Oracle Critical Patch Update Advisory - April 2019

Oracle Critical Patch Update Advisory - April 2019

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. Critical Patch Update patches are usually cumulative, but each advisory describes only the security fixes added since the previous Critical Patch Update advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security fixes. 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 fixes. 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 fixes without delay.

This Critical Patch Update contains 297 new security fixes 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 April 2019 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

Agile Recipe Management for Pharmaceuticals, versions 9.3.3, 9.3.4	Oracle Supply Chain Products
Enterprise Manager Base Platform, versions 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0	Enterprise Manager
Enterprise Manager Ops Center, version 12.3.3	Enterprise Manager
FMW Platform, version 12.2.1.3.0	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineering Suite
JD Edwards EnterpriseOne Tools, version 9.2	JD Edwards
JD Edwards World Technical Foundation, versions A9.2, A9.3.1, A9.4	JD Edwards
MICROS Lucas, versions 2.9.5.6, 2.9.5.7	Retail Applications
MICROS Relate CRM Software, version 11.4	Retail Applications
MICROS Retail-J, version 12.1.2	Retail Applications
MySQL Connectors, versions 5.3.12 and prior, 8.0.15 and prior	MySQL
MySQL Enterprise Backup, versions 3.12.3 and prior, 4.1.2 and prior	MySQL
MySQL Enterprise Monitor, versions 4.0.8 and prior, 8.0.14 and prior	MySQL
MySQL Server, versions 5.6.43 and prior, 5.7.25 and prior, 8.0.15 and prior	MySQL
Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5	Oracle Supply Chain Products
Oracle API Gateway, version 11.1.2.4.0	Fusion Middleware
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle AutoVue 3D Professional Advanced, versions 21.0.0, 21.0.1	Oracle Supply Chain Products
Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.5.0, 2.6.0	Oracle Banking Platform
Oracle Berkeley DB, versions prior to 6.138, prior to 18.1.32	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 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Process Management Suite, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Business Transaction Management, version 12.1.0	Enterprise Manager
Oracle Commerce Merchandising, version 11.2.0.3	Oracle Commerce
Oracle Commerce Platform, versions 11.2.0.3, 11.3.1	Oracle Commerce

Oracle Communications Application Session Controller, versions 3.7.1, 3.8.0	Oracle Communications Application Session Controller
Oracle Communications EAGLE Application Processor, versions 16.1.0, 16.2.0	Oracle Communications EAGLE Application Processor
Oracle Communications EAGLE LNP Application Processor, versions 10.0, 10.1, 10.2	Oracle Communications EAGLE LNP Application Processor
Oracle Communications Instant Messaging Server, version 10.0.1	Oracle Communications Instant Messaging Server
Oracle Communications Interactive Session Recorder, versions 6.0, 6.1, 6.2	Oracle Communications Interactive Session Recorder
Oracle Communications LSMS, versions 13.1, 13.2, 13.3	Oracle Communications LSMS
Oracle Communications Messaging Server, versions 8.0, 8.1	Oracle Communications Messaging Server
Oracle Communications Operations Monitor, versions 3.4, 4.0	Oracle Communications Operations Monitor
Oracle Communications Policy Management, versions 12.1, 12.2, 12.3, 12.4	Oracle Communications Policy Management
Oracle Communications Pricing Design Center, versions 11.1, 12.0	Oracle Communications Pricing Desig Center
Oracle Communications Service Broker, version 6.0	Oracle Communications Service Broke
Oracle Communications Service Broker Engineered System Edition, version 6.0	Oracle Communications Service Broke Engineered System Edition
Oracle Communications Session Border Controller, versions 8.0.0, 8.1.0, 8.2.0	Oracle Communications Session Bord Controller
Oracle Communications Unified Inventory Management, versions 7.3.2, 7.3.4, 7.3.5, 7.4.0	Oracle Communications Unified Inven Management
Oracle Configuration Manager, version 12.1.0	Enterprise Manager
Oracle Configurator, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Data Integrator, versions 11.1.1.9.0, 12.2.1.3.0	Fusion Middleware
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c	Database
Oracle E-Business Suite, versions 0.9.8, 1.0.0, 1.0.1, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8	E-Business Suite
Oracle Endeca Information Discovery Integrator, version 3.2.0	Fusion Middleware
Oracle Enterprise Communications Broker, versions 3.0.0, 3.1.0	Oracle Enterprise Communications Br
Oracle Enterprise Operations Monitor, versions 3.4, 4.0	Oracle Enterprise Operations Monitor

Oracle Enterprise Session Border Controller, versions 8.0.0, 8.1.0, 8.2.0	Oracle Enterprise Session Border Controller
Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3 - 7.3.5, 8.0.0 - 8.0.7	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Asset Liability Management, versions 8.0.4 - 8.0.7	Oracle Financial Services Asset Liabilit Management
Oracle Financial Services Data Integration Hub, versions 8.0.5 - 8.0.7	Oracle Financial Services Data Integrat Hub
Oracle Financial Services Funds Transfer Pricing, versions 8.0.4 - 8.0.7	Oracle Financial Services Funds Transf Pricing
Oracle Financial Services Hedge Management and IFRS Valuations, versions 8.0.4 - 8.0.7	Oracle Financial Services Hedge Management and IFRS Valuations
Oracle Financial Services Liquidity Risk Management, versions 8.0.2 - 8.0.6	Oracle Financial Services Liquidity Risl Management
Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.2 - 8.0.7	Oracle Financial Services Loan Loss Forecasting and Provisioning
Oracle Financial Services Market Risk Measurement and Management, versions 8.0.5, 8.0.6	Oracle Financial Services Market Risk Measurement and Management
Oracle Financial Services Profitability Management, versions 8.0.4 - 8.0.6	Oracle Financial Services Profitability Management
Oracle Financial Services Reconciliation Framework, versions 8.0.5, 8.0.6	Oracle Financial Services Analytical Applications Reconciliation Framework
Oracle FLEXCUBE Private Banking, versions 2.0.0.0, 2.2.0.1, 12.0.1.0, 12.0.3.0, 12.1.0.0	Oracle Financial Services Applications
Oracle Fusion Middleware MapViewer, version 12.2.1.3.0	Fusion Middleware
Oracle Health Sciences Data Management Workbench, version 2.4.8	Health Sciences
Oracle Healthcare Master Person Index, versions 3.0, 4.0	Health Sciences
Oracle Hospitality Cruise Dining Room Management, version 8.0.80	Oracle Hospitality Cruise Dining Room Management
Oracle Hospitality Cruise Fleet Management, version 9.0.11	Oracle Hospitality Cruise Fleet Management
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 HTTP Server, version 12.2.1.3.0	Fusion Middleware
Oracle Identity Analytics, version 11.1.1.5.8	Fusion Middleware
Oracle Java SE, versions 7u211, 8u202, 11.0.2, 12	Java SE

