Oracle Critical Patch Update Advisory - July 2020

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. 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. Please refer to:

- Critical Patch Updates, Security Alerts and Bulletins for information about Oracle Security advisories.

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 444 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 July 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
Category Management Planning & Optimization, version 15.0.3	Retail Applications
Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0	Retail Applications

Affected Products and Versions	Patch Availability Document
Enterprise Manager Base Platform, versions 12.1.0.5, 13.3.0.0, 13.4.0.0	Enterprise Manager
Enterprise Manager for Fusion Middleware, version 12.1.0.5	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
GoldenGate Stream Analytics, versions prior to 19.1.0.0.1	Database
Hyperion Financial Close Management, version 11.1.2.4	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1-17.3	Oracle Construction and Engineerin Suite
JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.4.2	JD Edwards
JD Edwards EnterpriseOne Tools, versions prior to 9.2.3.3, prior to 9.2.4.2	JD Edwards
MySQL Client, versions 5.6.48 and prior, 5.7.30 and prior, 8.0.20 and prior	MySQL
MySQL Cluster, versions 7.3.29 and prior, 7.4.28 and prior, 7.5.18 and prior, 7.6.14 and prior, 8.0.20 and prior	MySQL
MySQL Connectors, versions 8.0.20 and prior	MySQL
MySQL Enterprise Monitor, versions 4.0.12 and prior, 8.0.20 and prior	MySQL
MySQL Server, versions 5.6.48 and prior, 5.7.30 and prior, 8.0.20 and prior	MySQL
Oracle Agile Engineering Data Management, version 6.2.1.0	Oracle Supply Chain Products
Oracle Application Express, versions 5.1-19.2	Database
Oracle Application Testing Suite, versions 13.2.0.1, 13.3.0.1	Enterprise Manager
Oracle AutoVue, version 21.0	Oracle Supply Chain Products
Oracle Banking Enterprise Collections, versions 2.7.0-2.9.0	Oracle Banking Platform
Oracle Banking Payments, versions 14.1.0-14.4.0	Oracle Financial Services Applicatio
Oracle Banking Platform, versions 2.4.0-2.10.0	Oracle Banking Platform
Oracle Berkeley DB, versions prior to 6.1.38, prior to 18.1.40	Berkeley DB
Oracle BI Publisher, versions 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 Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Commerce Guided Search / Oracle Commerce Experience Manager, versions 11.0, 11.1, 11.2, prior to 11.3.1	Oracle Commerce
Oracle Commerce Platform, versions 11.1, 11.2, prior to 11.3.1	Oracle Commerce
Oracle Commerce Service Center, versions 11.1, 11.2, prior to 11.3.1	Oracle Commerce
Oracle Communications Analytics, version 12.1.1	Oracle Communications Analytics
Oracle Communications Billing and Revenue Management, versions 7.5.0.23.0, 12.0.0.3.0	Oracle Communications Billing and Revenue Management
Oracle Communications BRM - Elastic Charging Engine, versions 11.3, 12.0	Oracle Communications BRM - Elas Charging Engine
Oracle Communications Contacts Server, version 8.0.0.4.0	Oracle Communications Contacts Server
Oracle Communications Convergence, versions 3.0.1.0-3.0.2.1	Oracle Communications Convergen
Oracle Communications Diameter Signaling Router (DSR), versions 8.0-8.4	Oracle Communications Diameter Signaling Router
Oracle Communications Element Manager, versions 8.1.1, 8.2.0, 8.2.1	Oracle Communications Element Manager
Oracle Communications Evolved Communications Application Server, version 7.1	Oracle Communications Evolved Communications Application Server
Oracle Communications Instant Messaging Server, version 10.0.1.4.0	Oracle Communications Instant Messaging Server
Oracle Communications Interactive Session Recorder, versions 6.1-6.4	Oracle Communications Interactive Session Recorder
Oracle Communications IP Service Activator, versions 7.3.0, 7.4.0	Oracle Communications IP Service Activator
Oracle Communications LSMS, versions 13.0-13.3	Oracle Communications LSMS
Oracle Communications Messaging Server, versions 8.0.2, 8.1.0	Oracle Communications Messaging Server
Oracle Communications MetaSolv Solution, version 6.3.0	Oracle Communications MetaSolv Solution
Oracle Communications Network Charging and Control, versions 6.0.1, 12.0.0-12.0.3	Oracle Communications Network Charging and Control
Oracle Communications Network Integrity, versions 7.3.2-7.3.6	Oracle Communications Network Integrity
Oracle Communications Operations Monitor, versions 3.4, 4.1-4.3	Oracle Communications Operations Monitor
Oracle Communications Order and Service Management, versions 7.3, 7.4	Oracle Communications Order and Service Management

Affected Products and Versions	Patch Availability Document
Oracle Communications Services Gatekeeper, versions 6.0, 6.1, 7.0	Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller, versions 8.1.0, 8.2.0, 8.3.0	Oracle Communications Session Bo Controller
Oracle Communications Session Report Manager, versions 8.1.1, 8.2.0, 8.2.1	Oracle Communications Session Re Manager
Oracle Communications Session Route Manager, versions 8.1.1, 8.2.0, 8.2.1	Oracle Communications Session Ro Manager
Oracle Configuration Manager, version 12.1.2.0.6	Enterprise Manager
Oracle Configurator, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Data Masking and Subsetting, versions 13.3.0.0, 13.4.0.0	Enterprise Manager
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c, [Spatial Studio] prior to 19.2.1	Database
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.9	E-Business Suite
Oracle Endeca Information Discovery Studio, version 3.2.0	Fusion Middleware
Oracle Enterprise Communications Broker, versions 3.0.0-3.2.0	Oracle Enterprise Communications Broker
Oracle Enterprise Repository, version 11.1.1.7.0	Fusion Middleware
Oracle Enterprise Session Border Controller, versions 8.1.0, 8.2.0, 8.3.0	Oracle Enterprise Session Border Controller
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.0	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Compliance Regulatory Reporting, versions 8.0.6-8.0.8	Oracle Financial Services Compliand Regulatory Reporting
Oracle Financial Services Lending and Leasing, versions 12.5.0, 14.1.0-14.8.0	Oracle Financial Services Applicatio
Oracle Financial Services Liquidity Risk Management, version 8.0.6	Oracle Financial Services Liquidity R Management
Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.6-8.0.8	Oracle Financial Services Loan Loss Forecasting and Provisioning
Oracle Financial Services Market Risk Measurement and Management, versions 8.0.6, 8.0.8	Oracle Financial Services Market Ris Measurement and Management
Oracle Financial Services Regulatory Reporting for De Nederlandsche Bank, version 8.0.4	Oracle Financial Services Regulatory Reporting for De Nederlandsche Ba
Oracle FLEXCUBE Investor Servicing, versions 12.1.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0	Oracle Financial Services Applicatio
Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0	Oracle Financial Services Applicatio

Affected Products and Versions	Patch Availability Document
Oracle Fusion Middleware MapViewer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Global Lifecycle Management/OPatch, versions prior to 12.2.0.1.20	Global Lifecycle Management
Oracle GoldenGate, versions prior to 19.1.0.0.0	Database
Oracle GraalVM Enterprise Edition, versions 19.3.2, 20.1.0	Oracle GraalVM Enterprise Edition
Oracle Health Sciences Empirica Inspections, version 1.0.1.2	Health Sciences
Oracle Health Sciences Empirica Signal, version 7.3.3	Health Sciences
Oracle Healthcare Master Person Index, version 4.0.2	Health Sciences
Oracle Healthcare Translational Research, versions 3.2.1, 3.3.1, 3.3.2, 3.4.0	Health Sciences
Oracle Help Technologies, versions 11.1.1.9.0, 12.2.1.3.0	Fusion Middleware
Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1	Oracle Hospitality Guest Access
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle Hyperion BI+, version 11.1.2.4	Fusion Middleware
Oracle iLearning, versions 6.1, 6.1.1	iLearning
Oracle Insurance Accounting Analyzer, versions 8.0.6-8.0.9	Oracle Insurance Accounting Analyz
Oracle Insurance Data Gateway, version 1.0	Oracle Insurance Applications
Oracle Insurance Policy Administration J2EE, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0, 11.2.0	Oracle Insurance Applications
Oracle Insurance Rules Palette, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0, 11.2.0	Oracle Insurance Applications
Oracle Java SE, versions 7u261, 8u251, 11.0.7, 14.0.1	Java SE
Oracle Java SE Embedded, version 8u251	Java SE
Oracle Outside In Technology, versions 8.5.4, 8.5.5	Fusion Middleware
Oracle Rapid Planning, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Real User Experience Insight, version 13.3.1.0	Enterprise Manager
Oracle Retail Assortment Planning, versions 15.0, 15.0.3, 16.0, 16.0.3	Retail Applications
Oracle Retail Bulk Data Integration, versions 15.0, 16.0	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, version 18.0	Retail Applications
Oracle Retail Data Extractor for Merchandising, versions 1.9, 1.10, 18.0	Retail Applications

