Oracle Critical Patch Update Advisory - July 2018

Oracle Critical Patch Update Advisory - July 2018

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 334 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 July 2018 Critical Patch Update: Executive Summary and Analysis.

Many industry experts anticipate that exploits leveraging known flaws in modern processor designs will continue to be disclosed for the foreseeable future (i.e., “Spectre” variants). For information related to these issues, please refer to:

- the January 2018 Critical Patch Update (and later) Advisories,
- the "Addendum to the January 2018 Critical Patch Update Advisory for Spectre (CVE-2017-5715, CVE-2017-5753) and Meltdown (CVE-2017-5754)" (Doc ID 2347948.1), and
- "Information about processor vulnerabilities CVE-2018-3640 ("Spectre v3a") and CVE-2018-3639 ("Spectre v4")" (Doc ID 2399123.1).

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, version 9.3.4	Oracle Supply Chain Products
Enterprise Manager Base Platform, versions 12.1.0.5, 13.2.x	Enterprise Manager
Enterprise Manager for Fusion Middleware, versions 12.1.0.5, 13.2.x	Enterprise Manager
Enterprise Manager for MySQL Database, versions 13.2.2.0.0 and prior	Enterprise Manager
Enterprise Manager for Oracle Database, versions 12.1.0.8, 13.2.2	Enterprise Manager
Enterprise Manager for Peoplesoft, versions 13.1.1.1, 13.2.1.1	Enterprise Manager
Enterprise Manager for Virtualization, versions 13.2.2, 13.2.3	Enterprise Manager
Enterprise Manager Ops Center, versions 12.2.2, 12.3.3	Enterprise Manager
FMW Platform, versions 12.2.1.2.0, 12.2.1.3.0	Fusion Middleware
Hardware Management Pack, version 11.3	Systems
Hyperion Data Relationship Management, version 11.1.2.4.330	Fusion Middleware
Hyperion Financial Reporting, version 11.1.2	Fusion Middleware
JD Edwards EnterpriseOne Tools, version 9.2	JD Edwards
JD Edwards World Security, versions A9.3, A9.3.1, A9.4	JD Edwards
MICROS 700 Series Tablet, versions Prior to BIOS 0.00.13ORC, Prior to BIOS 0.01.25ORC	MICROS 700 Series Tablet
MICROS Handheld Terminal, versions 2018, Android 4.4.4 Security Patch Bulletin prior to February 1	MICROS Handheld Terminal
MICROS Kitchen Display Controller, versions Prior to BIOS 0.00.16ORC	MICROS Kitchen Display System Hardware
MICROS Lucas, versions 2.9.5.3, 2.9.5.4, 2.9.5.5, 2.9.5.6	Retail Applications
MICROS Relate CRM Software, versions 10.8.x, 11.4.x	Retail Applications
MICROS Retail-J, versions 10.2.x, 11.0.x, 12.0.x, 12.1.x, 12.1.1.x, 12.1.2.x, 13.1.x	Retail Applications
MICROS Workstation 6, versions prior to BIOS 1.3.1.0, prior to BIOS 1.5.2.0, prior to BIOS 2.3.1.0	MICROS Workstation
MICROS XBR, versions 7.0.2, 7.0.4	Retail Applications

Affected Products and Versions	Patch Availability Document
MySQL Client, versions 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior, 8.0.11 and prior	MySQL
MySQL Connectors, versions 5.3.10 and prior, 8.0.11 and prior	MySQL
MySQL Enterprise Monitor, versions 3.4.7.4297 and prior, 4.0.4.5235 and prior, 8.0.0.8131 and prior	MySQL
MySQL Server, versions 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior, 8.0.11 and prior	MySQL
MySQL Workbench, versions 6.3.10 and prior, 8.0.11 and prior	MySQL
Oracle Agile Engineering Data Management, versions 6.1.3, 6.2.0, 6.2.1	Oracle Supply Chain Products
Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5, 9.3.6	Oracle Supply Chain Products
Oracle Agile PLM MCAD Connector, versions 3.3, 3.4, 3.5, 3.6	Oracle Supply Chain Products
Oracle Agile Product Lifecycle Management for Process, version 6.2.0.0	Oracle Supply Chain Products
Oracle API Gateway, version 11.1.2.4.0	Fusion Middleware
Oracle Application Testing Suite, version 10.1	Enterprise Manager
Oracle AutoVue VueLink Integration, versions 21.0.0, 21.0.1	Oracle Supply Chain Products
Oracle Banking Corporate Lending, versions 12.3.0, 12.4.0, 12.5.0, 14.0.0, 14.1.0	Oracle Financial Services Applications
Oracle Banking Payments, versions 12.2.0, 12.3.0, 12.4.0, 12.5.0, 14.1.0	Oracle Financial Services Applications
Oracle Banking Platform, versions 2.6.0, 2.6.1, 2.6.2	Oracle Banking Platform
Oracle BI Publisher, versions 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0	Fusion Middleware
Oracle Business Process Management Suite, versions 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0	Fusion Middleware
Oracle Communications Diameter Signaling Router (DSR), versions 7.x, 8.x	Oracle Communications Diamete Signaling Router
Oracle Communications EAGLE LNP Application Processor, version 10.x	Oracle Communications EAGLE I Application Processor
Oracle Communications Interactive Session Recorder, versions 5.x, 6.x	Oracle Communications Interact Session Recorder
Oracle Communications Messaging Server, version 3.x	Oracle Communications Convergence
Oracle Communications Network Charging and Control, versions 4.4.1.5.0, 5.0.0.1.0, 5.0.0.2.0, 5.0.1.0.0, 5.0.2.0.0	Oracle Communications Networl Charging and Control
Oracle Communications Policy Management, version 12.x	Oracle Communications Policy Management