Oracle Java SE Embedded, version 8u201	Java SE
Oracle JDeveloper, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Knowledge, versions 8.5.1.0 - 8.5.1.7, 8.6.0, 8.6.1	Oracle Knowledge
Oracle Managed File Transfer, versions 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Outside In Technology, versions 8.5.3, 8.5.4	Fusion Middleware
Oracle Real-Time Scheduler, version 2.3.0	Oracle Utilities Applications
Oracle Retail Allocation, version 15.0.2	Retail Applications
Oracle Retail Convenience Store Back Office, version 3.6	Retail Applications
Oracle Retail Customer Engagement, versions 16.0, 17.0	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0	Retail Applications
Oracle Retail Invoice Matching, versions 12.0, 13.0, 13.1, 13.2, 14.0, 14.1, 15.0	Retail Applications
Oracle Retail Merchandising System, versions 15.0, 16.0	Retail Applications
Oracle Retail Order Broker, versions 5.1, 5.2, 15.0, 16.0	Retail Applications
Oracle Retail Point-of-Service, versions 13.4, 14.0, 14.1	Retail Applications
Oracle Retail Workforce Management Software, version 1.60.9.0.0	Retail Applications
Oracle Retail Xstore Point of Service, versions 7.0, 7.1	Retail Applications
Oracle Secure Global Desktop, version 5.4	Virtualization
Oracle Service Bus, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle SOA Suite, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Solaris, versions 10, 11	Systems
Oracle Traffic Director, version 11.1.1.9.0	Fusion Middleware
Oracle Transportation Management, versions 6.3.7, 6.4.2, 6.4.3	Oracle Supply Chain Products
Oracle Tuxedo, version 12.1.1.0.0	Fusion Middleware
Oracle Utilities Framework, versions 2.2.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.2.0, 4.3.0.3.0, 4.3.0.4.0, 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0	Oracle Utilities Applications
Oracle Utilities Mobile Workforce Management, version 2.3.0	Oracle Utilities Applications
Oracle Utilities Network Management System, version 1.12.0.3	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 5.2.28, prior to 6.0.6	Virtualization
Oracle WebCenter Portal, version 12.2.1.3.0	Fusion Middleware
Oracle WebCenter Sites, version 12.2.1.3.0	Fusion Middleware

Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
OSS Support Tools, version 19.1	Support Tools
PeopleSoft Enterprise ELM, version 9.2	PeopleSoft
PeopleSoft Enterprise ELM Enterprise Learning Management, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Talent Acquisition Manager, version 9.2	PeopleSoft
PeopleSoft Enterprise HRMS, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56, 8.57	PeopleSoft
PeopleSoft Enterprise PT PeopleTools, versions 8.55, 8.56, 8.57	PeopleSoft
Primavera P6 Enterprise Project Portfolio Management, versions 8.4, 15.1, 15.2, 16.1, 16.2, 17.7 - 17.12, 18.8	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.1, 16.2, 17.7 - 17.12, 18.8	Oracle Construction and Engineering Suite
Siebel Applications, version 19.3	Siebel

Note:

- Vulnerabilities affecting Oracle Database and 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 fixes required to resolve ZFSSA issues published in Critical Patch Updates and Solaris Third Party bulletins.
- Users running Java SE with a browser can download the latest release from http://www.java.com/en/. 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 fixed by the patches associated with this advisory. Risk matrices for previous security fixes can be found in previous Critical Patch Update advisories. 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 a unique identifier for a vulnerability. 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 3.0 (see Oracle CVSS Scoring for an explanation of how Oracle applies CVSS version 3.0).

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 fixes as soon as possible. Until you apply the Critical Patch Update fixes, 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 fixes 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 fixes 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:

- Andrej Simko of Accenture: CVE-2019-2603, CVE-2019-2639, CVE-2019-2640, CVE-2019-2641, CVE-2019-2642, CVE-2019-2643, CVE-2019-2651, CVE-2019-2652, CVE-2019-2653, CVE-2019-2654, CVE-2019-2660, CVE-2019-2661, CVE-2019-2662, CVE-2019-2663, CVE-2019-2664, CVE-2019-2665
- Andrej Simko of Accenture working with iDefense Labs: CVE-2019-2551, CVE-2019-2600, CVE-2019-2603, CVE-2019-2604, CVE-2019-2622, CVE-2019-2652, CVE-2019-2669, CVE-2019-2670, CVE-2019-2671, CVE-2019-2673, CVE-2019-2674, CVE-2019-2675, CVE-2019-2676, CVE-2019-2677
- Andres Georgieff of Sandia National Laboratories: CVE-2019-2586, CVE-2019-2621
- Andy Nguyen: CVE-2019-2678, CVE-2019-2679, CVE-2019-2680
- anhdaden of StarLabs working with Trend Micro's Zero Day Initiative: CVE-2019-2722
- Athul Jayaram: CVE-2019-2706
- Badcode of Knownsec 404 Team: CVE-2019-2615, CVE-2019-2618
- Corwin de Boor: CVE-2019-2684
- Devin Rosenbauer of Identity Works LLC: CVE-2019-2572
- Dhiraj Mishra: CVE-2018-3123
- Ehsan Nikavar: CVE-2019-2605
- fluoroacetate working with Trend Micro's Zero Day Initiative: CVE-2019-2723