Affected Products and Versions	Patch Availability Document
Oracle Retail Extract Transform and Load, version 19.0	Retail Applications
Oracle Retail Financial Integration, versions 15.0, 16.0	Retail Applications
Oracle Retail Fusion Platform, version 5.5	Retail Applications
Oracle Retail Integration Bus, versions 15.0, 15.0.3, 16.0, 16.0.3	Retail Applications
Oracle Retail Invoice Matching, version 16.0	Retail Applications
Oracle Retail Item Planning, version 15.0.3	Retail Applications
Oracle Retail Macro Space Optimization, version 15.0.3	Retail Applications
Oracle Retail Merchandise Financial Planning, version 15.0.3	Retail Applications
Oracle Retail Merchandising System, versions 15.0.3, 16.0.2, 16.0.3	Retail Applications
Oracle Retail Order Broker, version 15.0	Retail Applications
Oracle Retail Predictive Application Server, versions 14.0.3, 14.1.3, 15.0.3, 16.0.3	Retail Applications
Oracle Retail Regular Price Optimization, versions 15.0.3, 16.0.3	Retail Applications
Oracle Retail Replenishment Optimization, version 15.0.3	Retail Applications
Oracle Retail Sales Audit, version 14.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Size Profile Optimization, version 15.0.3	Retail Applications
Oracle Retail Store Inventory Management, versions 14.0.4, 14.1.3, 15.0.3, 16.0.3	Retail Applications
Oracle Retail Xstore Point of Service, versions 7.1, 15.0, 16.0, 17.0, 18.0, 19.0	Retail Applications
Oracle SD-WAN Aware, versions 8.0, 8.1, 8.2	Oracle SD-WAN Aware
Oracle SD-WAN Edge, versions 8.0, 8.1, 8.2, 9.0	Oracle SD-WAN Edge
Oracle Security Service, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Solaris, version 11	Systems
Oracle TimesTen In-Memory Database, versions prior to 18.1.2.1.0	Database
Oracle Transportation Management, versions 6.3.7, 6.4.3	Oracle Supply Chain Products
Oracle Unified Directory, versions 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Utilities Framework, versions 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 5.2.44, prior to 6.0.24, prior to 6.1.12	Virtualization

Affected Products and Versions	Patch Availability Document
Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Sites, versions 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 FIN Expenses, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Global Payroll Switzerland, version 9.2	PeopleSoft
PeopleSoft Enterprise HRMS, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft
Primavera Gateway, versions 16.2.0-16.2.11, 17.12.0-17.12.7, 18.8.0-18.8.9, 19.12.0-19.12.4	Oracle Construction and Engineering Suite
Primavera P6 Enterprise Project Portfolio Management, versions 16.1.0.0-16.2.20.1, 17.1.0.0-17.12.17.1, 18.1.0.0-18.8.19, 19.12.0-19.12.6	Oracle Construction and Engineering Suite
Primavera Portfolio Management, versions 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0, 19.0.0.0	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12, [Mobile App] prior to 20.6	Oracle Construction and Engineering Suite
Siebel Applications, versions 2.20.5 and prior, 20.6 and prior	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:

- Abdullah Alzahrani: CVE-2020-14554, CVE-2020-14635
- Alessandro Bosco of TIM S.p.A: CVE-2020-14690
- Alexander Kornbrust of Red Database Security: CVE-2020-2984
- Alves Christopher (Telecom Nancy): CVE-2020-14550, CVE-2020-14553, CVE-2020-14623
- Ammarit Thongthua of Secure D Center Cybersecurity Team: CVE-2020-14558, CVE-2020-14564
- Andrej Simko of Accenture: CVE-2020-14534, CVE-2020-14555, CVE-2020-14590, CVE-2020-14657, CVE-2020-14658, CVE-2020-14659, CVE-2020-14660, CVE-2020-14661, CVE-2020-14665, CVE-2020-14666, CVE-2020-14667, CVE-2020-14679, CVE-2020-14688
- Antonin B. of NCIA / NCSC: CVE-2020-14610
- Arseniy Sharoglazov of Positive Technologies: CVE-2020-14622

- Artur Wojtkowski and CQURE Team: CVE-2020-14617, CVE-2020-14618
- Billy Cody of Context Information Security: CVE-2020-14595
- Bui Duong from Viettel Cyber Security: CVE-2020-14611
- CERT/CC: CVE-2020-14558
- Chathura Abeydeera of Deloitte Risk Advisory Pty Ltd: CVE-2020-14531
- Chi Tran: CVE-2020-14534, CVE-2020-14716, CVE-2020-14717
- Conor McErlane working with Trend Micro's Zero Day Initiative: CVE-2020-14628
- Damian Bury: CVE-2020-14546
- Edoardo Predieri of TIM S.p.A: CVE-2020-14690
- Emad Al-Mousa of Saudi Aramco: CVE-2020-2969, CVE-2020-2978
- Fabio Minarelli of TIM S.p.A: CVE-2020-14690
- Filip Ceglik: CVE-2020-14560, CVE-2020-14565
- Forum Bhayani: CVE-2020-14592
- Francesco Russo of TIM S.p.A: CVE-2020-14690
- Giovanni Delvecchio of Almaviva Security Assessment Team: CVE-2020-14607, CVE-2020-14608
- Hangfan Zhang: CVE-2020-14575, CVE-2020-14654
- Hugo Santiago dos Santos: CVE-2020-14613
- Johannes Kuhn: CVE-2020-14556
- Julien Zhan (Telecom Nancy): CVE-2020-14550, CVE-2020-14553, CVE-2020-14623
- kdot working with Trend Micro Zero Day Initiative: CVE-2020-14664
- Khuyen Nguyen of secgit.com: CVE-2020-14668, CVE-2020-14669, CVE-2020-14670, CVE-2020-14671, CVE-2020-14681, CVE-2020-14682, CVE-2020-14686
- Kingkk: CVE-2020-14642, CVE-2020-14644
- Kritsada Sunthornwutthikrai of Secure D Center Cybersecurity Team: CVE-2020-14558, CVE-2020-14564
- Larry W. Cashdollar: CVE-2020-14724
- Lionel Debroux: CVE-2020-2981
- Luca Di Giuseppe of TIM S.p.A: CVE-2020-14690
- Lucas Leong of Trend Micro Zero Day Initiative: CVE-2020-14646, CVE-2020-14647, CVE-2020-14648, CVE-2020-14649, CVE-2020-14650, CVE-2020-14673, CVE-2020-14674, CVE-2020-14694, CVE-2020-14695, CVE-2020-14703, CVE-2020-14704
- lufei of Tencent Force: CVE-2020-14645
- Lukas Braune of Siemens: CVE-2019-8457

- Lukasz Mikula: CVE-2020-14541
- Lukasz Rupala of ING Tech Poland: CVE-2020-14552
- Maoxin Lin of Dbappsecurity Team: CVE-2020-14645, CVE-2020-14652
- Marco Marsala: CVE-2020-14559
- Markus Loewe: CVE-2020-14583
- Markus Wulftange of Code White GmbH: CVE-2020-14644, CVE-2020-14645, CVE-2020-14687
- Massimiliano Brolli of TIM S.p.A: CVE-2020-14690
- Mateusz Dabrowski: CVE-2020-14584, CVE-2020-14585
- Maxime Escourbiac of Michelin CERT: CVE-2020-14719, CVE-2020-14720
- Mohamed Fadel: CVE-2020-14601, CVE-2020-14602, CVE-2020-14603, CVE-2020-14604, CVE-2020-14605
- Ntears of Chaitin Security Team: CVE-2020-14645, CVE-2020-14652
- Owais Zaman of Sabic: CVE-2020-14551
- Pavel Cheremushkin: CVE-2020-14713
- Philippe Antoine (Telecom Nancy): CVE-2020-14550, CVE-2020-14553, CVE-2020-14623
- Philippe Arteau of GoSecure: CVE-2020-14577
- Preeyakorn Keadsai of Secure D Center Cybersecurity Team: CVE-2020-14558, CVE-2020-14564
- Przemyslaw Nowakowski: CVE-2020-2977
- Quynh Le of VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2020-14625
- r00t4dm from A-TEAM of Legendsec at Qi'anxin Group: CVE-2020-14636, CVE-2020-14637, CVE-2020-14638, CVE-2020-14639, CVE-2020-14640, CVE-2020-14645, CVE-2020-14652
- Reno Robert working with Trend Micro Zero Day Initiative: CVE-2020-14629, CVE-2020-14675, CVE-2020-14676, CVE-2020-14677
- Roberto Suggi Liverani of NCIA / NCSC: CVE-2020-14610
- Roger Meyer: CVE-2020-2513, CVE-2020-2971, CVE-2020-2972, CVE-2020-2973, CVE-2020-2974, CVE-2020-2975, CVE-2020-2976
- Roman Shemyakin: CVE-2020-14621
- Rui Zhong: CVE-2020-14575, CVE-2020-14654
- Saeed Shiravi: CVE-2020-14548
- Shimizu Kawasaki of Asiainfo-sec of CSS Group: CVE-2020-14645, CVE-2020-14652
- Spyridon Chatzimichail of OTE Hellenic Telecommunications Organization S.A.: CVE-2020-14532, CVE-2020-14533

- Suthum Thitiananpakorn: CVE-2020-14569
- Ted Raffle of rapid7.com: CVE-2020-14535, CVE-2020-14536
- Tomasz Stachowicz: CVE-2020-14570, CVE-2020-14571
- Trung Le: CVE-2020-14534, CVE-2020-14716, CVE-2020-14717
- Tuan Anh Nguyen of Viettel Cyber Security: CVE-2020-14598, CVE-2020-14599
- Vijayakumar Muniraj of CybersecurityWorks Research Labs: CVE-2020-14723
- Yaoguang Chen of Ant-financial Light-Year Security Lab: CVE-2020-14654, CVE-2020-14725
- Yongheng Chen: CVE-2020-14575, CVE-2020-14654
- ZeddYu Lu of StarCross Tech: CVE-2020-14588, CVE-2020-14589
- Zhao Xin Jun: CVE-2020-14652
- Zhongcheng Li (CK01) from Zero-dayits Team of Legendsec at Qi'anxin Group: CVE-2020-14711, CVE-2020-14712
- Ziming Zhang from Codesafe Team of Legendsec at Qi'anxin Group: CVE-2020-14707, CVE-2020-14714, CVE-2020-14715
- Ziming Zhang from Codesafe Team of Legendsec at Qi'anxin Group working with Trend Micro Zero Day Initiative: CVE-2020-14698, CVE-2020-14699, CVE-2020-14700
- Zouhair Janatil-Idrissi (Telecom Nancy): CVE-2020-14550, CVE-2020-14553, CVE-2020-14623

