ensure that patches released through the Critical Patch Update program are available for the versions they are currently running.

Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, it is likely that

earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

Database, Fusion Middleware, and Oracle Enterprise Manager products are patched in accordance with the Software Error Correction Support Policy explained in My Oracle Support Note 209768.1. Please review the Technical Support Policies for further guidelines regarding support policies and phases of support.

Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Critical Patch Update to Oracle:

- 0rich1 Ant Security FG Lab: CVE-2020-14841
- Aaron Carreras of FireEye: CVE-2020-14871
- Abdulrahman Nour of Redforce: CVE-2020-14823
- Ahmed Elhady Mohamed of Ahmed Mohamed: CVE-2020-14768
- Akshay Gaikwad: CVE-2020-14762
- Alessandro Bosco of TIM S.p.A: CVE-2020-14842, CVE-2020-14843
- Alexander Kornbrust of Red Database Security: CVE-2020-14742, CVE-2020-14901
- Alves Christopher of Telecom Nancy: CVE-2020-14867
- Ammarit Thongthua of Secure D Center Cybersecurity Team: CVE-2020-14778
- Amy Tran: CVE-2020-14822, CVE-2020-14831, CVE-2020-14833, CVE-2020-14834, CVE-2020-14849, CVE-2020-14850, CVE-2020-14851, CVE-2020-14856, CVE-2020-14857
- Andrej Simko of Accenture: CVE-2020-14774, CVE-2020-14808
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2020-14841, CVE-2020-14881, CVE-2020-14884, CVE-2020-14885, CVE-2020-14886
- Bui Duong from Viettel Cyber Security: CVE-2020-14879, CVE-2020-14880
- Chi Tran: CVE-2020-14822, CVE-2020-14831, CVE-2020-14833, CVE-2020-14834, CVE-2020-14849, CVE-2020-14850, CVE-2020-14851, CVE-2020-14856, CVE-2020-14857
- codeplutos of AntGroup FG Security Lab: CVE-2020-14825
- Damian Bury: CVE-2020-14767, CVE-2020-14770
- Darragh Duffy: CVE-2020-14744
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2020-14741
- Edoardo Predieri of TIM S.p.A: CVE-2020-14842, CVE-2020-14843
- Fabio Minarelli of TIM S.p.A: CVE-2020-14842, CVE-2020-14843
- Filip Ceglik: CVE-2020-14772

- Francesco Russo of TIM S.p.A: CVE-2020-14842, CVE-2020-14843
- François Goichon of Google: CVE-2020-14735
- Gaoning Pan of Zhejiang University & Ant Security Light-Year Lab: CVE-2020-14872, CVE-2020-14892
- Graham Rymer of University Information Services, University of Cambridge: CVE-2020-14840
- Hangfan Zhang: CVE-2020-14828
- Ioannis Charalambous of NCC Group: CVE-2020-14787, CVE-2020-14788
- Ivo Palazzolo of Daimler TSS: CVE-2020-14864
- Jacob Thompson of FireEye: CVE-2020-14871
- Jakub Palaczynski: CVE-2020-14740, CVE-2020-14752
- Jakub Plusczok: CVE-2020-14854
- Jeffrey Martin of Rapid7: CVE-2020-14871
- Joe Almeida of Globlue Technologies: CVE-2020-14815
- Julien Zhan of Telecom Nancy: CVE-2020-14867
- Khuyen Nguyen of secgit.com: CVE-2020-14816, CVE-2020-14817, CVE-2020-14819, CVE-2020-14835
- Kritsada Sunthornwutthikrai of Secure D Center Cybersecurity Team: CVE-2020-14778
- Kylinking of NSFocus Security Team: CVE-2020-14841
- Larry W. Cashdollar: CVE-2020-14758, CVE-2020-14759
- Le Xuan Tuyen - VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2020-14841, CVE-2020-14859
- Long Nguyễn Hữu Vũ: CVE-2020-14863
- Longofo of Knownsec 404 Team: CVE-2020-14841
- Luca Di Giuseppe of TIM S.p.A: CVE-2020-14842, CVE-2020-14843
- Markus Loewe: CVE-2020-14796, CVE-2020-14797, CVE-2020-14798
- Massimiliano Brolli of TIM S.p.A: CVE-2020-14842, CVE-2020-14843
- Mateusz Dabrowski: CVE-2020-14784
- Philippe Antoine of Telecom Nancy: CVE-2020-14867
- Piotr Madej of ING Tech Poland: CVE-2020-14740
- Preeyakorn Keadsai of Secure D Center Cybersecurity Team: CVE-2020-14778
- Quynh Le of VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2020-14825
- r0 from A-TEAM of Legendsec at Qi'anxin Group: CVE-2020-14841

- Roger Meyer: CVE-2020-14745
- Rui Zhong: CVE-2020-14828
- Sergey Ostanin: CVE-2020-14781
- Shiva Gupta of Shiva Hacker One: CVE-2020-14890, CVE-2020-14897
- Spyridon Chatzimichail of OTE Hellenic Telecommunications Organization S.A.: CVE-2020-14764
- Thai Nguyen of ECQ: CVE-2020-14826
- thiscodecc: CVE-2020-14825
- Tomasz Stachowicz: CVE-2020-14780
- Trung Le: CVE-2020-14822, CVE-2020-14831, CVE-2020-14833, CVE-2020-14834, CVE-2020-14849, CVE-2020-14850, CVE-2020-14851, CVE-2020-14856, CVE-2020-14857
- Tuan Anh Nguyen of Viettel Cyber Security: CVE-2020-14855, CVE-2020-14862, CVE-2020-14875
- Tuan Anh Nguyen of Viettel Cyber Security working with Trend Micro Zero Day Initiative: CVE-2020-14876
- Ved Prabhu: CVE-2020-14762, CVE-2020-14763, CVE-2020-14898, CVE-2020-14899, CVE-2020-14900
- Venustech ADLab: CVE-2020-14820
- Viktor Gazdag of NCC Group: CVE-2020-14787, CVE-2020-14788
- voidfyoo of Chaitin Security Research Lab: CVE-2020-14882, CVE-2020-14883
- Walid Faour: CVE-2020-14783
- Xingwei Lin of Ant Security Light-Year Lab: CVE-2020-14872, CVE-2020-14889, CVE-2020-14892
- Xinlei Ying of Ant Security Light-Year Lab: CVE-2020-14892
- Xu Yuanzhen of Alibaba Cloud Security Team: CVE-2020-14841
- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2020-14828, CVE-2020-14861, CVE-2020-14893
- Yi Ren of Alibaba: CVE-2020-14790, CVE-2020-14828
- Yongheng Chen: CVE-2020-14828
- Yu Wang of BMH Security Team: CVE-2020-14841
- Yuyue Wang of Alibaba: CVE-2020-14828
- Zhiqiang Zang of University of Texas at Austin: CVE-2020-14792
- Zouhair Janatil-Idrissi of Telecom Nancy: CVE-2020-14867

Security-In-Depth Contributors

Oracle acknowledges people who have contributed to our Security-In-Depth program (see FAQ). People are acknowledged for Security-In-Depth contributions if they provide information, observations or suggestions pertaining to security vulnerability issues that result in significant modification of Oracle code or documentation in future releases, but are not of such a critical nature that they are distributed in Critical Patch Updates.

In this Critical Patch Update, Oracle recognizes the following for contributions to Oracle's Security-In-Depth program.:

- Amy Tran [35 reports]
- Chi Tran [35 reports]
- David Wilkins
- Markus Loewe [2 reports]
- Mateusz Dabrowski
- Trung Le [35 reports]

On-Line Presence Security Contributors

Oracle acknowledges people who have contributed to our On-Line Presence Security program (see FAQ). People are acknowledged for contributions relating to Oracle's on-line presence if they provide information, observations or suggestions pertaining to security-related issues that result in significant modification to Oracle's on-line external-facing systems.