- Frank Lycops: CVE-2019-2704
- huyna of Viettel Cyber Security working with Trend Micro Zero Day Initiative: CVE-2019-2574
- Jakub Palaczynski: CVE-2019-2591
- James Forshaw: CVE-2019-2721
- Jason Matthyser of MWR Labs working with Trend Micro Zero Day Initiative: CVE-2019-2574, CVE-2019-2656, CVE-2019-2657
- Jonas Mattsson of Outpost24 Ghost Labs: CVE-2019-2578, CVE-2019-2579
- Jonathan Jacobi: CVE-2019-2703
- Juan Pablo Perez Etchegoyen of Onapsis: CVE-2019-2568
- Krzysztof Przybylski of STM Solutions: CVE-2019-2720
- Lionel Debroux: CVE-2019-2708
- Luca Rupp of Usd AG: CVE-2019-2709
- Lucas Pinheiro of Microsoft Corp.: CVE-2019-2696
- Lukasz Mikula: CVE-2019-2598
- Lukasz Rupala of ING Tech Poland: CVE-2019-2595, CVE-2019-2601
- Martin Doyhenard of Onapsis: CVE-2019-2633, CVE-2019-2638
- Mateusz Jurczyk of Google Project Zero: CVE-2019-2697, CVE-2019-2698
- Matthew McPeak of Tempus Consulting Group: CVE-2019-2567
- Matthias Kaiser of Apple Information Security: CVE-2019-2645, CVE-2019-2646, CVE-2019-2647, CVE-2019-2648, CVE-2019-2649, CVE-2019-2650
- Mehdi Esmaeilpour: CVE-2019-2605
- Michael Nielson: CVE-2019-2692
- Minle Chen of PingAn Galaxy Lab: CVE-2019-2615, CVE-2019-2618
- Niklas Baumstark working with Trend Micro's Zero Day Initiative: CVE-2019-2690
- Omri Herscovici of Check Point Software: CVE-2019-2608, CVE-2019-2609, CVE-2019-2610, CVE-2019-2611, CVE-2019-2612, CVE-2019-2613, CVE-2019-2705
- Omur Ugur of Turk Telekom: CVE-2019-2576
- Quentin Rhoads-Herrera of Critical Start: CVE-2019-2564
- Robert Xiao: CVE-2019-2684
- Spyridon Chatzimichail of OTE Hellenic Telecommunications Organization S.A.: CVE-2019-2713
- Steven Seeley of Source Incite working with iDefense: CVE-2019-2557
- TheFloW working with Trend Micro Zero Day Initiative: CVE-2019-2574

- Vahagn Vardanyan: CVE-2019-2575, CVE-2019-2588, CVE-2019-2616
- Vladimir Egorov: CVE-2019-2575, CVE-2019-2588, CVE-2019-2616
- Wang Cheng of Venustech ADLab: CVE-2019-2615, CVE-2019-2647
- Yaniv Balmas of Check Point Software: CVE-2019-2608, CVE-2019-2609, CVE-2019-2610, CVE-2019-2611, CVE-2019-2612, CVE-2019-2613, CVE-2019-2705

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 Advisory, Oracle recognizes the following for contributions to Oracle's Security-In-Depth program.:

- Ian McLauchlan of Miton
- Jakub Tyrlik
- Jean-Benjamin Rousseau of SEC Consult Vulnerability Lab
- Guillaume Crouquet of SEC Consult Vulnerability Lab
- Richard O'Donnell of IRM Security
- Thomas Friedlein of Federal Motor Transport Authority (Germany)

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:

- Ankit Singh
- Bharat
- Brian Carpenter
- Celal Erdik of Ebruu Tech Limited
- Chirag Gupta

- David Wilkins
- Dhamu Harker
- F0xman
- Grishma Sinha of Lucideus Tech
- Ismail Tasdelen
- jw c
- Kamal Elsayed Hussein
- lhf012
- Mansouri Badis
- Markus Wulftange of Code White
- Mohit Tirkey
- Pratik Luhana
- Rajat Sharma
- Sagar Gharbudve
- Sameer Phad
- Sanjay Singh Jhala
- Seth Duda
- Shubham Maheshwari
- Small Boys
- Vismit Sudhir Rakhecha (Druk) (2 reports)
- Wai Yan Aung
- Yashraj Choudhary
- Zhouyuan of Fortinet, Inc.

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:

- 16 July 2019
- 15 October 2019
- 14 January 2020
- 14 April 2020

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - April 2019 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
- Software Error Correction Support Policy

Modification History

Date	Note
2019-May-28	Rev 6. Updated Security-In-Depth Contributors section.
2019-May-16	Rev 5. Corrected CVE# in Enterprise Manager Products Suite risk matrix. CVE-2018-0161 replaced with CVE-2019-2726.
2019-May-3	Rev 4. Updated Security-In-Depth Contributors section.
2019-May-1	Rev 3. Updated CVSS score for CVE-2019-2633 and CVE-2019-2638.
2019-April-19	Rev 2. Updated credit for CVE-2019-2696.
2019-April-16	Rev 1. Initial Release.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 6 new security fixes 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 fixes 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 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2517	Core RDBMS	DBFS_ROLE	Oracle Net	No	9.1	Network	Low	High
CVE-2019-2516	Portable Clusterware	Grid Infrastructure User	Multiple	No	8.2	Local	Low	High
CVE-2019-2619	Portable Clusterware	Grid Infrastructure User	Multiple	No	8.2	Local	Low	High
CVE-2019-2518	Java VM	Create Session, Create Procedure	Multiple	No	7.5	Network	High	Low
CVE-2019-2571	RDBMS DataPump	DBA role	Oracle Net	No	6.6	Network	High	High
CVE-2019-2582	Core RDBMS	None	Oracle Net	Yes	5.3	Network	Low	None

Oracle Berkeley DB Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Berkeley DB. 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#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2019-2708	Data Store	Local Logon	Local Logon	No	3.3	Local	Low	Low	Nc