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.:

- Alexander Kornbrust of Red Database Security [10 reports]
- Cao Linhong of Sangfor Furthereye Security Team
- Chi Tran [2 reports]
- Fatih Çelik
- James Nichols of 80/20 Labs
- lufei of Tencent Force
- Maoxin Lin of Dbappsecurity Team

- Marc Fielding of Google
- Markus Loewe [2 reports]
- r00t4dm from A-TEAM of Legendsec at Qi'anxin Group
- Ryan Gerstenkorn
- Saeid Tizpaz Niari
- Shimizu Kawasaki of Asiainfo-sec of CSS Group
- Trung Le [2 reports]
- Venustech ADLab
- Yu Wang of BMH Security Team [2 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:

- 0xd0ff9 aka Bao Bui
- 1ZRR4H aka Germán Fernández
- @ngkogkos hunt4p1zza
- Abdulkadir Mutlu
- Abdullah Mohamed
- Abhinav P
- Aditra Andri Laksana
- Ahmed Moustafa
- Alfie Njeru (emenalf)
- Aman Deep Singh Chawla
- Anas Rahmani
- Anat Bremler-Barr
- Anis Azzi
- Anon Venus
- Ansar Uddin Anan

- Ben Passmore
- Celal Erdik of Ebruu Tech Limited
- Chirag Prajapati
- Dave Altena
- Dhamu Harker
- Dhiral Patel
- Dhiren Kumar Pradhan
- Elmonzer Kamaleldin of Monzer Kamal
- HackersEra VMS [2 reports]
- Hamza Megahed
- Harpreet Singh of Pyramid Cyber Security & Forensic Pvt Ltd
- Harry The DevOps Guy
- Ilyas Orak
- Jagdish Bharucha
- Jatin Saini
- Jeremy Lindsey of Burns & McDonnell [2 reports]
- Jin DanLong
- Josue Acevedo Maldonado
- Ken Nevers
- Kishore Hariram [2 reports]
- Last Light [2 reports]
- Lior Shafir
- Luciano Anezin
- Maayan Amid of Orca Security
- Magrabur Alam Sofily
- Matthijs R. Koot [2 reports]
- Mayur Gupta
- Meridian Miftari
- Moaied Nagi Hassan (Moonlight)
- Mohit Khemchandani
- Muhammad Abdullah
- Naveen Kumar

- Ome Mishra
- Prathmesh Lalingkar
- Pratish Bhansali
- Prince Achillies
- Pritam Mukherjee
- Rajesh Patil
- Raphael Karger
- Ricardo Iramar dos Santos
- Ridvan Erbas
- Roger Meyer
- rootme34
- Russell Muetzelfeldt of Flybuys
- Saad Zitouni
- Sajid Ali
- Sam Jadali
- Sarath Kumar (Kadavul)
- Saurabh Dilip Mhatre
- Severus of VietSunshine Security Engineering Team
- Shailesh Kumar
- Shubham Khadgi
- Sipke Mellema
- Siva Pathela
- Smii Mondher
- Srinivas M
- Tinu Tomy
- Tony Marcel Nasr [2 reports]
- Tuatnh
- Tushar Bhardwaj
- Ujjwal Tyagi
- Valentin Virtejanu of Lifespan
- Victor Gevers
- Viet Nguyen [2 reports]

- Virendra Tiwari
- Vishal Ajwani
- Vlad Staricin
- Yehuda Afek
- Youssef A. Mohamed aka GeneralEG
- Zubin

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:

- 20 October 2020
- 19 January 2021
- 20 April 2021
- 20 July 2021

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - July 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-1	Rev 8. Updated CVSS score of CVE-2020-14564.

Date	Note
2020-August-31	Rev 7. Credit Statement Update.
2020-August-3	Rev 6. Credit Statement Update.
2020-July-27	Rev 5. Credit Statement Update.
2020-July-24	Rev 4. Affected version number changes to CVE-2020-14701 & CVE-2020-14606
2020-July-23	Rev 3. Added entry for CVE-2020-14725 in MySQL Risk Matrix. The fix was included i patches already released but was inadvertently not documented.
2020-July-20	Rev 2. Credit Statement Update.
2020-July-14	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 27 new security patches for the Oracle Database Products divided as follows:

- 19 new security patches for Oracle Database Server.
- 3 new security patches for Oracle Berkeley DB.
- 1 new security patch for Oracle Global Lifecycle Management.
- 3 new security patches for Oracle GoldenGate.
- 1 new security patch for Oracle TimesTen In-Memory Database.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 19 new security patches for the Oracle Database Server. 1 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 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2016-1000031	MapViewer (Apache Commons FileUpload)	Valid User Account	HTTP	No	8.8	Network	Low	Low

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2968	Java VM	Create Session, Create Procedure	Multiple	No	8.0	Network	High	Low
CVE-2016-9843	Core RDBMS (zlib)	Create Session	Oracle Net	No	7.2	Network	Low	High
CVE-2020-2969	Data Pump	DBA role account	Oracle Net	No	6.6	Network	High	High
CVE-2020-8112	GeoRaster (OpenJPG)	Create Session	Oracle Net	No	5.7	Network	Low	Low
CVE-2020-2513	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-2971	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-2972	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-2973	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-2974	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-2976	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2020-2975	Oracle Application Express	SQL Workshop	HTTP	No	5.4	Network	Low	Low
CVE-2019-17569	Workload Manager (Apache Tomcat)	None	HTTP	Yes	4.8	Network	High	None

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2977	Oracle Application Express	Valid User Account	HTTP	No	4.6	Network	Low	Low
CVE-2020-2978	Oracle Database - Enterprise Edition	DBA role account	Oracle Net	No	4.1	Network	Low	High
CVE-2019-13990	MapViewer (Terracotta Quartz Scheduler, Apache Batik, Google Guava)	Local Logon	None	No	0.0	Local	Low	Low
CVE-2018-18314	Oracle Database (Perl)	Local Logon	None	No	0.0	Local	High	High
CVE-2019-10086	Spatial Studio (Apache Commons Beanutils)	Local Logon	None	No	0.0	Local	Low	Low
CVE-2019-16943	TFA (jackson-databind)	Local Logon	None	No	0.0	Local	High	High

Notes:

1. MapViewer is not deployed with a default installation. To use MapViewer the customer needs to re-deploy MapViewer EAR file into Oracle WebLogic Server.

2. The CVE-2019-13990 and other CVEs listed for this patch are not exploitable in the context of Oracle Spatial and Graph MapViewer product, thus the CVSS score is 0.0.

3. None of the CVEs listed against this row are exploitable in the context of Oracle Database, thus the CVSS score is 0.0.

4. The CVE-2019-10086 is not exploitable in the context of Oracle Spatial Studio product, thus the CVSS score is 0.0.

5. The CVE-2019-16943 and additional CVEs addressed by this patch are not exploitable in the context of Oracle TFA, thus the CVSS score for TFA patch for this issue is is 0.0.

Additional CVEs addressed are below:

- The patch for CVE-2016-9843 also addresses CVE-2016-9840, CVE-2016-9841 and CVE-2016-9842.
- The patch for CVE-2018-18314 also addresses CVE-2015-8607, CVE-2015-8608, CVE-2016-2381, CVE-2017-12814, CVE-2017-12837, CVE-2017-12883, CVE-2018-12015, CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-6797, CVE-2018-6798 and CVE-2018-6913.
- The patch for CVE-2019-13990 also addresses CVE-2018-10237 and CVE-2018-8013.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.
- The patch for CVE-2019-17569 also addresses CVE-2020-1935 and CVE-2020-1938.
- The patch for CVE-2020-8112 also addresses CVE-2016-1923, CVE-2016-1924, CVE-2016-3183, CVE-2016-4796, CVE-2016-4797, CVE-2016-8332, CVE-2016-9112 and CVE-2020-6851.

Oracle Berkeley DB Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Berkeley DB. 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#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2017-10140	Data Store	None	None	No	7.3	Local	Low	Low	Re
CVE-2020-2981	Data Store	None	None	No	7.0	Local	High	None	Re
CVE-2019-8457	Data Store (SQLite)	None	TCP	No	0.0	Network	Low	None	Re

Notes:

1. The CVE-2019-8457 is not exploitable in the context of Oracle Berkeley DB product, thus the CVSS score is 0.0.

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Global Lifecycle Management. This vulnerability is not remotely exploitable without authentication, i.e., may

not 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 VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2020-9546	Oracle Global Lifecycle Management/OPatch	Patch Installer (jackson-databind)	None	No	0.0	Local	Low

Notes:
1. None of the CVEs listed against this row are exploitable in the Oracle Global Lifecycle Management product, thus the CVSS score is 0.0.

Additional CVEs addressed are below:
- The patch for CVE-2020-9546 also addresses 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-2020-9547 and CVE-2020-9548.