For this quarter, Oracle recognizes the following for contributions to Oracle's On-Line Presence Security program:

- Abdulrahman Ahmed [3 reports]
- Abhishek Morla
- Adam Willard [2 reports]
- Adam Willard of Raytheon Foreground Security
- Adarsh VS Mannarakkal
- Ahmed Elmalky
- Ahmed Omer Morve
- Ai Ho (j3ssiejjj)
- Alex Munene
- Alisha Sheikh

- Anil Bhatt
- Anurag Kumar Rawat (A1C3VENOM)
- Ayan Saha
- Badal Sardhara
- Bindiya Sardhara
- Bui Dinh Bao aka 0xd0ff9 of Zalo Security Team (VNG Corp).
- Danny
- Dhiraj Mishra
- Funny Tech
- Gaurav Kumar
- Gourab Sadhukhan
- Harsh Mukeshbhai Joshi [2 reports]
- Himanshu Phulwariya
- Karthick Selvaraj
- Kartik Sharma
- Kaustubh Kale
- Kirtan Patel
- Kryptos Logic - Threat Intelligence Platform
- Kunal Gambhir
- Magrabur Alam Sofily
- Mansouri Badis
- Marwan Ali Albahar [2 reports]
- Matthew Harlow of EthicalHacker 20
- Mayank Kumar
- Mayank Malik, Kartik Sharma
- Micah Van Deusen
- Omkar Ghaisas
- Osman Ahmed Hassan
- Pankaj Kumar Thakur from Nepal [3 reports]
- Pratish Bhansali
- Ria from iZOOlogic
- Riccardo Donini

- Rick Verdoes & Danny de Weille of HackDefense
- Robert Lee Dick [2 reports]
- Roger Meyer
- Ronak Nahar
- Rudi Andriano
- Ryan awsmhacks Preston
- Sai Prashanth Pulisetti
- Sameer Goyal
- Shahid Ahmed [2 reports]
- Shivang Trivedi [2 reports]
- Shubham Kalaria
- Shubham Maheshwari
- Sidney Omondi of Salaam Technology
- Siva Pathela
- Soumajit Mukherjee
- Sparsh Gupta
- Srikar V - exp1o1t9r
- Sumit Sah
- Supun Madubashana Halangoda
- Suresh Nadar
- Swapnil Maurya - "swapmaurya20"
- Syed Muhammad Asim [2 reports]
- Vaibhav Gaikwad of Knock Security Solutions
- Venkata Sateesh Netti (str4n63r)
- Walid Hossain
- Yassine Triki
- Yatin Sharma

Critical Patch Update Schedule

Critical Patch Updates are released on the Tuesday closest to the 17th day of January, April, July and October. The next four dates are:

- 19 January 2021

- 20 April 2021
- 20 July 2021
- 19 October 2021

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - October 2020 Documentation Map
- Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions
- Risk Matrix Definitions
- Use of Common Vulnerability Scoring System (CVSS) by Oracle
- English text version of the risk matrices
- CVRF XML version of the risk matrices
- Map of CVE to Advisory/Alert
- Software Error Correction Support Policy
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2020-December-8	Rev 6. Added a note for CVE-2020-14871.
2020-November-16	Rev 5. Updated Oracle ZFS Storage Appliance Kit row to include CVE-2020-14871.
2020-October-29	Rev 4. Added CVE-2018-2765.
2020-October-27	Rev 3. Credit statement update.
2020-October-22	Rev 2. Affected versions change for CVE-2020-14807, CVE-2020-14810 and credit statement update.
2020-October-20	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 29 new security patches for Oracle Database Products divided as follows:

- 19 new security patches for Oracle Database Products

- 1 new security patch for Oracle Big Data Graph
- 5 new security patches for Oracle REST Data Services
- 4 new security patches for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 19 new security patches plus additional third party patches noted below for Oracle Database Products. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 of these patches is applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-12900	Core RDBMS (bzip2)	DBA Level Account	Oracle Net	No	8.8	Network	Low	Low
CVE-2020-14735	Scheduler	Local Logon	None	No	8.8	Local	Low	Low
CVE-2020-14734	Oracle Text	None	Oracle Net	Yes	8.1	Network	High	None
CVE-2018-2765	Oracle SSL API	None	HTTPS	Yes	7.5	Network	Low	None
CVE-2020-13935	Workload Manager (Apache Tomcat)	None	HTTP	Yes	7.5	Network	Low	None
CVE-2020-11023	Oracle Application Express (jQuery)	None	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11023	ORDS (jQuery)	None	HTTP	Yes	6.1	Network	Low	None

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14762	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-9281	Oracle Application Express	Valid User Account	HTTP	No	5.4	Network	Low	Low
CVE-2020-14899	Oracle Application Express Data Reporter	Valid User Account	HTTP	No	5.4	Network	Low	Low
CVE-2020-14900	Oracle Application Express Group Calendar	Valid User Account	HTTP	No	5.4	Network	Low	Low
CVE-2020-14898	Oracle Application Express Packaged Apps	Valid User Account	HTTP	No	5.4	Network	Low	Low
CVE-2020-14763	Oracle Application Express Quick Poll	Valid User Account	HTTP	No	5.4	Network	Low	Low
CVE-2020-14741	Database Filesystem	Resource, Create Table, Create View, Create Procedure, Dbfs_role	Oracle Net	No	4.9	Network	Low	High
CVE-2020-14901	RDBMS Security	Analyze Any	Oracle Net	No	4.9	Network	Low	High
CVE-2020-14736	Database Vault	Create Public Synonym	Oracle Net	No	3.8	Network	Low	High

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14743	Java VM	Create Procedure	Multiple	No	3.1	Network	High	Low
CVE-2020-14740	SQL Developer Install	Client Computer User Account	Local Logon	No	2.8	Local	Low	Low
CVE-2020-14742	Core RDBMS	SYSDBA level account	Oracle Net	No	2.7	Network	Low	High

Notes:

1. Additional ORDS bugs are documented in the risk matrix "Oracle REST Data Services Risk Matrix"

Additional CVEs addressed are:

- The patch for CVE-2019-12900 also addresses CVE-2016-3189
- The patch for CVE-2020-11023 also addresses CVE-2019-11358 and CVE-2020-11022
- The patch for CVE-2020-13935 also addresses CVE-2020-11996, CVE-2020-13934 and CVE-2020-9484
- The patch for CVE-2020-14734 also addresses CVE-2016-10244, CVE-2016-10328, CVE-2016-5300, CVE-2016-6153, CVE-2017-10989, CVE-2017-13685, CVE-2017-13745, CVE-2017-14232, CVE-2017-15286, CVE-2017-7857, CVE-2017-7858, CVE-2017-7864, CVE-2017-8105, CVE-2017-8287, CVE-2018-18873, CVE-2018-19139, CVE-2018-19539, CVE-2018-19540, CVE-2018-19541, CVE-2018-19542, CVE-2018-19543, CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2018-20570, CVE-2018-20584, CVE-2018-20622, CVE-2018-20843, CVE-2018-6942, CVE-2018-8740, CVE-2018-9055, CVE-2018-9154, CVE-2018-9252, CVE-2019-15903, CVE-2019-16168, CVE-2019-5018, CVE-2019-8457, CVE-2019-9936 and CVE-2019-9937

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Core RDBMS (LZ4): CVE-2019-17543
- Core RDBMS (Zstandard): CVE-2019-11922
- Oracle Database (Perl Expat): CVE-2018-20843 and CVE-2019-15903