Oracle Commerce Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle Commerce. 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 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2019-2713	Oracle Commerce Merchandising	Asset Manager	HTTP	Yes	6.5	Network	Low	Non
CVE-2019-2659	Oracle Commerce Platform	Dynamo Application Framework	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-2712	Oracle Commerce Platform	Dynamo Application Framework	HTTP	Yes	6.1	Network	Low	Non

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 26 new security fixes for Oracle Communications Applications. 19 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 VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-7489	Oracle Communications Instant Messaging Server	Security (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2019-3822	Oracle Communications Operations Monitor	Security (curl)	HTTP	Yes	9.8	Network	Low
CVE-2018-11219	Oracle Communications Operations Monitor	Security (Redis)	RESP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Communications Pricing Design Center	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications	Admin server	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Service Broker	FileUpload (Apache Commons FileUpload)					
CVE-2016-1000031	Oracle Communications Service Broker Engineered System Edition	Admin server FileUpload (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2018-11236	Oracle Communications Session Border Controller	Security (glibc)	TCP	Yes	9.8	Network	Low
CVE-2018-11236	Oracle Enterprise Communications Broker	Security (glibc)	TCP	Yes	9.8	Network	Low
CVE-2018-11236	Oracle Enterprise Session Border Controller	Security (glibc)	TCP	Yes	9.8	Network	Low
CVE-2018-1258	Oracle Communications Unified Inventory Management	Security (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2017-5664	Oracle Communications Application Session Controller	Security (Apache Tomcat)	HTTP	Yes	8.1	Network	High
CVE-2016-1181	Oracle Communications Policy Management	Security (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2018-16864	Oracle Communications Session Border Controller	Security (Kernel)	None	No	7.8	Local	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-16864	Oracle Enterprise Communications Broker	Security (Kernel)	None	No	7.8	Local	Low
CVE-2018-16864	Oracle Enterprise Session Border Controller	Security (Kernel)	None	No	7.8	Local	Low
CVE-2018-1000180	Oracle Communications Application Session Controller	Security (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2018-0732	Oracle Communications Application Session Controller	Security (OpenSSL)	TLS	Yes	7.5	Network	Low
CVE-2018-0732	Oracle Communications EAGLE LNP Application Processor	Security (OpenSSL)	TLS	Yes	7.5	Network	Low
CVE-2017-5664	Oracle Communications Instant Messaging Server	Security (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2018-0732	Oracle Communications Operations Monitor	Security (OpenSSL)	TLS	Yes	7.5	Network	Low
CVE-2017-0861	Oracle Communications EAGLE Application Processor	Security (Kernel)	None	No	7.0	Local	High
CVE-2015-9251	Oracle Communications Interactive	Security (jQuery)	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Session Recorder						
CVE-2015-9251	Oracle Enterprise Operations Monitor	Security (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2018-12404	Oracle Communications Messaging Server	Security (NSS)	TLS	Yes	5.9	Network	High
CVE-2017-5753	Oracle Communications LSMS	Platform (Kernel)	None	No	5.6	Local	High
CVE-2017-5754	Oracle Communications LSMS	Platform (Kernel)	None	No	5.6	Local	High

Additional CVEs addressed are below:

- The fix for CVE-2016-1181 also addresses CVE-2016-1182.
- The fix for CVE-2017-0861 also addresses CVE-2017-15265, CVE-2018-1000004, CVE-2018-10901, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693 and CVE-2018-7566.
- The fix for CVE-2017-5664 also addresses CVE-2016-8735, CVE-2017-12617 and CVE-2018-11784.
- The fix for CVE-2018-0732 also addresses CVE-2016-7055, CVE-2017-3730, CVE-2017-3731, CVE-2017-3732, CVE-2017-3733, CVE-2017-3735, CVE-2017-3736, CVE-2017-3738, CVE-2018-0733, CVE-2018-0734, CVE-2018-0737 and CVE-2018-0739.
- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The fix for CVE-2018-11219 also addresses CVE-2018-11218.
- The fix for CVE-2018-11236 also addresses CVE-2018-11237 and CVE-2018-6485.
- The fix for CVE-2018-12404 also addresses CVE-2018-12384.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-16864 also addresses CVE-2018-16865.
- The fix for CVE-2018-7489 also addresses CVE-2017-7525.
- The fix for CVE-2019-3822 also addresses CVE-2018-16890 and CVE-2019-3823.

Oracle Construction and Engineering Suite Risk Matrix

This Critical Patch Update contains 8 new security fixes for the Oracle Construction and Engineering Suite. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2016-1000031	Primavera P6 Enterprise Project Portfolio Management	Web Access (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Primavera P6 Enterprise Project Portfolio Management	Web Access (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Primavera Unifier	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Primavera Unifier	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-11763	Instantis EnterpriseTrack	Core (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	
CVE-2018-0734	Primavera P6 Enterprise Project Portfolio Management	Project Manager (OpenSSL)	TLS	Yes	5.9	Network	High	
CVE-2018-11784	Instantis EnterpriseTrack	Core (Apache Tomcat)	HTTP	Yes	4.3	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-2701	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	No	4.3	Network	Low	

Additional CVEs addressed are below:

- The fix for CVE-2018-0734 also addresses CVE-2018-0735 and CVE-2018-5407.
- The fix for CVE-2018-11763 also addresses CVE-2017-9798.
- The fix for CVE-2018-11784 also addresses CVE-2018-8034.
- The fix for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 35 new security fixes for the Oracle E-Business Suite. 33 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 fixes 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 April 2019 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 (April 2019), My Oracle Support Note 2514102.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2638	Oracle General	Consolidation Hierarchy	HTTP	No	9.9	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
	Ledger	Viewer						
CVE-2019-2633	Oracle Work in Process	Messages	HTTP	No	9.9	Network	Low	Lo
CVE-2019-2663	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2682	Oracle Applications Framework	Attachments / File Upload	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2665	Oracle Common Applications	CRM User Management Framework	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2639	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2671	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2675	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2600	Oracle Email Center	Message Display	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2651	Oracle Email Center	Message Display	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2661	Oracle Email Center	Message Display	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2655	Oracle Interaction Center Intelligence	Business Intelligence (OLTP)	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2652	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2583	Oracle iSupplier Portal	Attachments	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2660	Oracle Knowledge Management	Setup, Admin	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2604	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2664	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2677	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2551	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2603	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2653	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2654	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2662	Oracle Territory Management	Territory Administration	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2640	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2641	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2642	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2643	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2018-0734	Application Server	Technology Stack Triage (OpenSSL)	HTTPS	Yes	5.9	Network	High	No
CVE-2019-2621	Oracle Application Object Library	Diagnostics	HTTP	Yes	4.7	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2669	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2676	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2670	Oracle Marketing	Marketing Administration	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2673	Oracle Marketing	Marketing Administration	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2674	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2622	Oracle Service	Renewals	HTTP	Yes	4.7	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
	Contracts							

Additional CVEs addressed are below:

- The fix for CVE-2018-0734 also addresses CVE-2018-0735 and CVE-2018-5407.

Oracle Enterprise Manager Products Suite Risk Matrix

This Critical Patch Update contains 11 new security fixes for the Oracle Enterprise Manager Products Suite. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these fixes are applicable to client-only installations, i.e., installations that do not have the Oracle Enterprise Manager Products Suite 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 fixes 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 April 2019 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 April 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2498664.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2016-1000031	Enterprise Manager Ops Center	Networking (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P Re
CVE-2016-4000	Oracle Configuration Manager	Collector of Config and Diag (Jython)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1258	Enterprise Manager Base Platform	Enterprise Manager Install (Spring Framework)	HTTP	No	8.8	Network	Low	L
CVE-2018-1258	Enterprise Manager Ops Center	Networking (Spring Framework)	HTTP	No	8.8	Network	Low	L
CVE-2018-11763	Enterprise Manager Ops Center	Networking (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle Business Transaction Management	Security (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-1656	Enterprise Manager Base Platform	Agent Next Gen (IBM Java)	HTTP	Yes	6.5	Network	Low	N
CVE-2019-2726	Enterprise Manager Ops Center	Services Integration	HTTP	No	6.3	Network	High	L
CVE-2019-2557	Oracle Application Testing Suite	Load Testing for Web Apps	HTTP	No	6.3	Network	Low	L
CVE-2018-0734	Enterprise Manager Base Platform	Discovery Framework (OpenSSL)	TLS	Yes	5.9	Network	High	N
CVE-2018-0734	Enterprise Manager Ops Center	Networking (OpenSSL)	TLS	Yes	5.9	Network	High	N

Additional CVEs addressed are below:

- The fix for CVE-2018-0734 also addresses CVE-2018-0735 and CVE-2018-5407.
- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The fix for CVE-2018-11763 also addresses CVE-2018-17189, CVE-2018-17199 and CVE-2019-0190.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257 and CVE-2018-15756.
- The fix for CVE-2018-1656 also addresses CVE-2018-12539.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 14 new security fixes for Oracle Financial Services Applications. 13 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-2016-1000031	Oracle Banking Platform	Collections (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N
CVE-2016-1000031	Oracle FLEXCUBE Private Banking	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1258	Oracle FLEXCUBE Private Banking	Core (Spring Framework)	HTTP	No	8.8	Network	Low	L
CVE-2018-11775	Oracle FLEXCUBE Private Banking	Core (Apache ActiveMQ)	HTTP	Yes	6.8	Network	High	N
CVE-2015-9251	Oracle Financial Services Analytical	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Applications Infrastructure							
CVE-2015-9251	Oracle Financial Services Asset Liability Management	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Data Integration Hub	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Funds Transfer Pricing	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Hedge Management and IFRS Valuations	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Liquidity Risk Management	Internal Operations (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Loan Loss Forecasting and Provisioning	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Market Risk Measurement	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	and Management							
CVE-2015-9251	Oracle Financial Services Profitability Management	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle Financial Services Reconciliation Framework	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	N

Additional CVEs addressed are below:

- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Food and Beverage 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#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2015-9251	Oracle Hospitality Reporting and Analytics	Report (jQuery)	HTTP	Yes	6.1	Network	Low	None	Rec

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 53 new security fixes for Oracle Fusion Middleware. 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.