Oracle GoldenGate Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle GoldenGate. 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14705	Oracle GoldenGate	Process Management	TCP	Yes	9.6	Adjacent Network	Low	None
CVE-2019-0222	GoldenGate Stream Analytics	Security (ActiveMQ)	TCP	No	6.5	Network	Low	Low
CVE-2019-14379	GoldenGate Stream Analytics	Security / Application Adapters (jackson-databind,	None	No	0.0	Local	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
		SLF4J, ZooKeeper, Apache Spark)						

Notes:
1. CVE-2019-14379 and other CVEs addressed by these patches are not exploitable in the Oracle GoldenGate product, thus the CVSS score is 0.0.

Additional CVEs addressed are below:
- The patch for CVE-2019-14379 also addresses CVE-2016-5017, CVE-2017-5637, CVE-2018-17190, CVE-2018-8012, CVE-2018-8088, CVE-2019-0201, CVE-2019-12086, CVE-2019-12384, CVE-2019-12814, CVE-2019-14439 and CVE-2019-14893.

Oracle TimesTen In-Memory Database Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle TimesTen In-Memory Database. This vulnerability is not remotely exploitable without authentication, i.e., may not 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-2018-18314	Oracle TimesTen In-Memory Database	Doc, EM Plug-in (Perl)	OracleNet	No	0.0	Network	Low	Low	

Notes:
1. None of the CVEs listed against this row are exploitable in the context of Oracle Database, thus the CVSS score is 0.0.

Additional CVEs addressed are below:
- The patch for CVE-2018-18314 also addresses CVE-2015-8607, CVE-2015-8608, CVE-2016-2381, CVE-2017-12814, CVE-2017-12837, CVE-2017-12883, CVE-2018-12015, CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-6797, CVE-2018-6798 and CVE-2018-6913.

Oracle Commerce Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Commerce. 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-2020-14536	Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Workbench	HTTP	Yes	7.4	Network	High	None
CVE-2020-14535	Oracle Commerce Service Center	Commerce Service Center	HTTP	Yes	7.4	Network	High	None
CVE-2020-14532	Oracle Commerce Platform	Dynamo Application Framework	HTTP	Yes	4.7	Network	Low	None
CVE-2020-14533	Oracle Commerce Platform	Dynamo Application Framework	HTTP	No	3.5	Network	Low	High

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 60 new security patches for Oracle Communications Applications. 46 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-2020-14701	Oracle SD-WAN Aware	User Interface	HTTP	Yes	10.0	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2020-14606	Oracle SD-WAN Edge	User Interface	HTTP	Yes	10.0	Network	Low
CVE-2018-11058	Oracle Communications Analytics	Platform (RSA BSAFE)	Multiple	Yes	9.8	Network	Low
CVE-2019-16943	Oracle Communications Billing and Revenue Management	Business Operation Center, Billing Care (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications Contacts Server	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2020-9546	Oracle Communications Contacts Server	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2020-1938	Oracle Communications Element Manager	Core (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low
CVE-2020-9546	Oracle Communications Evolved Communications Application Server	Session Design Center, Universal Data Recorder (jackson-databind)	Multiple	Yes	9.8	Network	Low
CVE-2020-1938	Oracle Communications Instant Messaging Server	Installation (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low
CVE-2020-9546	Oracle Communications Instant Messaging Server	Presence API (jackson-databind)	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2019-13990	Oracle Communications IP Service Activator	Netwok Processor Configuration Management (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low
CVE-2020-11656	Oracle Communications Network Charging and Control	Data Access Pack (SQLite)	HTTP	Yes	9.8	Network	Low
CVE-2019-2729	Oracle Communications Network Integrity	Integration (Oracle WebLogic Server)	HTTP	Yes	9.8	Network	Low
CVE-2019-2904	Oracle Communications Network Integrity	User Interface (Application Development Framework)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Communications Network Integrity	Cartridge Management (Log4j)	Multiple	Yes	9.8	Network	Low
CVE-2020-7060	Oracle Communications Diameter Signaling Router (DSR)	Platform (PHP)	HTTP	Yes	9.1	Network	Low
CVE-2020-1945	Oracle Communications MetaSolv Solution	Online Help (Apache Ant)	HTTP	Yes	9.1	Network	Low
CVE-2018-1258	Oracle Communications Network Integrity	Core (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2020-9546	Oracle Communications Network	Installer (jackson-databind)	None	No	8.4	Local	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
	Charging and Control						
CVE-2020-14580	Oracle Communications Session Border Controller	System Admin	SSH	No	8.2	Network	Low
CVE-2016-1181	Oracle Communications Network Integrity	MSS Integration Cartridge (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2017-0861	Oracle Communications LSMS	Kernel	None	No	7.8	Local	Low
CVE-2020-1945	Oracle Communications Order and Service Management	Installer (Apache Ant)	None	No	7.7	Local	Low
CVE-2020-5398	Oracle Communications BRM - Elastic Charging Engine	Orchestration (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2019-17359	Oracle Communications Convergence	S/MIME Configuration (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2020-5398	Oracle Communications Element Manager	Core (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2019-0227	Oracle Communications Network Integrity	Adapters (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-16056	Oracle Communications Operations Monitor	VSP implementing webserver (Python)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2019-0227	Oracle Communications Order and Service Management	Installer, CMWS, CMT (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2020-5398	Oracle Communications Session Report Manager	Core (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2020-5398	Oracle Communications Session Route Manager	Core (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2020-14630	Oracle Enterprise Session Border Controller	File Upload	HTTP	No	7.5	Network	Low
CVE-2019-10193	Oracle Communications Operations Monitor	FDP, VSP Login, Packet Inspector (Redis)	HTTP	No	7.2	Network	Low
CVE-2019-12423	Oracle Communications Element Manager	REST API (Apache CXF)	HTTP	No	6.5	Network	Low
CVE-2019-12423	Oracle Communications Session Report Manager	REST API (Apache CXF)	HTTP	No	6.5	Network	Low
CVE-2019-12423	Oracle Communications Session Route Manager	REST API (Apache CXF)	HTTP	No	6.5	Network	Low
CVE-2020-14721	Oracle Enterprise Communications Broker	WebGUI	HTTP	No	6.3	Network	Low
CVE-2020-11022	Oracle Communications Analytics	Platform (jQuery)	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2020-11022	Oracle Communications Element Manager	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-1941	Oracle Communications Element Manager	Workorders (Apache ActiveMQ)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Communications Interactive Session Recorder	Dashboard (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-17091	Oracle Communications Network Integrity	Core (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Communications Operations Monitor	Mediation Engine, Dashboard, Grapahs, Calls (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Communications Session Report Manager	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-1941	Oracle Communications Session Report Manager	Workorders (Apache ActiveMQ)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Communications Session Route Manager	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-1941	Oracle Communications Session Route Manager	Workorders (Apache ActiveMQ)	HTTP	Yes	6.1	Network	Low
CVE-2020-14563	Oracle Enterprise	WebGUI	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
	Communications Broker						
CVE-2020-14722	Oracle Enterprise Communications Broker	WebGUI	HTTP	Yes	5.8	Network	High
CVE-2018-3639	Oracle Communications LSMS	Kernel	None	No	5.5	Local	Low
CVE-2020-1951	Oracle Communications Messaging Server	Security (Apache Tika)	None	No	5.5	Local	Low
CVE-2019-10247	Oracle Communications Analytics	Platform (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2020-1934	Oracle Communications Element Manager	Core (Apache HTTP Server)	HTTP	Yes	5.3	Network	Low
CVE-2019-10247	Oracle Communications Services Gatekeeper	Platform Test Environment (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2020-1934	Oracle Communications Session Report Manager	Core (Apache HTTP Server)	HTTP	Yes	5.3	Network	Low
CVE-2020-1934	Oracle Communications Session Route Manager	Core (Apache HTTP Server)	HTTP	Yes	5.3	Network	Low
CVE-2020-14574	Oracle Communications Interactive Session Recorder	FACE	None	No	4.7	Local	High
CVE-2020-9488	Oracle Communications Instant	Installation (Log4j)	SMTPS	Yes	3.7	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
	Messaging Server						
CVE-2020-9488	Oracle Communications Interactive Session Recorder	API, FACE, Archiver (Log4j)	SMTPS	Yes	3.7	Network	High
CVE-2020-9488	Oracle Communications Network Charging and Control	Notification Gateway (Log4j)	SMTPS	Yes	3.7	Network	High

Additional CVEs addressed are below:

- The patch for CVE-2016-1181 also addresses CVE-2016-1182.
- The patch for CVE-2017-0861 also addresses CVE-2017-15265, CVE-2018-1000004, CVE-2018-10901, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390 and CVE-2018-7566.
- The patch for CVE-2017-5645 also addresses CVE-2020-9488.
- 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-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The patch for CVE-2018-3639 also addresses CVE-2018-10675, CVE-2018-10872 and CVE-2018-3665.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10193 also addresses CVE-2019-10192.
- The patch for CVE-2019-10247 also addresses CVE-2019-10246.
- The patch for CVE-2019-12423 also addresses CVE-2019-17573.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2019-16056 also addresses CVE-2019-16935.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.
- The patch for CVE-2019-2729 also addresses CVE-2019-2725.
- The patch for CVE-2019-2904 also addresses CVE-2019-2094.