- Oracle Spatial and Graph (Apache Log4j): CVE-2020-9488
- Oracle Spatial and Graph (jackson-databind): CVE-2019-16943, CVE-2017-15095, CVE-2017-17485, CVE-2017-7525, CVE-2018-5968, CVE-2018-7489, CVE-2019-16942 and CVE-2019-17531
- Oracle Spatial and Graph MapViewer (jQuery): CVE-2020-11023, CVE-2019-11358 and CVE-2020-11022
- SQL Developer (Apache Batik): CVE-2018-8013 and CVE-2017-5662
- SQL Developer (Apache Log4j): CVE-2017-5645
- SQL Developer (Apache POI): CVE-2017-12626, CVE-2016-5000, CVE-2017-5644 and CVE-2019-12415
- SQL Developer (jackson-databind): CVE-2018-7489, CVE-2017-15095, CVE-2017-17485, CVE-2018-1000873, CVE-2018-11307, CVE-2018-12022, CVE-2018-5968, CVE-2019-12086, CVE-2019-12384, CVE-2019-12814, CVE-2019-16335, CVE-2019-20330 and CVE-2020-8840
- SQL Developer (JCraft JSch): CVE-2016-5725
- SQL Developer Install (Bouncy Castle): CVE-2019-17359, CVE-2016-1000338, CVE-2016-1000339, CVE-2016-1000340, CVE-2016-1000341, CVE-2016-1000342, CVE-2016-1000343, CVE-2016-1000344, CVE-2016-1000345, CVE-2016-1000346, CVE-2016-1000352, CVE-2017-13098, CVE-2018-1000180, CVE-2018-1000613 and CVE-2018-5382

Oracle Database Server Client-Only Installations

- The following Oracle Database Server vulnerability included in this Critical Patch Update affects client-only installations: CVE-2020-14740.

Oracle Big Data Graph Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle Big Data Graph. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (se				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2019-0192	Big Data Spatial and Graph	Property Graph Analytics (Apache Solr)	HTTP	Yes	9.8	Network	Low	None	Nc

Additional CVEs addressed are:

- The patch for CVE-2019-0192 also addresses CVE-2017-3164

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Big Data Spatial and Graph
  - Property Graph Analytics (jQuery): CVE-2015-9251
  - Property Graph Analytics (jackson-databind): CVE-2020-9546, CVE-2015-9251, CVE-2017-5645, CVE-2018-12023, CVE-2018-14718, CVE-2018-7489, CVE-2019-10744, CVE-2019-12086, CVE-2019-14379, CVE-2019-16943, CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-11619, CVE-2020-11620, CVE-2020-14195, CVE-2020-9547 and CVE-2020-9548
  - Property Graph Analytics (lodash): CVE-2019-10744
  - Property Graph Analytics (Apache Log4j): CVE-2017-5645

Oracle REST Data Services Risk Matrix

This Critical Patch Update contains 5 new security patches plus additional third party patches noted below for Oracle REST Data Services. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2017-7658	Oracle REST Data Services	General (Eclipse Jetty)	HTTP	Yes	9.8	Network	Low	None
CVE-2016-1000031	Oracle REST Data Services	General (Apache Commons FileUpload)	HTTP	No	8.0	Network	Low	Low
CVE-2020-14744	Oracle REST	General	HTTP	No	6.5	Network	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
	Data Services								
CVE-2020-11023	Oracle REST Data Services	General (jQuery)	HTTP	Yes	6.1	Network	Low	None	
CVE-2020-14745	Oracle REST Data Services	General	HTTP	No	4.3	Network	Low	Low	

Additional CVEs addressed are:

- The patch for CVE-2017-7658 also addresses CVE-2016-4800, CVE-2017-7656, CVE-2017-7657, CVE-2017-9735, CVE-2018-12536, CVE-2018-12538, CVE-2018-12545, CVE-2019-10241, CVE-2019-10246, CVE-2019-10247 and CVE-2019-17632
- The patch for CVE-2020-11023 also addresses CVE-2019-11358 and CVE-2020-11022

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Oracle REST Data Services
  - General (Apache Batik): CVE-2018-8013 and CVE-2017-5662
  - General (jackson-databind): CVE-2019-16335, CVE-2019-12814, CVE-2019-14540, CVE-2019-14893, CVE-2019-17531, CVE-2019-20330, CVE-2020-11113, CVE-2020-11620 and CVE-2020-8840

Oracle TimesTen In-Memory Database Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle TimesTen In-Memory Database. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2018-11058	Oracle TimesTen In-Memory Database	EM TimesTen plugin (RSA BSAFE Crypto-C)	Multiple	Yes	9.8	Network	Low	Nc
CVE-2017-5645	Oracle TimesTen In-Memory Database	Install (Apache Log4j)	Multiple	Yes	9.8	Network	Low	Nc
CVE-2019-1010239	Oracle TimesTen In-Memory Database	Install (Dave Gamble/cJSON)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2019-0201	Oracle TimesTen In-Memory Database	Install (Apache ZooKeeper)	ZAB	Yes	5.9	Network	High	Nc

Additional CVEs addressed are:

- The patch for CVE-2017-5645 also addresses CVE-2020-1945
- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769
- The patch for CVE-2019-1010239 also addresses CVE-2019-11834 and CVE-2019-11835

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Communications Applications. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2019-10173	Oracle Communications BRM - Elastic Charging Engine	Diameter Gateway and SDK (xstream)	HTTP	Yes	9.8	Network	Low
CVE-2020-10683	Oracle Communications Unified Inventory Management	Core (dom4j)	HTTP	Yes	9.8	Network	Low
CVE-2019-10173	Oracle Communications Unified Inventory Management	Core (xstream)	HTTP	Yes	9.8	Network	Low
CVE-2020-10878	Oracle Communications Billing and Revenue Management	Core (Perl)	TCP	Yes	8.6	Network	Low
CVE-2020-11022	Oracle Communications Billing and Revenue Management	Billing Operation Center and Oracle Communication Billing Care (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-9489	Oracle Communications Messaging Server	Core (Apache Tika)	None	No	5.5	Local	Low
CVE-2020-9488	Oracle Communications Billing and Revenue Management	Billing Operation Center and Oracle Communication	SMTPS	Yes	3.7	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
		Billing Care (Apache Log4j)					
CVE-2020-9488	Oracle Communications Offline Mediation Controller	Core (Apache Log4j)	SMTPS	Yes	3.7	Network	High
CVE-2020-9488	Oracle Communications Unified Inventory Management	Core (Apache Log4j)	SMTPS	Yes	3.7	Network	High

Additional CVEs addressed are:

- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723
- The patch for CVE-2020-11022 also addresses CVE-2020-11023