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 fixes 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 April 2019 Critical Patch Update 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 April 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2498664.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2016-1000031	Oracle API Gateway	Oracle API Gateway (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-19362	Oracle Business Process Management Suite	Runtime Engine (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2015-3253	Oracle Data Integrator	Install, config, upgrade (Apache Groovy)	HTTP	Yes	9.8	Network	Low	N
CVE-2016-1000031	Oracle Endeca Information Discovery Integrator	Other Issues (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-3822	Oracle HTTP Server	Web Listener (curl)	HTTP	Yes	9.8	Network	Low	N
CVE-2016-1000031	Oracle Identity Analytics	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2017-5645	Oracle JDeveloper	None (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-8287	Oracle Outside In Technology	Installation (FreeType)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-8105	Oracle Outside In Technology	Installation (FreeType)	HTTP	Yes	9.8	Network	Low	N
CVE-2016-1000031	Oracle WebCenter Portal	Security Framework (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-19362	Oracle WebCenter Portal	Security Framework (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2658	Oracle WebLogic Server	WLS Core Components	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2646	Oracle WebLogic Server	EJB Container	T3	Yes	9.8	Network	Low	N
CVE-2019-2645	Oracle WebLogic Server	WLS Core Components	Multiple	Yes	9.8	Network	Low	N
CVE-2018-1258	Oracle WebLogic Server	WLS Core Components (Spring Framework)	HTTP	No	8.8	Network	Low	L
CVE-2019-2578	Oracle WebCenter Sites	Advanced UI	HTTP	Yes	8.6	Network	Low	N
CVE-2019-2595	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	Yes	8.2	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2706	Oracle Business Process Management Suite	BPM Foundation Services	HTTP	Yes	8.2	Network	Low	N
CVE-2019-2705	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	8.2	Network	Low	N
CVE-2018-14718	Oracle JDeveloper	Oracle JDeveloper (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2019-2601	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	No	7.6	Network	Low	L
CVE-2018-1000180	Oracle API Gateway	Oracle API Gateway (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-11761	Oracle Business Process Management Suite	Runtime Engine (Apache Tika)	HTTP	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle Managed File Transfer	MFT Runtime Server (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle SOA Suite	B2B Engine (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	N
CVE-2019-2647	Oracle WebLogic Server	WLS - Web Services	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2648	Oracle WebLogic Server	WLS - Web Services	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2649	Oracle WebLogic Server	WLS - Web Services	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2650	Oracle WebLogic Server	WLS - Web Services	HTTP	Yes	7.5	Network	Low	N
CVE-2018-8013	Oracle Data Integrator	Install, config, upgrade (Apache Batik)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-2608	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	N
CVE-2019-2616	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	Yes	7.2	Network	Low	N
CVE-2018-1305	FMW Platform	Provisioning (Apache Tomcat)	HTTP	No	6.5	Network	Low	L
CVE-2018-1305	Oracle Managed File Transfer	MFT Runtime Server (Apache Tomcat)	HTTP	No	6.5	Network	Low	L
CVE-2019-2609	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N
CVE-2019-2610	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N
CVE-2019-2611	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2612	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N
CVE-2019-2613	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N
CVE-2015-9251	Oracle Fusion Middleware MapViewer	Install (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle JDeveloper	ADF Faces (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2018-0734	Oracle API Gateway	Oracle API Gateway (OpenSSL)	HTTPS	Yes	5.9	Network	High	N
CVE-2018-0734	Oracle Tuxedo	SSL/TLS (OpenSSL)	HTTPS	Yes	5.9	Network	High	N
CVE-2019-2618	Oracle WebLogic Server	WLS Core Components	HTTP	No	5.5	Network	Low	H
CVE-2019-2576	Oracle Service Bus	Web Container	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2572	Oracle SOA Suite	Fabric Layer	HTTP	Yes	5.3	Network	Low	N
CVE-2018-0495	Oracle Traffic Director	Security (NSS)	None	No	5.1	Local	High	N
CVE-2019-2568	Oracle WebLogic Server	WLS Core Components	HTTP	No	5.0	Network	Low	L
CVE-2019-2588	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	No	4.9	Network	Low	H
CVE-2019-2615	Oracle WebLogic Server	WLS Core Components	HTTP	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-2019-2579	Oracle WebCenter Sites	Advanced UI	HTTP	No	4.3	Network	Low	L
CVE-2019-2605	Oracle Business Intelligence Enterprise Edition	Web Catalog	HTTP	Yes	3.4	Network	High	N
CVE-2019-2720	Oracle Data Integrator	ODI Tools	HTTP	No	3.1	Network	High	L

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 fix for CVE-2017-8287 also addresses CVE-2017-8105.
- The fix for CVE-2018-0734 also addresses CVE-2018-0735 and CVE-2018-5407.
- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-1305 also addresses CVE-2018-1304.
- The fix for CVE-2018-14718 also addresses CVE-2018-14719, CVE-2018-14720 and CVE-2018-14721.
- The fix for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.
- The fix for CVE-2019-3822 also addresses CVE-2018-16890 and CVE-2019-3823.

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle Health Sciences Applications. 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 3.0			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2016-1000031	Oracle Healthcare Master Person Index	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-2629	Oracle Health Sciences Data Management Workbench	User Interface	HTTP	No	5.4	Network	Low	L

Oracle Hospitality Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2016-1000031	Oracle Hospitality Guest Access	Base (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-2702	Oracle Hospitality Cruise Dining Room Management	Web Service	HTTP	Yes	9.3	Network	Low	No
CVE-2016-7103	Oracle Hospitality Cruise Fleet Management	FMS Suite (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2018-11763	Oracle Hospitality Guest Access	Base (Apache HTTP Server)	HTTP	Yes	5.9	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2018-11784	Oracle Hospitality Guest Access	Base (Apache Tomcat)	HTTP	Yes	4.3	Network	Low	No

Additional CVEs addressed are below:

- The fix for CVE-2016-7103 also addresses CVE-2015-9251.
- The fix for CVE-2018-11784 also addresses CVE-2018-8034.

Oracle Java SE Risk Matrix

This Critical Patch Update contains 5 new security fixes 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.

The CVSS scores below assume that a user running a Java applet or Java Web Start application (in Java SE 8) has administrator privileges (typical on Windows). When the user does not run with administrator privileges (typical on Solaris and Linux), the corresponding CVSS impact scores for Confidentiality, Integrity, and Availability are "Low" instead of "High", lowering the CVSS Base Score. For example, a Base Score of 9.6 becomes 7.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2699	Java SE	Windows DLL	Multiple	Yes	9.0	Network	High	None	
CVE-2019-2697	Java SE	2D	Multiple	Yes	8.1	Network	High	None	
CVE-2019-2698	Java SE	2D	Multiple	Yes	8.1	Network	High	None	
CVE-2019-2602	Java SE, Java SE Embedded	Libraries	Multiple	Yes	7.5	Network	Low	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2684	Java SE, Java SE Embedded	RMI	Multiple	Yes	5.9	Network	High	None	

Notes:

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.

2. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), 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).

3. 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.