- The patch for CVE-2020-11022 also addresses CVE-2019-11358 and CVE-2020-11023.
- The patch for CVE-2020-11656 also addresses CVE-2020-11655, CVE-2020-13434, CVE-2020-13435, CVE-2020-13630, CVE-2020-13631, CVE-2020-13632 and CVE-2020-9327.
- The patch for CVE-2020-1934 also addresses CVE-2020-1927.
- The patch for CVE-2020-1938 also addresses CVE-2019-17569 and CVE-2020-1935.
- 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-2020-7060 also addresses CVE-2020-7059.
- 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-2020-11619, CVE-2020-11620, CVE-2020-9547 and CVE-2020-9548.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 20 new security patches for Oracle Construction and Engineering. 15 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-2017-5645	Primavera Gateway	Admin (Apache Ant)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-10683	Primavera P6 Enterprise Project Portfolio Management	Web Access (dom4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-9546	Primavera Unifier	Platform (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-1945	Primavera Unifier	Core (Apache Ant)	HTTP	Yes	9.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2018-17196	Primavera P6 Enterprise Project Portfolio Management	Web Access (kafka client)	HTTP	No	8.8	Network	Low	L
CVE-2020-9484	Instantis EnterpriseTrack	Core (Apache Tomcat)	None	No	7.0	Local	High	L
CVE-2020-11022	Primavera Gateway	Admin (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-2562	Primavera Portfolio Management	Investor Module	HTTP	Yes	6.1	Network	Low	N
CVE-2020-14528	Primavera Portfolio Management	Web Access	HTTP	Yes	6.1	Network	Low	N
CVE-2020-14706	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	Yes	5.9	Network	High	N
CVE-2020-14527	Primavera Portfolio Management	Web Access	HTTP	Yes	5.9	Network	High	N
CVE-2020-14549	Primavera Portfolio Management	Web Server	HTTPS	Yes	5.9	Network	High	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-14618	Primavera Unifier	Mobile App	HTTPS	Yes	5.9	Network	High	N
CVE-2020-14617	Primavera Unifier	Platform, Mobile App	HTTPS	No	5.7	Network	Low	L
CVE-2020-14653	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	No	5.4	Network	Low	L
CVE-2020-14529	Primavera Portfolio Management	Investor Module	HTTP	No	5.4	Network	Low	L
CVE-2020-1934	Instantis EnterpriseTrack	Core (Apache HTTP Server)	HTTP	Yes	5.3	Network	Low	N
CVE-2020-14566	Primavera Portfolio Management	Web Access	HTTP	Yes	4.3	Network	Low	N
CVE-2020-9488	Instantis EnterpriseTrack	Logging (Log4j)	SMTPS	Yes	3.7	Network	High	N
CVE-2020-9488	Primavera Gateway	Admin (Log4j)	SMTPS	Yes	3.7	Network	High	N

Additional CVEs addressed are below:

- The patch for CVE-2017-5645 also addresses CVE-2020-1945.
- The patch for CVE-2018-17196 also addresses CVE-2017-12610 and CVE-2018-1288.
- The patch for CVE-2020-10683 also addresses CVE-2018-1000632.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-1934 also addresses CVE-2020-1927.
- The patch for CVE-2020-9484 also addresses CVE-2019-17569, CVE-2020-1935 and CVE-2020-1938.
- 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-2020-11619, CVE-2020-11620, CVE-2020-9547 and CVE-2020-9548.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 30 new security patches for the Oracle E-Business Suite. 24 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 July 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 (July 2020), My Oracle Support Note 2679563.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14598	Oracle CRM Gateway for Mobile Devices	Setup of Mobile Applications	HTTP	Yes	9.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P Re
CVE-2020-14599	Oracle CRM Gateway for Mobile Devices	Setup of Mobile Applications	HTTP	Yes	9.1	Network	Low	N
CVE-2020-14658	Oracle Marketing	Marketing Administration	HTTP	Yes	9.1	Network	Low	N
CVE-2020-14665	Oracle Trade Management	Invoice	HTTP	Yes	9.1	Network	Low	N
CVE-2020-14670	Oracle Advanced Outbound Telephony	Settings	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14671	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14534	Oracle Applications Framework	Popups	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14688	Oracle Common Applications	CRM User Management Framework	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14660	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14682	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14668	Oracle E-Business Intelligence	DBI Setups	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14681	Oracle E-Business Intelligence	DBI Setups	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14666	Oracle Email Center	Message Display	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 Re
CVE-2020-14596	Oracle iStore	Address Book	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14582	Oracle iStore	User Registration	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14686	Oracle iSupport	Others	HTTP	Yes	8.2	Network	Low	N
CVE-2020-14719	Oracle Internet Expenses	Mobile Expenses Admin Utilities	HTTP	No	7.7	Network	Low	L
CVE-2020-14720	Oracle Internet Expenses	Mobile Expenses Admin Utilities	HTTP	No	7.7	Network	Low	L
CVE-2020-14610	Oracle Applications Framework	Attachments / File Upload	HTTP	No	7.6	Network	Low	L
CVE-2020-14657	Oracle CRM Technical Foundation	Preferences	HTTP	No	7.6	Network	Low	L
CVE-2020-14667	Oracle CRM Technical Foundation	Preferences	HTTP	No	7.6	Network	Low	L
CVE-2020-14679	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	7.5	Network	Low	N
CVE-2020-14635	Oracle Application Object Library	Logging	HTTP	Yes	5.3	Network	Low	N
CVE-2020-14554	Oracle Application Object Library	Diagnostics	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14716	Oracle Common Applications	CRM User Management Framework	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14717	Oracle Common Applications	CRM User Management Framework	HTTP	Yes	4.7	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P Re
CVE-2020-14659	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14661	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14555	Oracle Marketing	Marketing Administration	HTTP	Yes	4.7	Network	Low	N
CVE-2020-14590	Oracle Applications Framework	Page Request	HTTP	No	2.7	Network	Low	H

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 14 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 July 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 July 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2664876.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-9546	Enterprise Manager Base Platform	Enterprise Manager Install (jackson-databind)	HTTP	Yes	9.8	Network	Low	Non
CVE-2017-5645	Oracle Application Testing Suite	Load Testing for Web Apps (Log4j)	Multiple	Yes	9.8	Network	Low	Non
CVE-2020-1945	Enterprise Manager Ops Center	Networking (Apache Ant)	HTTP	Yes	9.1	Network	Low	Non
CVE-2019-0227	Enterprise Manager for Fusion Middleware	Coherence Management (Apache Axis)	HTTP	Yes	8.8	Adjacent Network	Low	Non
CVE-2018-11776	Enterprise Manager Base Platform	Reporting Framework (Apache Struts 2)	HTTP	Yes	8.1	Network	High	Non
CVE-2019-0227	Enterprise Manager Base Platform	Application Service Level Mgmt (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Non
CVE-2020-7595	Oracle Real User Experience Insight	APM Mesh (libxml2)	HTTP	Yes	7.5	Network	Low	Non
CVE-2020-2982	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2984	Oracle Configuration Manager	Discovery and collection script	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2983	Oracle Data Masking and Subsetting	Data Masking	HTTP	No	7.1	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-17091	Oracle Application Testing Suite	Load Testing for Web Apps (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-12415	Enterprise Manager Base Platform	Application Service Level Mgmt (Apache POI)	None	No	5.5	Local	Low	Lo
CVE-2020-1934	Enterprise Manager Ops Center	Networking (Apache HTTP Server)	HTTP	Yes	5.3	Network	Low	Non
CVE-2019-1551	Enterprise Manager Ops Center	Networking (OpenSSL)	HTTPS	Yes	5.3	Network	Low	Non

Additional CVEs addressed are below:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-12415 also addresses CVE-2017-12626.
- The patch for CVE-2019-1551 also addresses CVE-2020-1967.
- The patch for CVE-2020-1934 also addresses CVE-2019-0220, CVE-2019-10081, CVE-2019-10082, CVE-2019-10092, CVE-2019-10097 and CVE-2020-1927.
- The patch for CVE-2020-1945 also addresses CVE-2017-5645.
- The patch for CVE-2020-7595 also addresses CVE-2019-19956 and CVE-2019-20388.
- 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-2020-11619, CVE-2020-11620, CVE-2020-9547 and CVE-2020-9548.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 38 new security patches for Oracle Financial Services Applications. 26 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	P R
CVE-2019-13990	Oracle Banking Payments	Core (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-9546	Oracle Banking Platform	Framework (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Financial Services Lending and Leasing	Core (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Financial Services Lending and Leasing	Core (Log4j)	Multiple	Yes	9.8	Network	Low	N
CVE-2017-15708	Oracle Financial Services Market Risk Measurement and Management	User Interface (Apache Synapse)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-13990	Oracle FLEXCUBE Investor Servicing	Infrastructure (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-13990	Oracle FLEXCUBE Private Banking	Core (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-11358	Oracle Insurance Accounting Analyzer	User Interface (jQuery)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-1945	Oracle Financial Services Analytical	Infrastructure (Apache Ant)	HTTP	Yes	9.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Applications Infrastructure							
CVE-2020-1945	Oracle FLEXCUBE Investor Servicing	Infrastructure (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle FLEXCUBE Private Banking	Utilities (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-14569	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	8.1	Network	Low	
CVE-2020-1945	Oracle Banking Enterprise Collections	Installer (Apache Ant)	None	No	7.7	Local	Low	
CVE-2020-1945	Oracle Banking Platform	Installer (Apache Ant)	None	No	7.7	Local	Low	
CVE-2019-0227	Oracle Financial Services Compliance Regulatory Reporting	Web Service to Regulatory Report (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	
CVE-2019-12402	Oracle FLEXCUBE Investor Servicing	Infrastructure (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	
CVE-2019-12423	Oracle FLEXCUBE Private Banking	Core (Apache CXF)	HTTP	Yes	7.5	Network	Low	
CVE-2019-0188	Oracle FLEXCUBE	Core (Apache Camel)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Private Banking							
CVE-2019-17359	Oracle FLEXCUBE Private Banking	Core (Bouncy Castle Java Library)	TLS	Yes	7.5	Network	Low	
CVE-2020-14602	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	No	7.1	Network	Low	
CVE-2020-14691	Oracle Financial Services Liquidity Risk Management	User Interface	HTTP	No	7.1	Network	Low	
CVE-2020-14605	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	No	6.5	Network	Low	
CVE-2020-14685	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	No	6.5	Network	Low	
CVE-2020-14692	Oracle Financial Services Loan Loss Forecasting and Provisioning	User Interface	HTTP	No	6.5	Network	Low	
CVE-2020-14693	Oracle Insurance Accounting Analyzer	User Interface	HTTP	No	6.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14662	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	No	6.3	Network	Low	
CVE-2020-11022	Oracle Banking Enterprise Collections	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-11022	Oracle Banking Platform	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-14601	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	Yes	6.1	Network	Low	N
CVE-2020-14615	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	Yes	6.1	Network	Low	N
CVE-2020-11022	Oracle Financial Services Regulatory Reporting for De Nederlandsche Bank	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-12415	Oracle Banking Payments	Core (Apache POI)	None	No	5.5	Local	Low	
CVE-2019-12415	Oracle FLEXCUBE Private Banking	Core (Apache POI)	None	No	5.5	Local	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-14603	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	Yes	5.3	Network	Low	
CVE-2020-14604	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	Yes	5.3	Network	Low	
CVE-2020-14684	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	Yes	4.3	Network	Low	
CVE-2020-9488	Oracle Banking Platform	Collections (Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle FLEXCUBE Investor Servicing	Infrastructure (Log4j)	SMTPS	Yes	3.7	Network	High	