Oracle Communications Risk Matrix

This Critical Patch Update contains 52 new security patches for Oracle Communications. 41 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-10683	Oracle Communications Application Session Controller	WS and WEB (dom4j)	Multiple	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-11973	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Apache Camel)	HTTP	Yes	9.8	Network	Low
CVE-2020-2555	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Oracle Coherence)	HTTP	Yes	9.8	Network	Low
CVE-2020-10683	Oracle Communications Diameter Signaling Router (DSR)	IDIH (dom4j)	HTTP	Yes	9.8	Network	Low
CVE-2019-2904	Oracle Communications Diameter Signaling Router (DSR)	Platform (Application Development Framework)	HTTP	Yes	9.8	Network	Low
CVE-2019-12260	Oracle Communications EAGLE Software	Network Stack (Wind River VxWorks)	TCP	Yes	9.8	Network	Low
CVE-2020-11984	Oracle Communications Element Manager	Core (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low
CVE-2020-11984	Oracle Communications Session Report Manager	Core (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low
CVE-2020-11984	Oracle Communications Session Route Manager	Core (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low
CVE-2019-13990	Oracle Communications Session Route Manager	Core (Quartz Scheduler)	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-17638	Oracle Communications Application Session Controller	WS and WEB (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low
CVE-2019-17638	Oracle Communications Element Manager	Core (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low
CVE-2019-17638	Oracle Communications Session Report Manager	Core (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low
CVE-2019-17638	Oracle Communications Session Route Manager	Core (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low
CVE-2020-14195	Oracle Communications Diameter Signaling Router (DSR)	IDIH (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-14195	Oracle Communications Element Manager	Core (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-14195	Oracle Communications Evolved Communications Application Server	Universal Data Record (jackson-databind)	XCAP	Yes	8.1	Network	High
CVE-2020-14195	Oracle Communications Session Report Manager	Core (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-14195	Oracle Communications Session Route Manager	Core (jackson-databind)	HTTP	Yes	8.1	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-5398	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2019-17359	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2019-12402	Oracle Communications Element Manager	Core (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2020-11080	Oracle Communications Session Border Controller	System (http2)	HTTP	Yes	7.5	Network	Low
CVE-2019-12402	Oracle Communications Session Report Manager	Core (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2019-12402	Oracle Communications Session Route Manager	Core (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2019-17359	Oracle Communications Session Route Manager	Core (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2019-10173	Oracle Communications Diameter Signaling Router (DSR)	IDIH (xstream)	HTTP	Yes	7.3	Network	Low
CVE-2020-9484	Oracle Communications Diameter Signaling Router (DSR)	Core (Apache Tomcat)	None	No	7.0	Local	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-9484	Oracle Communications Element Manager	Core (Apache Tomcat)	None	No	7.0	Local	High
CVE-2020-9484	Oracle Communications Session Report Manager	Core (Apache Tomcat)	None	No	7.0	Local	High
CVE-2020-9484	Oracle Communications Session Route Manager	Core (Apache Tomcat)	None	No	7.0	Local	High
CVE-2020-1945	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Apache Ant)	None	No	6.7	Local	High
CVE-2020-10722	Oracle Communications Session Border Controller	Platform (DPDK)	None	No	6.7	Local	Low
CVE-2020-5408	Oracle Communications Element Manager	Core (Spring Security)	HTTP	No	6.5	Network	Low
CVE-2020-5408	Oracle Communications Session Report Manager	Core (Spring Security)	HTTP	No	6.5	Network	Low
CVE-2020-5408	Oracle Communications Session Route Manager	Core (Spring Security)	HTTP	No	6.5	Network	Low
CVE-2020-11022	Oracle Communications Application Session Controller	Core (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-1941	Oracle Communications	IDIH (Apache ActiveMQ)	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
	Diameter Signaling Router (DSR)						
CVE-2020-11022	Oracle Communications Diameter Signaling Router (DSR)	IDIH (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-17091	Oracle Communications Diameter Signaling Router (DSR)	Platform (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low
CVE-2020-14788	Oracle Communications Diameter Signaling Router (DSR)	User Interface	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Communications WebRTC Session Controller	ME (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Enterprise Session Border Controller	Core (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-12415	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Apache POI)	None	No	5.5	Local	Low
CVE-2020-14787	Oracle Communications Diameter Signaling Router (DSR)	User Interface	HTTP	No	5.4	Network	Low
CVE-2019-11048	Oracle Communications Diameter Signaling Router (DSR)	Core (PHP)	HTTP	Yes	5.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-1954	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Apache CXF)	HTTP	Yes	5.3	Adjacent Network	High
CVE-2020-1954	Oracle Communications Element Manager	Core (Apache CXF)	HTTP	Yes	5.3	Adjacent Network	High
CVE-2020-1954	Oracle Communications Session Report Manager	Core (Apache CXF)	HTTP	Yes	5.3	Adjacent Network	High
CVE-2020-1954	Oracle Communications Session Route Manager	Core (Apache CXF)	HTTP	Yes	5.3	Adjacent Network	High
CVE-2020-9488	Oracle Communications Application Session Controller	WS and WEB (Apache Log4j)	SMTPS	Yes	3.7	Network	High
CVE-2020-9488	Oracle Communications Services Gatekeeper	Media Control UI (Apache Log4j)	SMTPS	Yes	3.7	Network	High

Additional CVEs addressed are:

- The patch for CVE-2019-11048 also addresses CVE-2020-7067
- The patch for CVE-2019-12260 also addresses CVE-2019-12261
- The patch for CVE-2019-13990 also addresses CVE-2019-5427
- The patch for CVE-2019-17638 also addresses CVE-2019-17632
- The patch for CVE-2020-10722 also addresses CVE-2020-10723 and CVE-2020-10724
- The patch for CVE-2020-11022 also addresses CVE-2020-11023
- The patch for CVE-2020-11080 also addresses CVE-2019-5436, CVE-2019-5481, CVE-2019-5482, CVE-2019-9511 and CVE-2019-9513
- The patch for CVE-2020-11973 also addresses CVE-2020-11971 and CVE-2020-11972

- The patch for CVE-2020-11984 also addresses CVE-2020-11993 and CVE-2020-9490
- The patch for CVE-2020-14195 also addresses CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-14060, CVE-2020-14061, CVE-2020-14062, CVE-2020-9546, CVE-2020-9547 and CVE-2020-9548
- The patch for CVE-2020-1941 also addresses CVE-2020-13920
- The patch for CVE-2020-1945 also addresses CVE-2017-5645
- The patch for CVE-2020-1954 also addresses CVE-2019-12423
- The patch for CVE-2020-5398 also addresses CVE-2020-5397
- The patch for CVE-2020-5408 also addresses CVE-2020-5407

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Construction and Engineering. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-11984	Instantis EnterpriseTrack	Core (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2019-17495	Primavera Gateway	Admin (Swagger UI)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2015-1832	Primavera Unifier	Platform (Apache Derby)	HTTP	Yes	9.1	Network	Low	Nc
CVE-2017-9096	Primavera Unifier	Platform (iText)	HTTP	Yes	8.8	Network	Low	Nc
CVE-2020-13935	Instantis EnterpriseTrack	Core (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-17558	Primavera Unifier	Platform (Apache Solr)	HTTP	No	7.5	Network	High	Lo
CVE-2018-17196	Primavera Unifier	Core (Apache Kafka)	HTTP	Yes	7.0	Network	High	No
CVE-2020-9489	Primavera Unifier	Platform (Apache Tika)	None	No	5.5	Local	Low	No
CVE-2020-9488	Primavera Unifier	Core (Apache Log4j)	SMTPS	Yes	3.7	Network	High	No

Additional CVEs addressed are:

- The patch for CVE-2020-11984 also addresses CVE-2020-11993 and CVE-2020-9490
- The patch for CVE-2020-13935 also addresses CVE-2020-13934

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 27 new security patches for Oracle E-Business Suite. 25 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle E-Business Suite products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle E-Business Suite products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that customers apply the October 2020 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Oracle E-Business Suite. For information on what patches need to be applied to your environments, refer to Oracle E-Business Suite Release 12 Critical Patch Update Knowledge Document (October 2020), My Oracle Support Note 2707309.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14855	Oracle Universal Work Queue	Work Provider Administration	HTTP	Yes	9.8	Network	Low	N
CVE-2020-14805	Oracle E-Business Suite Secure Enterprise Search	Search Integration Engine	HTTP	Yes	9.1	Network	Low	N
CVE-2020-14875	Oracle Marketing	Marketing Administration	HTTP	Yes	9.1	Network	Low	N
CVE-2020-14876	Oracle Trade Management	User Interface	HTTP	Yes	9.1	Network	Low	N
CVE-2020-14862	Oracle Universal Work Queue	Internal Operations	HTTP	No	8.8	Network	Low	L
CVE-2020-14850	Oracle CRM Technical Foundation	Flex Fields	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14816	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14817	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14831	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14835	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14849	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14819	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14863	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14808	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14833	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14834	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14851	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14856	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14857	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14774	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	7.5	Network	Low	N
CVE-2020-14761	Oracle Applications Manager	Oracle Diagnostics Interfaces	HTTP	Yes	6.5	Network	Low	N
CVE-2020-14823	Oracle CRM Technical Foundation	Preferences	HTTP	No	6.5	Network	Low	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14811	Oracle Applications Manager	AMP EBS Integration	HTTP	Yes	5.3	Network	Low	N
CVE-2020-14826	Oracle Applications Manager	SQL Extensions	HTTP	Yes	5.3	Network	Low	N
CVE-2020-14840	Oracle Application Object Library	Diagnostics	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14746	Oracle Applications Framework	Popup windows	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14822	Oracle Installed Base	APIs	HTTP	Yes	4.7	Network	Low	N

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle Enterprise Manager. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found here.