Oracle JD Edwards Products Risk Matrix

This Critical Patch Update contains 8 new security fixes for Oracle JD Edwards Products. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2017-5645	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
		(Apache Log4j)						
CVE-2018-12023	JD Edwards EnterpriseOne Tools	EnterpriseOne Mobility Sec (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2018-12023	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2018-12023	JD Edwards EnterpriseOne Tools	Web Runtime (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2018-0732	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure SEC (OpenSSL)	JDENET	Yes	7.5	Network	Low	N
CVE-2019-2565	JD Edwards World Technical Foundation	Service Enablement	HTTP	Yes	7.5	Network	Low	N
CVE-2015-9251	JD Edwards EnterpriseOne Tools	Web Runtime (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-2564	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	No	4.3	Network	Low	L

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- The fix for CVE-2018-12023 also addresses CVE-2018-11307 and CVE-2018-12022.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 45 new security fixes for Oracle MySQL. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-2632	MySQL Server	Server : Pluggable Auth	MySQL Protocol	Yes	7.5	Network	Low	Nc
CVE-2019-2693	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lc
CVE-2019-2694	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lc
CVE-2019-2695	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lc
CVE-2019-2692	MySQL Connectors	Connector/J	JDBC	No	6.3	Local	High	Hi
CVE-2019-1559	MySQL Connectors	Connector/ODBC (OpenSSL)	TLS	Yes	5.9	Network	High	Nc
CVE-2019-1559	MySQL Server	Server: Compiling (OpenSSL)	MySQL Protocol	Yes	5.9	Network	High	Nc
CVE-2018-3123	MySQL Server	Server: libmysqld	MySQL Protocol	Yes	5.9	Network	High	Nc
CVE-2019-2623	MySQL Server	Server: Options	MySQL Protocol	No	5.3	Network	High	Lc
CVE-2018-0734	MySQL Enterprise Backup	Enterprise Backup (OpenSSL)	TLS	No	5.1	Local	High	Nc
CVE-2019-2634	MySQL Server	Server: Replication	MySQL Protocol	No	5.1	Local	High	Nc
CVE-2019-2580	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2585	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-2593	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2624	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2628	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2566	MySQL Server	Server: Audit Plug-in	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2626	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2644	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2631	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2581	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2596	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2607	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2625	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2681	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2685	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2686	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2687	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-2688	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2689	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2683	MySQL Server	Server: Options	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2592	MySQL Server	Server: PS	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2587	MySQL Server	Server: Partition	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2635	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2584	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2589	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2606	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2620	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2627	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2691	MySQL Server	Server: Security: Roles	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2019-2636	MySQL Server	Server: Group Replication Plugin	MySQL Procotol	No	4.4	Network	High	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-2614	MySQL Server	Server: Replication	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2019-2617	MySQL Server	Server: Replication	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2019-2630	MySQL Server	Server: Replication	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2019-1559	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	None	No	0.0	Local	Low	Nc

Notes:

1. MySQL Enterprise Monitor is not vulnerable to this CVE because it does not use the SSL/TLS functionality included in OpenSSL. The CVSS v3.0 Base Score for this CVE in the National Vulnerability Database (NVD) is 5.9.

Additional CVEs addressed are below:

- The fix for CVE-2018-0734 also addresses CVE-2018-5407.

Oracle PeopleSoft Products Risk Matrix

This Critical Patch Update contains 12 new security fixes for Oracle PeopleSoft Products. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-2598	PeopleSoft Enterprise PeopleTools	SQR	HTTP	No	8.7	Network	Low	H
CVE-2019-2590	PeopleSoft Enterprise	Job Opening	HTTP	Yes	8.2	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
	HCM Talent Acquisition Manager							
CVE-2018-1000180	PeopleSoft Enterprise PeopleTools	Security (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-2594	PeopleSoft Enterprise PT PeopleTools	Application Server	HTTP	No	6.8	Network	High	L
CVE-2019-2707	PeopleSoft Enterprise ELM Enterprise Learning Management	Application Search	HTTP	Yes	6.1	Network	Low	No
CVE-2019-2591	PeopleSoft Enterprise HRMS	Candidate Gateway	HTTP	Yes	6.1	Network	Low	No
CVE-2019-2637	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.1	Network	Low	No
CVE-2018-0734	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	5.9	Network	High	No
CVE-2019-2597	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	5.4	Network	Low	No
CVE-2019-2700	PeopleSoft Enterprise ELM	Enterprise Learning Mgmt	HTTP	No	4.3	Network	Low	L
CVE-2019-2573	PeopleSoft Enterprise PeopleTools	Fluid Homepage & Navigation	HTTP	Yes	4.3	Network	Low	No
CVE-2019-2586	PeopleSoft Enterprise PT PeopleTools	RemoteCall	HTTP	No	4.3	Network	Low	L

Additional CVEs addressed are below:

- The fix for CVE-2018-0734 also addresses CVE-2018-0735 and CVE-2018-5407.
- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 24 new security fixes for Oracle Retail Applications. 20 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 VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2014-9515	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations (Dozer)	HTTP	Yes	9.8	Network	Low
CVE-2019-3772	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations (Spring Framework)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Retail Order Broker	System Administration (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2017-5533	Oracle Retail Order Broker	System Administration (Jasper)	HTTP	Yes	9.8	Network	Low
CVE-2018-19362	Oracle Retail Workforce Management Software	Framework (jQuery)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Retail Xstore Point of Service	Xenvironment (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-3314	MICROS Relate CRM Software	Customer	HTTP	No	8.2	Network	High
CVE-2018-12023	Oracle Retail Merchandising System	Documentation (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2018-14718	Oracle Retail Merchandising System	Documentation (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2018-3120	MICROS Lucas	Security	HTTP	No	7.5	Network	High
CVE-2018-2880	MICROS Retail-J	Back Office	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Retail Invoice Matching	Security (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Retail Order Broker	System Administration (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2018-11763	Oracle Retail Xstore Point of Service	Point of Sale (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low
CVE-2018-11763	Oracle Retail Xstore Point of Service	Xstore Office (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low
CVE-2018-1000180	Oracle Retail Xstore Point of Service	Xenvironment (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2019-2424	Oracle Retail Convenience Store Back Office	Level 3 Maintenance Functions	HTTP	Yes	7.3	Network	Low
CVE-2019-2558	Oracle Retail Point-of-Service	Infrastructure	HTTP	Yes	7.3	Network	Low
CVE-2018-1305	MICROS Relate CRM Software	Internal Operations	HTTP	No	6.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
		(Apache Tomcat)					
CVE-2015-9251	Oracle Retail Allocation	General (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2015-9251	Oracle Retail Invoice Matching	Security (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2018-3312	Oracle Retail Customer Engagement	Segment	HTTP	No	5.5	Network	High
CVE-2018-11784	Oracle Retail Order Broker	System Administration (Apache Tomcat)	HTTP	Yes	4.3	Network	Low
CVE-2018-11784	Oracle Retail Order Broker	Upgrade Install (Apache Tomcat)	HTTP	Yes	4.3	Network	Low