Additional CVEs addressed are below:

- The patch for CVE-2017-5645 also addresses CVE-2020-9488.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-12423 also addresses CVE-2019-17573.
- The patch for CVE-2019-13990 also addresses CVE-2019-12402 and CVE-2019-5427.
- 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-2020-9546 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-2020-11619, CVE-2020-11620, 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. 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 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14543	Oracle Hospitality Reporting and Analytics	Installation	None	No	7.3	Local	Low	Low
CVE-2020-14561	Oracle Hospitality Reporting and Analytics	Installation	None	No	7.3	Local	Low	Low
CVE-2020-14594	Oracle Hospitality Reporting and Analytics	Inventory Integration	None	No	6.5	Local	Low	High
CVE-2020-14616	Oracle Hospitality Reporting and Analytics	Reporting	HTTP	No	2.7	Network	Low	High

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 52 new security patches for Oracle Fusion Middleware. 48 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 July 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 July 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2664876.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2017-5645	Oracle Endeca Information Discovery Studio	Studio (Apache Ant)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-17531	Oracle WebCenter Portal	Security Framework (jackson-databind)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2020-9546	Oracle WebLogic Server	Centralized Thirdparty Jars (jackson-databind)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2018-11058	Oracle WebLogic Server	Security Service (RSA BSAFE)	HTTPS	Yes	9.8	Network	Low	Nor
CVE-2020-14625	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low	Nor
CVE-2020-14644	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low	Nor
CVE-2020-14645	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low	Nor
CVE-2020-14687	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low	Nor
CVE-2017-5645	Oracle WebLogic Server	Centralized Thirdparty Jars (Log4j)	Multiple	Yes	9.8	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2017-5645	Oracle WebLogic Server	Console (Log4j)	Multiple	Yes	9.8	Network	Low	Nor
CVE-2020-1945	Oracle Endeca Information Discovery Studio	Studio (Apache Ant)	HTTP	Yes	9.1	Network	Low	Nor
CVE-2020-1945	Oracle Enterprise Repository	Security Subsystem (Apache Ant)	HTTP	Yes	9.1	Network	Low	Nor
CVE-2020-8112	Oracle Outside In Technology	Installation (OpenJPEG)	HTTP	Yes	8.8	Network	Low	Nor
CVE-2020-14609	Oracle Business Intelligence Enterprise Edition	Analytics Web Answers	HTTP	Yes	8.6	Network	Low	Nor
CVE-2020-14611	Oracle WebCenter Portal	Composer	HTTP	Yes	8.6	Network	Low	Nor
CVE-2020-14584	Oracle BI Publisher	BI Publisher Security	HTTP	Yes	8.2	Network	Low	Nor
CVE-2020-14585	Oracle BI Publisher	Mobile Service	HTTP	Yes	8.2	Network	Low	Nor
CVE-2020-14690	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	Yes	8.2	Network	Low	Nor
CVE-2020-14608	Oracle Fusion Middleware MapViewer	Tile Server	HTTP	Yes	8.2	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-14723	Oracle Help Technologies	Web UIX	HTTP	Yes	8.2	Network	Low	Nor
CVE-2020-14588	Oracle WebLogic Server	Web Container	HTTP	Yes	8.2	Network	Low	Nor
CVE-2020-14626	Oracle Business Intelligence Enterprise Edition	Analytics Web General	HTTP	Yes	8.1	Network	High	Nor
CVE-2020-14565	Oracle Unified Directory	Security	HTTP	No	8.1	Network	Low	Hig
CVE-2019-17359	Oracle Business Process Management Suite	Runtime Engine (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	Nor
CVE-2020-14642	Oracle Coherence	CacheStore	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-0227	Oracle WebCenter Portal	WebCenter Spaces Application (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Nor
CVE-2020-14639	Oracle WebLogic Server	Sample apps	HTTP	Yes	7.5	Network	Low	Nor
CVE-2020-5398	Oracle WebLogic Server	Sample apps (Spring Framework)	HTTP	Yes	7.5	Network	High	Nor
CVE-2020-14589	Oracle WebLogic	Web Container	HTTP	Yes	7.5	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Server							
CVE-2020-2967	Oracle WebLogic Server	Web Services	IIOP, T3	Yes	7.5	Network	Low	Nor
CVE-2020-14696	Oracle BI Publisher	Layout Templates	HTTP	Yes	7.2	Network	Low	Nor
CVE-2020-14571	Oracle BI Publisher	Mobile Service	HTTP	Yes	7.2	Network	Low	Nor
CVE-2020-14570	Oracle BI Publisher	Mobile Service	HTTP	Yes	7.1	Network	Low	Nor
CVE-2020-14552	Oracle WebCenter Portal	Security Framework	HTTP	No	6.8	Network	Low	Lov
CVE-2020-14557	Oracle WebLogic Server	Web Container	HTTP	Yes	6.8	Network	High	Nor
CVE-2020-14655	Oracle Security Service	SSL API	HTTPS	Yes	6.5	Network	High	Nor
CVE-2020-14652	Oracle WebLogic Server	Core	HTTP	Yes	6.5	Network	Low	Nor
CVE-2019-14862	Oracle Business Intelligence Enterprise Edition	BI Platform Security (Knockout)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-1941	Oracle Enterprise Repository	Security Subsystem	HTTP	Yes	6.1	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
		(Apache ActiveMQ)						
CVE-2020-14607	Oracle Fusion Middleware MapViewer	Tile Server	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14613	Oracle WebCenter Sites	Advanced User Interface	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14572	Oracle WebLogic Server	Console	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14636	Oracle WebLogic Server	Sample apps	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14637	Oracle WebLogic Server	Sample apps	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14638	Oracle WebLogic Server	Sample apps	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14640	Oracle WebLogic Server	Sample apps	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-14530	Oracle Security Service	None	HTTPS	Yes	5.9	Network	High	Nor
CVE-2019-12415	Oracle WebCenter Portal	Security Framework (Apache POI)	None	No	5.5	Local	Low	Lov
CVE-2020-2966	Oracle WebLogic Server	Console	HTTP	Yes	5.4	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-14622	Oracle WebLogic Server	Core	HTTP	No	4.9	Network	Low	Hig
CVE-2020-9488	Oracle Fusion Middleware MapViewer	Install (Log4j)	SMTPS	Yes	3.7	Network	High	Nor
CVE-2020-14548	Oracle Business Intelligence Enterprise Edition	Analytics Web General	HTTP	Yes	3.4	Network	High	Nor

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 below:
- The patch for CVE-2017-5645 also addresses CVE-2019-17571.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-17531 also addresses CVE-2019-16943, CVE-2019-17267, CVE-2019-20330 and CVE-2020-9546.
- The patch for CVE-2020-1945 also addresses CVE-2017-5645.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.
- The patch for CVE-2020-8112 also addresses CVE-2018-6616, CVE-2019-12973 and CVE-2020-6851.
- 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-2020-11619, CVE-2020-11620, CVE-2020-9547 and CVE-2020-9548.

Oracle GraalVM Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle GraalVM. 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 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-17560	Oracle GraalVM Enterprise Edition	GraalVM Compiler (Apache NetBeans)	HTTPS	Yes	9.1	Network	Low	None	
CVE-2020-14583	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	8.3	Network	High	None	
CVE-2020-11080	Oracle GraalVM Enterprise Edition	JavaScript (Node.js)	HTTP	Yes	7.5	Network	Low	None	
CVE-2020-14718	Oracle GraalVM Enterprise Edition	JVMCI	Multiple	No	7.2	Network	Low	High	

Additional CVEs addressed are below:

- The patch for CVE-2019-17560 also addresses CVE-2019-17561.
- The patch for CVE-2020-11080 also addresses CVE-2020-8172.