Affected Products and Versions	Patch Availability Document
Oracle Communications Session Border Controller, versions ECz7.x, ECz8.x	Oracle Communications Session Border Controller
Oracle Communications User Data Repository, versions 10.x, 12.x	Oracle Communications User Da Repository
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1, 18.2	Database
Oracle E-Business Suite, versions 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7	E-Business Suite
Oracle Endeca Information Discovery Studio, versions 3.1, 3.2	Fusion Middleware
Oracle Enterprise Data Quality, version 12.2.1.3.0	Fusion Middleware
Oracle Enterprise Repository, versions 11.1.1.7.0, 12.1.3.0.0	Fusion Middleware
Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3.x, 8.0.x	Oracle Financial Services Analyti Applications Infrastructure
Oracle Financial Services Behavior Detection Platform, version 8.0.x	Oracle Financial Services Behavi Detection Platform
Oracle Financial Services Funds Transfer Pricing, versions 6.1.1, 8.0.x	Oracle Financial Services Funds Transfer Pricing
Oracle Financial Services Hedge Management and IFRS Valuations, versions 8.0.4, 8.0.5	Oracle Financial Services Hedge Management and IFRS Valuatior
Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.4, 8.0.5	Oracle Financial Services Loan L Forecasting and Provisioning
Oracle Financial Services Profitability Management, versions 6.1.1, 8.0.x	Oracle Financial Services Profitability Management
Oracle Financial Services Revenue Management and Billing, versions 2.3.0.2.0, 2.4.0.0.0, 2.4.0.1.0, 2.5.0.1.0, 2.5.0.2.0, 2.5.0.3.0	Oracle Financial Services Revenu Management and Billing
Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 12.3.0, 14.0.0, 14.1.0	Oracle Financial Services Applications
Oracle FLEXCUBE Investor Servicing, versions 12.0.4, 12.1.0, 12.3.0, 12.4.0	Oracle Financial Services Applications
Oracle FLEXCUBE Universal Banking, versions 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0	Oracle Financial Services Applications
Oracle Fusion Middleware, versions 12.2.1.2, 12.2.1.3	Fusion Middleware
Oracle Fusion Middleware MapViewer, versions 12.2.1.2, 12.2.1.3	Fusion Middleware
Oracle Global Lifecycle Management OPatchAuto, version All	Oracle Global Lifecycle Managen OPatchAuto
Oracle Hospitality Cruise Fleet Management System, version 9.x	Oracle Hospitality Cruise Fleet Management