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the October 2020 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Enterprise Manager. For information on what patches need to be applied to your environments, refer to Critical Patch Update

October 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2694898.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-13990	Enterprise Manager Ops Center	Agent Provisioning (Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	Non
CVE-2018-11058	Oracle Application Testing Suite	Load Testing for Web Apps (RSA BSAFE Crypto-C)	HTTP	Yes	9.8	Network	Low	Non
CVE-2019-17638	Oracle Application Testing Suite	Load Testing for Web Apps (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low	Non
CVE-2020-5398	Enterprise Manager Base Platform	Connector Framework (Spring Framework)	HTTP	Yes	7.5	Network	High	Non
CVE-2020-1967	Enterprise Manager for Storage Management	Privilege Management (OpenSSL)	HTTPS	Yes	7.5	Network	Low	Non
CVE-2020-5398	Oracle Application Testing Suite	Load Testing for Web Apps (Spring Framework)	HTTP	Yes	7.5	Network	High	Non
CVE-2019-3740	Application Performance Management (APM)	Comp Management and Life Cycle Management (RSA BSAFE Crypto-J)	HTTPS	Yes	6.5	Network	Low	Non
CVE-2019-2897	Enterprise Manager Base Platform	Event Management	HTTP	No	6.4	Network	Low	Low
CVE-2020-11022	Enterprise Manager	Reports in Ops Center	HTTP	Yes	6.1	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
	Ops Center	(jQuery)						
CVE-2020-1954	Enterprise Manager Base Platform	Connector Framework (Apache CXF)	HTTP	Yes	5.3	Adjacent Network	High	Nor
CVE-2020-9488	Enterprise Manager for Peoplesoft	PSEM Plugin (Apache Log4j)	SMTPS	Yes	3.7	Network	High	Nor

Additional CVEs addressed are:

- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769
- The patch for CVE-2019-13990 also addresses CVE-2019-5427
- The patch for CVE-2019-17638 also addresses CVE-2019-17632
- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739
- The patch for CVE-2020-1954 also addresses CVE-2019-12419
- The patch for CVE-2020-5398 also addresses CVE-2020-5397

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 53 new security patches for Oracle Financial Services Applications. 49 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-17495	Oracle Banking Platform	Collections (Swagger UI)	HTTP	Yes	9.8	Network	Low	
CVE-2020-10683	Oracle Banking Platform	Collections (dom4j)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-10173	Oracle Banking Platform	Collections (xstream)	HTTP	Yes	9.8	Network	Low	
CVE-2020-10683	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Financial Services Institutional Performance Analytics	User Interface (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Financial Services Price Creation and Discovery	User Interface (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2017-5645	Oracle Financial Services Regulatory Reporting with AgileREPORTER	Core (Apache Ant)	Multiple	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Financial Services Retail Customer Analytics	User Interface (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-11973	Oracle FLEXCUBE Private Banking	Core (Apache Camel)	HTTP	Yes	9.8	Network	Low	
CVE-2020-14824	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	Yes	8.6	Network	Low	
CVE-2020-14195	Oracle Banking Digital	Framework (jackson-	HTTPS	Yes	8.1	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Experience	databind)						
CVE-2020-5398	Oracle Financial Services Regulatory Reporting with AgileREPORTER	Core (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2020-5398	Oracle FLEXCUBE Private Banking	Core (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2020-14894	Oracle Banking Corporate Lending	Core	HTTP	No	6.5	Network	Low	
CVE-2020-14896	Oracle Banking Payments	Core	HTTP	No	6.5	Network	Low	
CVE-2020-14890	Oracle FLEXCUBE Direct Banking	Pre Login	HTTP	Yes	6.5	Network	Low	
CVE-2020-14897	Oracle FLEXCUBE Direct Banking	Pre Login	HTTP	Yes	6.5	Network	Low	
CVE-2020-14887	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.5	Network	Low	
CVE-2020-11022	Oracle Banking Digital Experience	Framework (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Analytical Applications Reconciliation Framework	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-11022	Oracle Financial Services Asset Liability Management	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Balance Sheet Planning	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Basel Regulatory Capital Basic	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Data Foundation	Infrastructure (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Data Governance for US Regulatory Reporting	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Data Integration Hub	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Funds Transfer Pricing	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Hedge Management and IFRS Valuations	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Institutional	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Performance Analytics							
CVE-2020-11022	Oracle Financial Services Liquidity Risk Management	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Liquidity Risk Measurement and Management	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Loan Loss Forecasting and Provisioning	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Market Risk Measurement and Management	Infrastructure (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Price Creation and Discovery	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Profitability Management	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Regulatory Reporting for European Banking Authority	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Financial Services Regulatory	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Reporting for US Federal Reserve							
CVE-2020-1941	Oracle FLEXCUBE Private Banking	Core (Apache ActiveMQ)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Insurance Accounting Analyzer	IFRS17 (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Insurance Allocation Manager for Enterprise Profitability	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	Oracle Insurance Data Foundation	Infrastructure (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-1951	Oracle FLEXCUBE Private Banking	Core (Apache Tika)	None	No	5.5	Local	Low	
CVE-2019-10247	Oracle FLEXCUBE Core Banking	Core (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	
CVE-2020-9488	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle Financial Services Institutional Performance Analytics	User Interface (Apache Log4j)	SMTPS	Yes	3.7	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-9488	Oracle Financial Services Market Risk Measurement and Management	Infrastructure (Apache log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle Financial Services Price Creation and Discovery	User Interface (Apache Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle Financial Services Retail Customer Analytics	User Interface (Apache Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle FLEXCUBE Core Banking	Core (Apache Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle FLEXCUBE Private Banking	Core (Apache Log4j)	SMTPS	Yes	3.7	Network	High	

Additional CVEs addressed are:

- The patch for CVE-2019-10173 also addresses CVE-2013-7285
- The patch for CVE-2019-10247 also addresses CVE-2019-10246
- The patch for CVE-2020-11022 also addresses CVE-2020-11023
- The patch for CVE-2020-11973 also addresses CVE-2020-11971 and CVE-2020-11972
- The patch for CVE-2020-14195 also addresses CVE-2020-14060, CVE-2020-14061 and CVE-2020-14062
- The patch for CVE-2020-1941 also addresses CVE-2020-13920
- The patch for CVE-2020-1951 also addresses CVE-2020-1950
- The patch for CVE-2020-5398 also addresses CVE-2020-5397
- The patch for CVE-2020-9546 also addresses CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-9547 and CVE-2020-9548

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Food and Beverage Applications. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-11022	Oracle Hospitality Materials Control	Mobile Authorization (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11022	Oracle Hospitality Simphony	Simphony Apps (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14753	Oracle Hospitality Reporting and Analytics	Installation	None	No	5.9	Local	Low	Low
CVE-2020-14783	Oracle Hospitality RES 3700	CAL	TCP	Yes	5.3	Network	Low	None