Additional CVEs addressed are below:

- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The fix for CVE-2018-11784 also addresses CVE-2018-8034.
- The fix for CVE-2018-12023 also addresses CVE-2018-12022.
- The fix for CVE-2018-1305 also addresses CVE-2018-11784 and CVE-2018-1304.
- The fix for CVE-2018-14718 also addresses CVE-2018-14719, CVE-2018-14720, CVE-2018-14721 and CVE-2018-19362.
- The fix for CVE-2018-19362 also addresses CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361 and CVE-2018-7489.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 8 new security fixes for Oracle Siebel CRM. 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 3.0 RISK (s			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2014-0114	Oracle Knowledge	Information Manager Console (Apache Commons BeanUtils)	HTTP	Yes	9.8	Network	Low	Non
CVE-2016-1000031	Oracle Knowledge	Information Manager Console (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	Non
CVE-2016-2141	Oracle Knowledge	Information Manager Console (JGroups)	HTTP	Yes	9.8	Network	Low	Non
CVE-2015-1832	Oracle Knowledge	Information Manager Console (Apache Derby)	HTTP	Yes	9.1	Network	Low	Non
CVE-2016-0635	Oracle Knowledge	AnswerFlow (Spring Framework)	HTTP	No	8.8	Network	Low	Low
CVE-2014-0107	Oracle Knowledge	Information Manager Console (Apache Xalan)	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2719	Oracle Knowledge	Web Applications (InfoCenter)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-2570	Siebel Core - Server BizLogic Script	Integration - Scripting	HTTP	No	4.7	Network	Low	High

Additional CVEs addressed are below:

- The fix for CVE-2014-0114 also addresses CVE-2016-1000031 and CVE-2016-3092.
- The fix for CVE-2015-1832 also addresses CVE-2016-2141.
- The fix for CVE-2016-1000031 also addresses CVE-2016-3092.
- The fix for CVE-2016-2141 also addresses CVE-2015-1832.

Oracle Sun Systems Products Suite Risk Matrix

This Critical Patch Update contains 3 new security fixes for the Oracle Sun Systems Products Suite. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2019-2704	Oracle Solaris	IPS Package Manager	HTTP	Yes	5.3	Network	Low	None	
CVE-2018-20685	Oracle Solaris	SunSSH	SSH	Yes	5.3	Network	High	None	Re
CVE-2019-2577	Oracle Solaris	File Locking Services	None	No	3.3	Local	Low	Low	

Oracle Supply Chain Products Suite Risk Matrix

This Critical Patch Update contains 5 new security fixes for the Oracle Supply Chain Products Suite. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2016-1000031	Agile Recipe Management for Pharmaceuticals	Recipe (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Agile PLM	Application Server (Apache	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
		Commons FileUpload)					
CVE-2019-2567	Oracle Configurator	Active Model Generation	HTTP	Yes	7.5	Network	Low
CVE-2019-2709	Oracle Transportation Management	Security	HTTP	Yes	6.1	Network	Low
CVE-2019-2575	Oracle AutoVue 3D Professional Advanced	Format Handling - 2D	HTTP	Yes	5.3	Network	Low

Oracle Support Tools Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Support Tools. 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 3.0 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2015-9251	OSS Support Tools	Remote Diagnostic Agent (jQuery)	Multiple	Yes	6.1	Network	Low	None	Requ

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 6 new security fixes for Oracle Utilities Applications. 5 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-2017-14952	Oracle Utilities Framework	Common (icu4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-8088	Oracle Utilities Framework	Common (slf4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2016-1000031	Oracle Utilities Framework	User Interface (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-1258	Oracle Utilities Network Management System	Web Gateway client (Spring Framework)	T3	No	8.8	Network	Low	L
CVE-2015-9251	Oracle Real-Time Scheduler	Mobile Platform (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2015-9251	Oracle Utilities Mobile Workforce Management	Mobile Platform (jQuery)	HTTP	Yes	6.1	Network	Low	No

Additional CVEs addressed are below:

- The fix for CVE-2017-14952 also addresses CVE-2014-7923, CVE-2014-7926, CVE-2014-7940, CVE-2014-8146, CVE-2014-8147, CVE-2014-9654, CVE-2014-9911, CVE-2015-5922, CVE-2016-6293, CVE-2016-7415, CVE-2017-17484, CVE-2017-7867 and CVE-2017-7868.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 15 new security fixes for Oracle Virtualization. 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 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-3822	Oracle Secure Global Desktop	Core (curl)	HTTP	Yes	9.8	Network	Low	None	
CVE-2019-2656	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2680	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2696	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2703	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2721	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2722	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2723	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2657	Oracle VM VirtualBox	Core	None	No	7.8	Local	Low	Low	
CVE-2019-2690	Oracle VM VirtualBox	Core	None	No	7.8	Local	High	Low	
CVE-2019-2679	Oracle VM VirtualBox	Core	None	No	7.3	Local	Low	Low	
CVE-2019-2678	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2574	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-1559	Oracle Secure Global Desktop	Core (OpenSSL)	TLS	Yes	5.9	Network	High	None	
CVE-2018-11784	Oracle Secure Global Desktop	Application Server (Apache Tomcat)	HTTP	Yes	4.3	Network	Low	None	F

Additional CVEs addressed are below:

- The fix for CVE-2018-11784 also addresses CVE-2018-8034.
- The fix for CVE-2019-1559 also addresses CVE-2018-0734, CVE-2018-0735 and CVE-2018-5407.

- The fix for CVE-2019-3822 also addresses CVE-2018-16890 and CVE-2019-3823.