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 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-1938	Oracle Health Sciences Empirica Inspections	Web server (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2020-1938	Oracle Health Sciences Empirica Signal	Web server (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low	Non
CVE-2020-5398	Oracle Healthcare Master Person Index	Master Data Management (Spring Framework)	HTTP	Yes	7.5	Network	High	Non
CVE-2020-11022	Oracle Healthcare Translational Research	Cohort Explorer (jQuery)	HTTP	Yes	6.1	Network	Low	Non

Additional CVEs addressed are below:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-1938 also addresses CVE-2019-17569 and CVE-2020-1935.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Hospitality Applications. 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	In
CVE-2020-1938	Oracle Hospitality Guest Access	Base (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low	None	

Additional CVEs addressed are below:

- The patch for CVE-2020-1938 also addresses CVE-2019-17569 and CVE-2020-1935.

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Hyperion. 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			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-14546	Hyperion Financial Close Management	Close Manager	HTTP	No	4.2	Network	High	Hig
CVE-2020-14560	Oracle Hyperion BI+	UI and Visualization	HTTP	No	4.2	Network	High	Hig
CVE-2020-14541	Hyperion Financial Close Management	Close Manager	HTTP	No	2.0	Network	High	Hig

Oracle iLearning Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle iLearning. 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	I
CVE-2020-14595	Oracle iLearning	Assessment Manager	HTTP	Yes	8.2	Network	Low	None	

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Insurance Applications. 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	Priv Req
CVE-2017-12626	Oracle Insurance Policy Administration J2EE	Architecture (Apache POI)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2020-5398	Oracle Insurance Policy Administration J2EE	Architecture (Spring Framework)	HTTP	Yes	7.5	Network	High	Nor
CVE-2020-5398	Oracle Insurance Rules Palette	Architecture (Spring Framework)	HTTP	Yes	7.5	Network	High	Nor
CVE-2019-12415	Oracle Insurance Policy Administration J2EE	Architecture (Apache POI)	None	No	5.5	Local	Low	Lov
CVE-2019-12415	Oracle Insurance Rules Palette	Architecture (Apache POI)	None	No	5.5	Local	Low	Lov
CVE-2020-9488	Oracle Insurance Data Gateway	Security (Log4j)	SMTPS	Yes	3.7	Network	High	Nor

Additional CVEs addressed are below:

- The patch for CVE-2019-12415 also addresses CVE-2017-12626.
- The patch for CVE-2020-5398 also addresses CVE-2018-15756 and CVE-2020-5397.

Oracle Java SE Risk Matrix

This Critical Patch Update contains 11 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-2020-14664	Java SE	JavaFX	Multiple	Yes	8.3	Network	High	None
CVE-2020-14583	Java SE, Java SE Embedded	Libraries	Multiple	Yes	8.3	Network	High	None
CVE-2020-14593	Java SE, Java SE Embedded	2D	Multiple	Yes	7.4	Network	Low	None
CVE-2020-14562	Java SE	ImageIO	Multiple	Yes	5.3	Network	Low	None
CVE-2020-14621	Java SE, Java SE Embedded	JAXP	Multiple	Yes	5.3	Network	Low	None
CVE-2020-14556	Java SE, Java SE Embedded	Libraries	Multiple	Yes	4.8	Network	High	None
CVE-2020-14573	Java SE	Hotspot	Multiple	Yes	3.7	Network	High	None
CVE-2020-14581	Java SE, Java SE Embedded	2D	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
CVE-2020-14578	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.7	Network	High	None
CVE-2020-14579	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.7	Network	High	None
CVE-2020-14577	Java SE, Java SE Embedded	JSSE	TLS	Yes	3.7	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. This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.

3. 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 JD Edwards Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle JD Edwards. 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-2020-9546	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-9546	JD Edwards EnterpriseOne Tools	EnterpriseOne Mobility Sec (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-9546	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-9546	JD Edwards EnterpriseOne Tools	Web Runtime (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-9488	JD Edwards EnterpriseOne Tools	Installation SEC (Log4j)	SMTPS	Yes	3.7	Network	High	No
CVE-2020-9488	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics (Log4j)	SMTPS	Yes	3.7	Network	High	No

Additional CVEs addressed are below:

- 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-2020-11619, CVE-2020-11620, CVE-2020-9547 and CVE-2020-9548.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 41 new security patches for Oracle MySQL. 6 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	P R
CVE-2020-1938	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low	N
CVE-2020-1967	MySQL Connectors	Connector/C++ (OpenSSL)	TLS	Yes	7.5	Network	Low	N
CVE-2020-1967	MySQL Connectors	Connector/ODBC (OpenSSL)	TLS	Yes	7.5	Network	Low	N
CVE-2020-5398	MySQL Enterprise Monitor	Monitoring: General (Spring Framework)	HTTPS	Yes	7.5	Network	High	N
CVE-2020-1967	MySQL Server	Server: Security: Encryption (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low	N
CVE-2020-14663	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	7.2	Network	Low	H
CVE-2020-14678	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	7.2	Network	Low	H
CVE-2020-14697	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	7.2	Network	Low	H
CVE-2020-14591	MySQL Server	Server: Audit Plug-in	MySQL Protocol	No	6.5	Network	Low	L
CVE-2020-14539	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	L
CVE-2020-14680	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	L
CVE-2020-14619	MySQL Server	Server: Parser	MySQL Protocol	No	6.5	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14576	MySQL Server	Server: UDF	MySQL Protocol	No	6.5	Network	Low	L
CVE-2020-14643	MySQL Server	Server: Security: Roles	MySQL Protocol	No	5.5	Network	Low	H
CVE-2020-14651	MySQL Server	Server: Security: Roles	MySQL Protocol	No	5.5	Network	Low	H
CVE-2020-14550	MySQL Client	C API	MySQL Protocol	No	5.3	Network	High	L
CVE-2019-1551	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	HTTPS	Yes	5.3	Network	Low	N
CVE-2020-14568	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14623	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14540	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14575	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14620	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14624	MySQL Server	Server: JSON	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14656	MySQL Server	Server: Locking	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14547	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-14597	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14614	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14654	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14725	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14632	MySQL Server	Server: Options	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14567	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14631	MySQL Server	Server: Security: Audit	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14586	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14702	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14641	MySQL Server	Server: Security: Roles	MySQL Protocol	No	4.9	Network	Low	H
CVE-2020-14559	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.3	Network	Low	I
CVE-2020-14553	MySQL Server	Server: Pluggable Auth	MySQL Protocol	No	4.3	Network	Low	I
CVE-2020-14633	MySQL Server	InnoDB	MySQL Protocol	No	2.7	Network	Low	H
CVE-2020-14634	MySQL Server	InnoDB	MySQL Protocol	No	2.7	Network	Low	H
CVE-2020-5258	MySQL Cluster	Cluster: Packaging (dojo)	Multiple	No	0.0	Network	Low	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-1967	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	HTTPS	No	0.0	Network	Low	N

Notes:
1. This CVE is not exploitable in MySQL Cluster. The CVSS v3.1 Base Score for this CVE in the National Vulnerability Database (NVD) is 7.5.

2. This CVE is not exploitable in MySQL Enterprise Monitor. The CVSS v3.1 Base Score for this CVE in the National Vulnerability Database (NVD) is 7.5.

Additional CVEs addressed are below:
- The patch for CVE-2020-1938 also addresses CVE-2019-17569 and CVE-2020-1935.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle PeopleSoft. 9 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'd
CVE-2019-17359	PeopleSoft Enterprise HCM Global Payroll Switzerland	Global Payroll for Switzerland (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-16056	PeopleSoft Enterprise PeopleTools	Porting (Python)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-11358	PeopleSoft Enterprise FIN Expenses	Expenses (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14627	PeopleSoft Enterprise PeopleTools	Query	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14592	PeopleSoft Enterprise PeopleTools	Rich Text Editor	HTTP	Yes	6.1	Network	Low	None
CVE-2020-14587	PeopleSoft Enterprise FIN Expenses	Expenses	HTTP	No	5.4	Network	Low	Low
CVE-2020-14612	PeopleSoft Enterprise HRMS	Time and Labor	HTTP	No	5.4	Network	Low	Low
CVE-2020-14558	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	5.3	Network	Low	None
CVE-2019-1551	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	5.3	Network	Low	None
CVE-2020-14600	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	4.3	Network	Low	None
CVE-2020-14564	PeopleSoft Enterprise PeopleTools	Environment Mgmt Console	HTTP	No	2.7	Network	Low	High

Additional CVEs addressed are below:

- The patch for CVE-2019-16056 also addresses CVE-2019-16935.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 47 new security patches for Oracle Retail Applications. 42 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	I
CVE-2019-13990	Customer Management and Segmentation Foundation	Segment (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	
CVE-2019-12086	Customer Management and Segmentation Foundation	Segment (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-2555	Oracle Retail Assortment Planning	Application Core (Coherence)	HTTP	Yes	9.8	Network	Low	
CVE-2017-5645	Oracle Retail Extract Transform and Load	Mathematical Operators (Log4j)	Multiple	Yes	9.8	Network	Low	
CVE-2020-1945	Oracle Retail Financial Integration	PeopleSoft Integration (Apache Ant)	HTTP	Yes	9.8	Network	Low	
CVE-2020-10683	Oracle Retail Integration Bus	RIB Kernal (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2019-13990	Oracle Retail Integration Bus	RIB Kernal (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	
CVE-2019-16943	Oracle Retail Merchandising System	Inventory Movement (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2019-16943	Oracle Retail Sales Audit	Transaction Maintenance (jackson-databind)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2017-5645	Oracle Retail Service Backbone	Installer (Log4j)	Multiple	Yes	9.8	Network	Low	
CVE-2019-13990	Oracle Retail Xstore Point of Service	Xenvironment (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Retail Xstore Point of Service	Xenvironment (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-1945	Category Management Planning & Optimization	ODI Integration (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Assortment Planning	Application Core (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Data Extractor for Merchandising	ODI Knowledge Module (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Item Planning	Application Core (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Macro Space Optimization	ODI Integration (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Merchandise Financial Planning	Application Core (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Predictive Application Server	RPAS Server (Apache Ant)	HTTP	Yes	9.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-1945	Oracle Retail Regular Price Optimization	Operations & Maintenance (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Replenishment Optimization	Application Core (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Service Backbone	Install (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Size Profile Optimization	Application Core (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-1945	Oracle Retail Store Inventory Management	SIM Integration (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2015-9251	Oracle Retail Customer Management and Segmentation Foundation	Promotions (jQuery)	HTTP	No	8.0	Network	Low	
CVE-2020-5398	Oracle Retail Assortment Planning	Application Core (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2020-5398	Oracle Retail Financial Integration	PeopleSoft Integration (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2017-12626	Oracle Retail Fusion Platform	Retail Portal Framework (Apache POI)	HTTP	Yes	7.5	Network	Low	
CVE-2020-5398	Oracle Retail Integration Bus	RIB Kernal (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2019-12423	Oracle Retail Order Broker	System Administration (Apache CXF)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-5398	Oracle Retail Predictive Application Server	RPAS Server (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2020-5398	Oracle Retail Service Backbone	RSB Installation (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2019-10086	Customer Management and Segmentation Foundation	Promotions (Apache Commons-Beanutils)	HTTP	Yes	7.3	Network	Low	
CVE-2020-14709	Customer Management and Segmentation Foundation	Card	HTTP	No	7.1	Network	Low	
CVE-2019-3740	Oracle Retail Store Inventory Management	SIM Integration (BSAFE Crypto-J)	TLS	Yes	6.5	Network	Low	
CVE-2019-17091	Oracle Retail Financial Integration	PeopleSoft Integration (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2019-17091	Oracle Retail Integration Bus	RIB Kernal (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2019-17091	Oracle Retail Invoice Matching	Pricing (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2019-17091	Oracle Retail Service Backbone	RSB kernel (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2018-10237	Oracle Retail Integration Bus	Packaging (Google Guava)	HTTP	Yes	5.9	Network	High	
CVE-2020-14710	Customer Management	Security	HTTP	No	5.4	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	and Segmentation Foundation							
CVE-2020-14708	Customer Management and Segmentation Foundation	Segment	HTTP	No	4.3	Network	Low	
CVE-2018-15756	Oracle Retail Xstore Point of Service	Point of Sale (Spring Framework)	HTTP	No	4.3	Network	Low	
CVE-2020-9488	Oracle Retail Data Extractor for Merchandising	Knowledge Module (Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle Retail Financial Integration	PeopleSoft Integration (Log4j)	SMTPS	Yes	3.7	Network	High	
CVE-2020-9488	Oracle Retail Store Inventory Management	SIM Integration (Log4j)	SMTPS	Yes	3.7	Network	High	

Additional CVEs addressed are below:

- The patch for CVE-2015-9251 also addresses CVE-2020-11022.
- The patch for CVE-2017-12626 also addresses CVE-2019-12415.
- The patch for CVE-2018-15756 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1199, CVE-2018-1257, CVE-2018-1270, CVE-2018-1271, CVE-2018-1272 and CVE-2018-1275.
- The patch for CVE-2019-12086 also addresses CVE-2019-14540, CVE-2019-16335, CVE-2019-16942, CVE-2019-16943, CVE-2019-17267, CVE-2019-17531 and CVE-2019-20330.
- The patch for CVE-2019-12423 also addresses CVE-2019-17573.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.
- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739.
- The patch for CVE-2020-1945 also addresses CVE-2017-5645.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.

- The patch for CVE-2020-9546 also addresses CVE-2019-16942, CVE-2019-16943, CVE-2019-17531, 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-2020-9547 and CVE-2020-9548.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 5 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 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-16943	Siebel Engineering - Installer & Deployment	Siebel Approval Manager (jackson-databind)	HTTP	Yes	9.8	Network	Low	None
CVE-2020-1938	Siebel UI Framework	EAI, SWSE (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	9.8	Network	Low	None
CVE-2019-16943	Siebel UI Framework	EAI (jackson-databind)	HTTP	Yes	9.8	Network	Low	None
CVE-2020-14531	Siebel UI Framework	SWSE Server	HTTP	Yes	5.9	Network	High	None
CVE-2020-9488	Siebel Engineering - Installer & Deployment	Siebel Approval Manager (Log4j)	SMTPS	Yes	3.7	Network	High	None

Additional CVEs addressed are below:

- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 22 new security patches for Oracle Supply Chain. 18 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-2019-2729	Oracle Rapid Planning	Middle Tier	HTTP	Yes	9.8	Network	Low	
CVE-2020-2555	Oracle Rapid Planning	Middle Tier	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Rapid Planning	Middle Tier (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-5019	Oracle Rapid Planning	Middle Tier (Apache Trinidad)	HTTP	Yes	9.8	Network	Low	
CVE-2020-10683	Oracle Rapid Planning	Middle Tier (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2016-4000	Oracle Rapid Planning	Middle Tier (jython)	HTTP	Yes	9.8	Network	Low	
CVE-2017-5645	Oracle Rapid Planning	Middle Tier (Apache Ant)	Multiple	Yes	9.8	Network	Low	
CVE-2017-5645	Oracle Rapid Planning	Middle Tier (Log4j)	Multiple	Yes	9.8	Network	Low	
CVE-2019-17563	Oracle Transportation Management	Install (Apache Tomcat)	HTTP	Yes	9.8	Network	Low	
CVE-2016-6814	Oracle Agile Engineering Data Management	Install (Apache Groovy)	HTTP	Yes	9.6	Network	Low	
CVE-2020-1945	Oracle Rapid Planning	Middle Tier (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2015-7501	Oracle Rapid Planning	Middle Tier (Apache Commons Collections)	HTTP	No	8.8	Network	Low	
CVE-2020-14669	Oracle Configurator	UI Servlet	HTTP	Yes	8.2	Network	Low	
CVE-2019-0227	Oracle Agile Engineering	Install (Apache	HTTP	Yes	7.5	Adjacent Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Data Management	Axis)						
CVE-2019-0227	Oracle Rapid Planning	Installation (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	
CVE-2020-5398	Oracle Rapid Planning	Installation (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2018-15756	Oracle Rapid Planning	Middle Tier (Spring Framework)	HTTP	Yes	7.5	Network	Low	
CVE-2018-8013	Oracle Rapid Planning	Middle Tier (Apache Batik)	HTTP	Yes	7.3	Network	Low	
CVE-2019-17091	Oracle Rapid Planning	Installation (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2019-1547	Oracle Agile Engineering Data Management	Install (OpenSSL)	None	No	4.7	Local	High	
CVE-2020-14551	Oracle AutoVue	Security	HTTP	No	4.3	Network	Low	
CVE-2020-14544	Oracle Transportation Management	Data, Domain & Function Security	HTTP	No	4.3	Network	Low	

Additional CVEs addressed are below:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.
- The patch for CVE-2019-17563 also addresses CVE-2019-17569, CVE-2020-1935 and CVE-2020-1938.
- The patch for CVE-2019-2729 also addresses CVE-2019-2725.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.

Oracle Systems Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Systems. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-11656	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	9.8	Network	Low	None	
CVE-2020-14724	Oracle Solaris	Device Driver Utility	None	No	7.3	Local	Low	Low	F
CVE-2018-12207	Oracle Solaris	Kernel	None	No	6.5	Local	Low	Low	
CVE-2020-14537	Oracle Solaris	Packaging Scripts	None	No	5.5	Local	Low	High	F
CVE-2020-14545	Oracle Solaris	Device Driver Utility	None	No	5.0	Local	High	Low	F
CVE-2019-5489	Oracle Solaris	Kernel	Multiple	No	3.5	Network	High	Low	
CVE-2020-14542	Oracle Solaris	libsuri	None	No	3.3	Local	Low	Low	

Notes:
1. Please refer to My Oracle Support Note 2609642.1 for further information on how CVE-2018-12207 impacts Oracle Solaris.

Additional CVEs addressed are below:
- The patch for CVE-2020-11656 also addresses CVE-2020-1927 and CVE-2020-1934.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Utilities Applications. 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 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2018-12023	Oracle Utilities Framework	Common (jackson-databind)	HTTP	Yes	7.5	Network	High	None	

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 25 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	I
CVE-2020-14628	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2020-14646	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14647	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14649	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2020-14713	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14674	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14675	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14676	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14677	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14699	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-14711	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	High	R

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-14629	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14703	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14704	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-14648	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2020-14650	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2020-14673	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2020-14694	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-14695	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2020-14698	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2020-14700	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2020-14712	Oracle VM VirtualBox	Core	None	No	5.0	Local	Low	Low	R
CVE-2020-14707	Oracle VM VirtualBox	Core	None	No	5.0	Local	Low	Low	R
CVE-2020-14714	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	
CVE-2020-14715	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	

Notes:

1. The CVE-2020-14628 is applicable to Windows VM only.
2. The CVE-2020-14711 is applicable to macOS host only.