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 46 new security patches for Oracle Fusion Middleware. 36 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security updates are not listed in the Oracle Fusion Middleware risk matrix. However,

since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the Critical Patch Update October 2020 to the Oracle Database components of Oracle Fusion Middleware products. For information on what patches need to be applied to your environments, refer to Critical Patch Update October 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2694898.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2017-5645	Identity Manager Connector	General and Misc (Apache Log4j)	Multiple	Yes	9.8	Network	Low	N
CVE-2018-11058	Oracle Access Manager	Web Server Plugin (RSA BSafe)	HTTPS	Yes	9.8	Network	Low	N
CVE-2017-9800	Oracle Data Integrator	Install, config, upgrade (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-10683	Oracle Endeca Information Discovery Integrator	Integrator ETL (dom4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10173	Oracle Endeca Information Discovery Studio	Endeca Server (xstream)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Enterprise Repository	Security Subsystem - 12c (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-8088	Oracle GoldenGate Application Adapters	Application Adapters (SLF4J)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-17531	Oracle GoldenGate Application Adapters	Build Request (jackson-databind)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P Re
CVE-2018-11058	Oracle GoldenGate Application Adapters	Security Service (RSA BSAFE)	HTTPS	Yes	9.8	Network	Low	N
CVE-2019-5482	Oracle HTTP Server	Web Listener (cURL)	TFTP	Yes	9.8	Network	Low	N
CVE-2020-10683	Oracle WebCenter Portal	Portlet Services (dom4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-2555	Oracle WebCenter Portal	Security Framework (Oracle Coherence)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10173	Oracle WebCenter Portal	Security Framework (xstream)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-17267	Oracle WebLogic Server	Centralized Thirdparty Jars (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-14882	Oracle WebLogic Server	Console	HTTP	Yes	9.8	Network	Low	N
CVE-2020-14841	Oracle WebLogic Server	Core	IIOP	Yes	9.8	Network	Low	N
CVE-2020-14825	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low	N
CVE-2020-14859	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low	N
CVE-2020-14879	BI Publisher	E-Business Suite - XDO	HTTP	No	8.5	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14880	BI Publisher	E-Business Suite - XDO	HTTP	No	8.5	Network	Low	L
CVE-2020-14842	BI Publisher	BI Publisher Security	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14784	Oracle BI Publisher	Mobile Service	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14815	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	Yes	8.2	Network	Low	N
CVE-2016-2510	Oracle Data Integrator	Jave APIs (BeanShell)	HTTP	Yes	8.1	Network	High	N
CVE-2020-3235	Management Pack for Oracle GoldenGate	Monitor (SNMP)	SNMP	No	7.7	Network	Low	L
CVE-2020-14864	Oracle Business Intelligence Enterprise Edition	Installation	HTTP	Yes	7.5	Network	Low	N
CVE-2020-1967	Oracle HTTP Server	SSL Module (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2020-14820	Oracle WebLogic Server	Core	IIOP, T3	Yes	7.5	Network	Low	N
CVE-2019-10097	Oracle HTTP Server	Core (Apache HTTP Server)	HTTP	No	7.2	Network	Low	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P Re
CVE-2020-14883	Oracle WebLogic Server	Console	HTTP	No	7.2	Network	Low	H
CVE-2020-14780	BI Publisher	BI Publisher Security	HTTP	Yes	7.1	Network	Low	N
CVE-2020-14843	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	Yes	7.1	Network	Low	N
CVE-2020-14766	Oracle Business Intelligence Enterprise Edition	Analytics Web Administration	HTTP	No	7.1	Network	Low	L
CVE-2020-9484	Oracle Managed File Transfer	MFT Runtime Server (Apache Tomcat)	None	No	7.0	Local	High	L
CVE-2020-14757	Oracle WebLogic Server	Web Services	HTTP	Yes	6.8	Network	High	N
CVE-2020-15389	Oracle Outside In Technology	Installation (OpenJPEG)	HTTP	Yes	6.5	Network	High	N
CVE-2020-1945	Oracle Business Process Management Suite	Runtime Engine (Apache Ant)	None	No	6.3	Local	High	L
CVE-2019-11358	BI Publisher	BI Publisher Security (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-11358	Oracle Business Process	Runtime Engine (jQuery)	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Management Suite							
CVE-2019-2904	Oracle Business Process Management Suite	Runtime Engine (Application Development Framework)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-11022	Oracle JDeveloper	ADF Faces (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-9281	Oracle WebCenter Portal	Blogs and Wikis (CKEditor)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-11022	Oracle WebLogic Server	Console (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-1951	Oracle Business Process Management Suite	Document Service (Apache Tika)	None	No	5.5	Local	Low	N
CVE-2020-13631	Oracle Outside In Technology	Installation (SQLite)	None	No	5.5	Local	Low	L
CVE-2020-9488	Oracle WebLogic Server	Core (Apache Log4j)	SMTPS	Yes	3.7	Network	High	N

Notes:

1. Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower.

Additional CVEs addressed are:

- The patch for CVE-2017-9800 also addresses CVE-2016-2167, CVE-2016-2168 and CVE-2016-8734
- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769
- The patch for CVE-2019-17267 also addresses CVE-2019-14540, CVE-2019-16335, CVE-2019-16942 and CVE-2019-16943
- The patch for CVE-2019-17531 also addresses CVE-2019-16943, CVE-2019-17267 and CVE-2019-20330
- The patch for CVE-2019-5482 also addresses CVE-2019-5435, CVE-2019-5436, CVE-2019-5443 and CVE-2019-5481
- The patch for CVE-2020-11022 also addresses CVE-2020-11023
- The patch for CVE-2020-13631 also addresses CVE-2020-11655, CVE-2020-11656, CVE-2020-13630, CVE-2020-13632, CVE-2020-15358 and CVE-2020-9327
- The patch for CVE-2020-1951 also addresses CVE-2020-1950

Oracle GraalVM Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle GraalVM. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-14803	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	5.3	Network	Low	None	

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Health Sciences Applications. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-1953	Oracle Healthcare Foundation	Self Service Analytics (Apache Commons Configuration)	HTTP	Yes	10.0	Network	Low	Non
CVE-2020-10683	Oracle Health Sciences Empirica Signal	User Interface (dom4j)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-2555	Oracle Healthcare Data Repository	Database Module (Oracle Coherence)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-11022	Oracle Healthcare Foundation	Admin Console (jQuery)	HTTP	Yes	6.1	Network	Low	Non

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Hospitality Applications. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-17638	Oracle Hospitality Guest Access	Base (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14807	Oracle Hospitality Suite8	WebConnect	HTTP	Yes	7.1	Network	Low	None
CVE-2020-9484	Oracle Hospitality Guest Access	Base (Apache Tomcat)	None	No	7.0	Local	High	Low
CVE-2020-14858	Oracle Hospitality OPERA 5 Property Services	Logging	HTTP	No	6.8	Network	Low	High
CVE-2020-14877	Oracle Hospitality OPERA 5 Property Services	Logging	HTTP	No	6.5	Network	Low	High
CVE-2020-14810	Oracle Hospitality Suite8	WebConnect	HTTP	Yes	5.4	Network	Low	None

Additional CVEs addressed are:

- The patch for CVE-2019-17638 also addresses CVE-2019-17632

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Hyperion. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-5482	Hyperion Essbase	Security and Provisioning	TFTP	Yes	9.8	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
		(cURL)						
CVE-2020-14854	Hyperion Infrastructure Technology	UI and Visualization	HTTP	No	6.1	Network	Low	Hi
CVE-2019-1547	Hyperion Essbase	Security and Provisioning (OpenSSL)	None	No	4.7	Local	High	Lo
CVE-2020-14768	Hyperion Analytic Provider Services	Smart View Provider	HTTP	No	4.3	Adjacent Network	High	Lo
CVE-2020-14767	Hyperion BI+	IQR-Foundation service	Multiple	No	4.2	Network	High	Hi
CVE-2020-14752	Hyperion Lifecycle Management	Shared Services	HTTP	No	4.2	Network	High	Hi
CVE-2020-14772	Hyperion Lifecycle Management	Shared Services	HTTP	No	4.2	Network	High	Hi
CVE-2020-14764	Hyperion Planning	Application Development Framework	HTTP	No	4.2	Network	High	Hi
CVE-2020-14770	Hyperion BI+	IQR-Foundation service	Multiple	No	2.0	Network	High	Hi

Additional CVEs addressed are:

- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563
- The patch for CVE-2019-5482 also addresses CVE-2019-5481

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Insurance Applications. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be

exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-9546	Oracle Insurance Policy Administration J2EE	Architecture (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-5398	Oracle Insurance Policy Administration J2EE	Admin Console (Spring Framework)	HTTP	Yes	7.5	Network	High	No
CVE-2020-11022	Oracle Insurance Insbridge Rating and Underwriting	Framework Administrator IBFA (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2020-9488	Oracle Insurance Insbridge Rating and Underwriting	Framework Administrator IBFA (Apache Log4j)	SMTPS	Yes	3.7	Network	High	No
CVE-2020-9488	Oracle Insurance Policy Administration J2EE	Architecture (Apache Log4j)	SMTPS	Yes	3.7	Network	High	No
CVE-2020-9488	Oracle Insurance Rules Palette	Architecture (Apache Log4j)	SMTPS	Yes	3.7	Network	High	No

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2019-11358 and CVE-2020-11023
- The patch for CVE-2020-9546 also addresses CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-9547 and CVE-2020-9548

Oracle Java SE Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Java SE. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14803	Java SE	Libraries	Multiple	Yes	5.3	Network	Low	None
CVE-2020-14792	Java SE, Java SE Embedded	Hotspot	Multiple	Yes	4.2	Network	High	None
CVE-2020-14781	Java SE, Java SE Embedded	JNDI	Multiple	Yes	3.7	Network	High	None
CVE-2020-14782	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.7	Network	High	None
CVE-2020-14797	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.7	Network	High	None
CVE-2020-14779	Java SE, Java SE	Serialization	Multiple	Yes	3.7	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	Embedded							
CVE-2020-14796	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.1	Network	High	None
CVE-2020-14798	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.1	Network	High	None

Notes:

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

2. Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 53 new security patches plus additional third party patches noted below for Oracle MySQL. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-8174	MySQL Cluster	Cluster: JS module (Node.js)	Multiple	Yes	9.8	Network	Low	Nor
CVE-2020-14878	MySQL Server	Server: Security: LDAP Auth	MySQL Protocol	No	8.0	Adjacent Network	Low	Lo
CVE-2020-13935	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	HTTPS	Yes	7.5	Network	Low	Nor
CVE-2020-1967	MySQL Workbench	Workbench: Security: Encryption (OpenSSL)	MySQL Workbench	Yes	7.5	Network	Low	Nor
CVE-2020-14828	MySQL Server	Server: DML	MySQL Protocol	No	7.2	Network	Low	Hig
CVE-2020-14775	MySQL Server	InnoDB	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14765	MySQL Server	Server: FTS	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14769	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14830	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14836	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-14846	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14800	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14827	MySQL Server	Server: Security: LDAP Auth	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-14760	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low	Hig
CVE-2020-1730	MySQL Workbench	MySQL Workbench (libssh)	MySQL Workbench	Yes	5.3	Network	Low	Nor
CVE-2020-14776	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14821	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14829	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14848	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14852	MySQL Server	Server: Charsets	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14814	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14789	MySQL Server	Server: FTS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14804	MySQL Server	Server: FTS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14812	MySQL Server	Server: Locking	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-14773	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14777	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14785	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14793	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14794	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14809	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14837	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14839	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14845	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14861	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14866	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14868	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14888	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14891	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14893	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14786	MySQL Server	Server: PS	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-14790	MySQL Server	Server: PS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14844	MySQL Server	Server: PS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14799	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14869	MySQL Server	Server: Security: LDAP Auth	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14672	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14870	MySQL Server	Server: X Plugin	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2020-14853	MySQL Cluster	Cluster: NDBCluster Plugin	Multiple	No	4.6	Network	Low	Lo
CVE-2020-14867	MySQL Server	Server: DDL	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2020-14873	MySQL Server	Server: Logging	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2020-14838	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.3	Network	Low	Lo
CVE-2020-14860	MySQL Server	Server: Security: Roles	MySQL Protocol	No	2.7	Network	Low	Hig
CVE-2020-14791	MySQL Server	InnoDB	MySQL Protocol	No	2.2	Network	High	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-14771	MySQL Server	Server: Security: LDAP Auth	MySQL Protocol	No	2.2	Network	High	Hig

Additional CVEs addressed are:

- The patch for CVE-2020-13935 also addresses CVE-2020-11996, CVE-2020-13934 and CVE-2020-9484
- The patch for CVE-2020-8174 also addresses CVE-2020-11080 and CVE-2020-8172

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- MySQL Cluster
  - Cluster: Configuration (dojo): CVE-2020-4051

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle PeopleSoft. 12 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2018-11058	PeopleSoft Enterprise PeopleTools	Weblogic (RSA BSafe)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-14865	PeopleSoft Enterprise SCM eSupplier Connection	eSupplier Connection	HTTP	No	8.1	Network	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2020-14795	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.5	Network	Low	None
CVE-2020-14778	PeopleSoft Enterprise HCM Global Payroll Core	Security	HTTP	No	6.3	Network	Low	Low
CVE-2020-14832	PeopleSoft Enterprise PeopleTools	Integration Broker	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14801	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14802	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11022	PeopleSoft Enterprise PeopleTools	PIA Core Technology (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14813	PeopleSoft Enterprise PeopleTools	PIA Grids	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11022	PeopleSoft Enterprise PeopleTools	Portal, Charting (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-1954	PeopleSoft Enterprise PeopleTools	Elastic Search (Apache CXF)	HTTP	Yes	5.3	Adjacent Network	High	None
CVE-2020-14806	PeopleSoft Enterprise PeopleTools	Query	HTTP	Yes	5.3	Network	Low	None
CVE-2020-9488	PeopleSoft Enterprise PeopleTools	Tools Admin API (Apache Log4j)	SMTPS	Yes	3.7	Network	High	None
CVE-2020-9488	PeopleSoft Enterprise PeopleTools	Updates Environment Mgmt	SMTPS	Yes	3.7	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
		(Apache Log4j)						
CVE-2020-14847	PeopleSoft Enterprise PeopleTools	Query	HTTP	No	2.7	Network	Low	High