Affected Products and Versions	Patch Availability Document
Oracle Hospitality Cruise Shipboard Property Management System, version 8.x	Oracle Hospitality Cruise Shipbo Property Management System
Oracle Hospitality Gift and Loyalty, version 9.0.0	Oracle Hospitality Gift and Loyal
Oracle Hospitality OPERA 5 Property Services, version 5.5.x	Oracle Hospitality OPERA 5 Prop Services
Oracle Hospitality Reporting and Analytics, version 9.0.0	Oracle Hospitality Reporting and Analytics
Oracle Hospitality Simphony, versions 2.8, 2.9, 2.10	Oracle Hospitality Simphony
Oracle iLearning, version 6.2	iLearning
Oracle Insurance Policy Administration, versions 10.0, 10.1, 10.2, 11.0	Oracle Insurance Applications
Oracle Internet Directory, version 11.1.1.9.0	Fusion Middleware
Oracle Java SE, versions 6u191, 7u181, 8u172, 10.0.1	Java SE
Oracle Java SE Embedded, version 8u171	Java SE
Oracle JDeveloper, versions 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0	Fusion Middleware
Oracle JRockit, version R28.3.18	Java SE
Oracle Outside In Technology, version 8.5.3	Fusion Middleware
Oracle Policy Automation, versions 10.4.7, 12.1.0, 12.1.1, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10	Oracle Policy Automation
Oracle Policy Automation Connector for Siebel, version 10.4.6	Oracle Policy Automation
Oracle Policy Automation for Mobile Devices, versions 10.4.7, 12.1.0, 12.1.1, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10	Oracle Policy Automation
Oracle Retail Back Office, versions 14.0, 14.1	Retail Applications
Oracle Retail Bulk Data Integration, version 16.0	Retail Applications
Oracle Retail Central Office, versions 14.0, 14.1	Retail Applications
Oracle Retail Clearance Optimization Engine, version 14.0.5	Retail Applications
Oracle Retail Convenience and Fuel POS Software, version 2.1.132	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 16.x, 17.x	Retail Applications
Oracle Retail Financial Integration, versions 13.2.x, 14.0.x, 14.1.x, 15.0.x, 16.0.x	Retail Applications
Oracle Retail Integration Bus, versions 12.0.x, 13.0.x, 13.1.x, 13.2.x, 14.0.0 14.1.0, 14.0.x, 14.1.x, 15.0, 15.0.x, 16.0, 16.0.x	Retail Applications
Oracle Retail Order Broker, versions 5.2, 15.0, 16.0	Retail Applications
Oracle Retail Point-of-Sale, versions 14.0, 14.1	Retail Applications

Affected Products and Versions	Patch Availability Document
Oracle Retail Point-of-Service, versions 14.0, 14.1	Retail Applications
Oracle Retail Predictive Application Server, version 15.0.3	Retail Applications
Oracle Retail Returns Management, versions 14.0, 14.1	Retail Applications
Oracle Retail Service Backbone, versions 14.0.x, 14.1.x, 15.0.x, 16.0.x	Retail Applications
Oracle Retail Service Layer, versions 12.0.x, 13.0.x, 13.1.x, 13.2.x, 14.0.x	Retail Applications
Oracle Secure Global Desktop, versions 5.3, 5.4	Virtualization
Oracle SOA Suite, versions 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0	Fusion Middleware
Oracle SuperCluster Specific Software, versions prior to 2.5.0	Systems
Oracle Transportation Management, versions 6.2, 6.3.7, 6.4.1	Oracle Supply Chain Products
Oracle Tuxedo, versions 12.1.1, 12.1.3, 12.2.2	Fusion Middleware
Oracle Utilities Framework, version 4.3.x	Oracle Utilities Applications
Oracle Utilities Network Management System, versions 1.12.x, 2.3.x	Oracle Utilities Applications
Oracle Utilities Work and Asset Management, version 1.9.1.2.12	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 5.2.16	Virtualization
Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0	Fusion Middleware
Oracle WebLogic Server, versions 10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3	Fusion Middleware
OSS Support Tools, versions prior to 18.3	Support Tools
PeopleSoft Enterprise CS Financial Aid, versions 9.0, 9.2	PeopleSoft
PeopleSoft Enterprise FIN Install, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Human Resources, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56	PeopleSoft
PeopleSoft HRMS, version 9.2	PeopleSoft
Primavera P6 Enterprise Project Portfolio Management, versions 8.4, 15.x, 16.x, 17.x	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.x, 17.x, 18.x	Oracle Construction and Engineering Suite
Siebel Applications, version 18.0	Siebel
Solaris, versions 10, 11.2, 11.3	Systems
Solaris Cluster, versions 3.3, 4.3	Systems
Sun ZFS Storage Appliance Kit (AK), versions prior to 8.7.20	Systems
Tape Library ACSLS, versions Prior to ACSLS 8.4.0-3	Systems

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://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 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:

- 0c0c0f: CVE-2018-2893
- Adam Willard: CVE-2018-3017, CVE-2018-3018
- Add of MeePwn working with Trend Micro's Zero Day Initiative: CVE-2018-3055
- Amin Moralic of Pure Hacking: CVE-2018-2953
- André Lenoir of Tehtris: CVE-2018-2991, CVE-2018-2993, CVE-2018-2996, CVE-2018-3012
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2018-3087, CVE-2018-3088, CVE-2018-3089, CVE-2018-3090
- Badcode of Knownsec 404 Team: CVE-2018-2893
- Bartłomiej Stasiek: CVE-2018-2900
- Behzad Najjarpour Jabbari, Secunia Research at Flexera Software: CVE-2018-2992, CVE-2018-3009, CVE-2018-3010, CVE-2018-3092, CVE-2018-3093, CVE-2018-3094, CVE-2018-3095, CVE-2018-3096, CVE-2018-3097, CVE-2018-3098, CVE-2018-3099, CVE-2018-3102, CVE-2018-3103, CVE-2018-3104
- Daniel Bleichenbacher of Google: CVE-2018-2972
- Dario Weißer: CVE-2018-3081
- David Litchfield of Apple: CVE-2018-2894
- Denis Andzakovic of Pulse Security: CVE-2018-2933, CVE-2018-2998
- Fabio Pires of NCC Group: CVE-2018-2907
- Faizal Hasanwala: CVE-2018-2936
- Gregory Draperi: CVE-2018-2938
- Gregory Smiley of Security Compass: CVE-2018-2955, CVE-2018-2957, CVE-2018-3000, CVE-2018-3001, CVE-2018-3002, CVE-2018-3003
- Jackson Thuraisamy of Security Compass: CVE-2018-2955, CVE-2018-2957
- Jakub Palaczynski of ING Services Polska: CVE-2018-2958
- Jayson Grace of Sandia National Laboratories: CVE-2018-2996
- Jim LaValley, Towerwall, Inc.: CVE-2018-2960, CVE-2018-2961, CVE-2018-2962, CVE-2018-2963, CVE-2018-2965, CVE-2018-2966, CVE-2018-2967, CVE-2018-2968, CVE-2018-2969
- John Beeson of Baker Hughes, a GE Company: CVE-2018-2976
- Krisorn Phochalam: CVE-2018-2899
- Liao Xinxi of NSFOCUS Security Team: CVE-2018-2893
- Lilei of Venustech ADLab: CVE-2018-2893
- Linpei Sheng of 360 Enterprise Security Group: CVE-2018-2997

- Lokesh Sharma: CVE-2018-2934
- Lukasz Plonka of ING Services Polska: CVE-2018-2915, CVE-2018-2987
- Marcin Wołoszyn of ING Services Polska: CVE-2018-2958
- Mathew Nash of NCC Group: CVE-2018-2907
- Matthew E. Fulton: CVE-2018-3109
- Matthew Fulton of Pure Hacking: CVE-2018-2953
- Mingxuan Song of CNCERT: CVE-2018-2894
- Neil Kettle of Trustwave Spiderlabs: CVE-2018-2892
- Nicolas Verdier of Tehtris: CVE-2018-2991, CVE-2018-2993, CVE-2018-2996, CVE-2018-3012
- Niklas Baumstark working with Trend Micro's Zero Day Initiative: CVE-2018-3055, CVE-2018-3085, CVE-2018-3091
- Pawan Patil of Electronic Arts: CVE-2018-2994, CVE-2018-2995
- Pawel Gocyla: CVE-2018-2925
- Rich Mirch: CVE-2018-2939
- Root Object working with Trend Micro's Zero Day Initiative: CVE-2018-3086
- Sidney Markowitz: CVE-2018-2942
- Thomas Barabosch of Fraunhofer FKIE: CVE-2018-3005
- Xu Yuanzhen of Alibaba Cloud Security Team: CVE-2018-2893
- Zhong Zhaochen: CVE-2018-2964

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.:

- Jim LaValley, Towerwall, Inc.
- Lokesh Sharma (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:

- Adam Willard
- Anil Tom
- Cedric Zirtacic
- Cem Onat Karagun (6 reports)
- Dmitry Ivanov
- Elif Zehra Karabiber (2 reports)
- Omkar Avasthi
- Jacob 'kobsoN' Hazak
- Jamal Elfitory
- Jayesh Patel
- Jose Carlos Exposito Bueno
- Kerem TAMCI
- Mushraf Mustafa
- Nalla Muthu
- Nick Marcoccio @1oopho1e
- re4lity of Polaris Lab
- Richard Cocks
- Rick Ramgattie
- Sara Badran
- TrendyTofu working with Trend Micro's Zero Day Initiative
- Viral Bhatt
- Vishakh B
- Vismit Rakhecha
- Youssef A. Mohamed aka GeneralEG

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 October 2018
- 15 January 2019
- 16 April 2019
- 16 July 2019