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023

Oracle Policy Automation Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Policy Automation. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-11022	Oracle Policy Automation	Core (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11022	Oracle Policy Automation Connector for Siebel	Core (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11022	Oracle Policy Automation for Mobile Devices	Core (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-9488	Oracle Policy Automation	Core (Apache Log4j)	HTTP	Yes	3.7	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-9488	Oracle Policy Automation Connector for Siebel	Core (Apache Log4j)	HTTP	Yes	3.7	Network	High	None
CVE-2020-9488	Oracle Policy Automation for Mobile Devices	Core (Apache Log4j)	HTTP	Yes	3.7	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 28 new security patches for Oracle Retail Applications. 25 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VER		
					Base Score	Attack Vector	Atta Comp
CVE-2020-10683	Oracle Retail Order Broker	System Administration (dom4j)	HTTP	Yes	9.8	Network	Lo
CVE-2020-10683	Oracle Retail Price Management	Security (dom4j)	HTTP	Yes	9.8	Network	Lo
CVE-2020-9546	Oracle Retail Service Backbone	RSB kernel (jackson-databind)	HTTP	Yes	9.8	Network	Lo
CVE-2020-1945	Oracle Retail Back Office	Security (Apache Ant)	HTTP	Yes	9.1	Network	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VEF		
					Base Score	Attack Vector	Atta Comp
CVE-2020-1945	Oracle Retail Central Office	Security (Apache Ant)	HTTP	Yes	9.1	Network	Lo
CVE-2020-1945	Oracle Retail Integration Bus	RIB Kernal (Apache Ant)	HTTP	Yes	9.1	Network	Lo
CVE-2020-1945	Oracle Retail Point-of-Service	Security (Apache Ant)	HTTP	Yes	9.1	Network	Lo
CVE-2020-1945	Oracle Retail Returns Management	Security (Apache Ant)	HTTP	Yes	9.1	Network	Lo
CVE-2020-9410	Oracle Retail Order Broker	Order Broker Foundation (jasperreports_server)	HTTP	Yes	8.8	Network	Lo
CVE-2019-3740	Oracle Retail Assortment Planning	Application Core (RSA BSAFE Crypto-J)	HTTP	Yes	6.5	Network	Lo
CVE-2019-3740	Oracle Retail Integration Bus	RIB Kernal (RSA BSAFE Crypto-J)	HTTP	Yes	6.5	Network	Lo
CVE-2019-3740	Oracle Retail Predictive Application Server	RPAS Server (RSA BSAFE Crypto-J)	HTTP	Yes	6.5	Network	Lo
CVE-2019-3740	Oracle Retail Service Backbone	RSB kernel (RSA BSAFE Crypto-J)	HTTP	Yes	6.5	Network	Lo
CVE-2019-3740	Oracle Retail Xstore Point of Service	Xenvironment (RSA BSAFE Crypto-J)	HTTP	Yes	6.5	Network	Lo
CVE-2020-11022	Oracle Retail Back Office	Security (jQuery)	HTTP	Yes	6.1	Network	Lo
CVE-2020-11022	Oracle Retail Central Office	Security (jQuery)	HTTP	Yes	6.1	Network	Lo
CVE-2020-11022	Oracle Retail Customer Management	Segments (jQuery)	HTTP	Yes	6.1	Network	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VEF		
					Base Score	Attack Vector	Atta Comp
	and Segmentation Foundation						
CVE-2019-11358	Oracle Retail Point-of-Service	Mobile POS (jQuery)	HTTP	Yes	6.1	Network	Lo
CVE-2020-11022	Oracle Retail Returns Management	Security (jQuery)	HTTP	Yes	6.1	Network	Lo
CVE-2019-12415	Oracle Retail Order Broker	Store Connect (Apache POI)	none	No	5.5	Local	Lo
CVE-2020-9488	Oracle Retail Advanced Inventory Planning	AIP Dashboard (Apache Log4j)	HTTP	Yes	3.7	Network	Hig
CVE-2020-9488	Oracle Retail Assortment Planning	Application Core (Apache Log4j)	HTTP	Yes	3.7	Network	Hig
CVE-2020-9488	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Log4j)	HTTP	Yes	3.7	Network	Hig
CVE-2020-9488	Oracle Retail Integration Bus	RIB Kernal (Apache Log4j)	HTTP	Yes	3.7	Network	Hig
CVE-2020-9488	Oracle Retail Order Broker	Store Connect (Apache Log4j)	HTTP	Yes	3.7	Network	Hig
CVE-2020-9488	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache Log4j)	HTTP	Yes	3.7	Network	Hig
CVE-2020-14732	Oracle Retail Customer Management and Segmentation Foundation	Promotions	HTTP	No	3.1	Network	Hig
CVE-2020-14731	Oracle Retail Customer Management	Segment	HTTP	No	3.1	Network	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VER		
					Base Score	Attack Vector	Atta Comp
	and Segmentation Foundation						

Additional CVEs addressed are:

- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739
- The patch for CVE-2020-11022 also addresses CVE-2020-11023
- The patch for CVE-2020-1945 also addresses CVE-2017-5645
- The patch for CVE-2020-9410 also addresses CVE-2020-9409
- The patch for CVE-2020-9546 also addresses CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-9547 and CVE-2020-9548

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Siebel CRM. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2016-1000031	Siebel Apps - Marketing	Mktg/Email Mktg Stand-Alone (Apache Commons File Upload)	HTTP	Yes	9.8	Network	Low	
CVE-2019-10072	Siebel Apps - Marketing	Mktg/Campaign Mgmt (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11022	Siebel UI Framework	UIF Open UI (jQuery)	HTTP	Yes	6.1	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Supply Chain. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-1938	Oracle Agile PLM	Folders, Files & Attachments (Apache Tomcat)	AJP	Yes	9.8	Network	Low	Nc
CVE-2020-10683	Oracle Agile PLM	Security (dom4j)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2020-9484	Oracle Transportation Management	Install (Apache Tomcat)	AJP	No	7.0	Local	High	Lc
CVE-2020-11022	Oracle Agile Product Lifecycle Management for Process	Supplier Portal (jQuery)	HTTP	Yes	6.1	Network	Low	Nc

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023
- The patch for CVE-2020-1938 also addresses CVE-2019-17569, CVE-2020-13934, CVE-2020-13935, CVE-2020-1935 and CVE-2020-9484

Oracle Systems Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Systems. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14871	Oracle Solaris	Pluggable authentication module	Multiple	Yes	10.0	Network	Low	None
CVE-2020-14871	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	10.0	Network	Low	None
CVE-2019-11477	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (Linux Kernel)	TCP	Yes	7.5	Network	Low	None
CVE-2018-3693	Fujitsu M12-1, M12-2, M12-2S Servers	XCP Firmware (Kernel)	None	No	5.6	Local	High	Low
CVE-2020-14758	Oracle Solaris	Kernel	None	No	5.6	Local	Low	Low
CVE-2020-14754	Oracle Solaris	Filesystem	None	No	5.5	Local	Low	Low
CVE-2020-14818	Oracle Solaris	Utility	SSH	No	3.0	Network	High	Low
CVE-2020-14759	Oracle Solaris	Kernel	None	No	2.5	Local	High	Low

Notes:

1. This CVE is not exploitable for Solaris 11.1 and later releases, and ZFSSA 8.7 and later releases, thus the CVSS Base Score is 0.0.

Additional CVEs addressed are:

- The patch for CVE-2019-11477 also addresses CVE-2019-11478 and CVE-2019-11479
- The patch for CVE-2020-14871 for Oracle ZFS Storage Appliance Kit also addresses CVE-2019-18348, CVE-2020-3909, CVE-2020-10108, CVE-2020-12243, CVE-2020-13630, CVE-2020-14758 and CVE-2020-14759

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle Utilities Applications. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-10173	Oracle Utilities Framework	Common (xstream)	HTTP	Yes	9.8	Network	Low	None
CVE-2020-10683	Oracle Utilities Framework	General (dom4j)	HTTP	Yes	9.8	Network	Low	None
CVE-2020-1945	Oracle Utilities Framework	General (Apache Ant)	None	No	6.3	Local	High	Low
CVE-2020-14895	Oracle Utilities Framework	System Wide	HTTP	No	5.4	Network	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-9488	Oracle Utilities Framework	Common (Apache Log4j)	HTTP	Yes	3.7	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2020-1945 also addresses CVE-2017-5645

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Virtualization. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Ir
CVE-2020-14872	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2020-14881	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14884	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14885	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14886	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14889	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14892	Oracle VM VirtualBox	Core	None	No	5.5	Local	Low	Low