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - July 2018 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
2018-October-12	Rev 8. Updated credit for CVE-2018-3055.
2018-September-18	Rev 7. Updated credit for CVE-2018-2996.
2018-September-4	Rev 6. Updated CVSS score of CVE-2018-2943.
2018-August-2	Rev 5. Updated affected versions of CVE-2018-2894 and CVE-2018-7489 for WebLogic Server.
2018-July-27	Rev 4. Updated On-Line Presence Security Contributors.
2018-July-23	Rev 3. Updated CVE-2018-2938.
2018-July-20	Rev 2. Updated CVE-2018-2938.
2018-July-17	Rev 1. Initial Release.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 4 new security fixes for the Oracle Database Server divided as follows:

- 3 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.
- 1 new security fix for Oracle Global Lifecycle Management. 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 RIS			
					Base Score	Attack Vector	Attack Complexity	Privs Req'd
CVE-2017-15095	Oracle Spatial (jackson-databind)	None	Multiple	Yes	9.8	Network	Low	None
CVE-2018-2939	Core RDBMS	Local Logon	Local Logon	No	8.4	Local	Low	Low
CVE-2018-3004	Java VM	Create Session, Create Procedure	Multiple	No	5.3	Network	High	Low

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Global Lifecycle Management. 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 R			
					Base Score	Attack Vector	Attack Complexity	Pri Req
CVE-2018-7489	Oracle Global Lifecycle Management OPatchAuto	DB specific extensions (jackson-databind)	Multiple	Yes	9.8	Network	Low	No

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 14 new security fixes for Oracle Communications Applications. 10 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 Complexity
CVE-2016-2099	Oracle Communications User Data Repository	Security (Apache Xerces)	HTTP	Yes	9.8	Network	Low
CVE-2016-0714	Oracle Communications Policy Management	Security (Apache Tomcat)	HTTP	No	8.8	Network	Low
CVE-2016-2176	Oracle Communications Policy Management	Security (OpenSSL)	TLS	Yes	8.2	Network	Low
CVE-2017-7525	Oracle Communications Policy Management	Security (Apache Struts 2)	HTTP	Yes	8.1	Network	High
CVE-2016-5195	Oracle Communications Policy Management	Platform (Kernel)	None	No	7.8	Local	Low
CVE-2017-6074	Oracle Communications Session Border Controller	Security (Kernel)	None	No	7.8	Local	Low
CVE-2017-0379	Oracle Communications Interactive Session Recorder	Security (libgcrypt)	HTTP	Yes	7.5	Network	Low
CVE-2015-7940	Oracle Communications Policy Management	CMP (Bouncy Castle)	TLS	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complexity
CVE-2017-5662	Oracle Communications Diameter Signaling Router (DSR)	Security (Apache Batik)	HTTP	No	7.3	Network	Low
CVE-2018-2904	Oracle Communications EAGLE LNP Application Processor	GUI	HTTP	Yes	6.5	Network	Low
CVE-2018-0739	Oracle Communications Network Charging and Control	Security (OpenSSL)	TLS	Yes	6.5	Network	Low
CVE-2017-3633	Oracle Communications Policy Management	Security (MySQL)	Multiple	Yes	6.5	Network	High
CVE-2018-2936	Oracle Communications Messaging Server	Web Client	HTTP	Yes	6.1	Network	Low
CVE-2015-5600	Oracle Communications Policy Management	Security (OpenSSH)	SSH	Yes	5.3	Network	Low

Additional CVEs addressed are below:

- The fix for CVE-2015-5600 also addresses CVE-2014-2532.
- The fix for CVE-2016-0714 also addresses CVE-2014-0230, CVE-2014-7810, CVE-2015-5174, CVE-2015-5345, CVE-2015-5346, CVE-2015-5351, CVE-2016-0706 and CVE-2016-3092.
- The fix for CVE-2016-2099 also addresses CVE-2016-4463.
- The fix for CVE-2016-2176 also addresses CVE-2016-2105, CVE-2016-2106, CVE-2016-2107 and CVE-2016-2109.
- The fix for CVE-2017-3633 also addresses CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653 and CVE-2017-3732.

- The fix for CVE-2017-7525 also addresses CVE-2017-15707 and CVE-2018-1327.

Oracle Construction and Engineering Suite Risk Matrix

This Critical Patch Update contains 11 new security fixes for the Oracle Construction and Engineering Suite. 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			
					Base Score	Attack Vector	Attack Complexity	Pri Re
CVE-2018-2966	Primavera Unifier	Core	HTTP	Yes	7.4	Network	Low	No
CVE-2018-2968	Primavera Unifier	Core	HTTP	Yes	6.5	Network	Low	No
CVE-2016-4055	Primavera Unifier	Core (Moment)	HTTP	No	6.5	Network	Low	Lo
CVE-2018-2960	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	Yes	6.1	Network	Low	No
CVE-2018-2961	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	Yes	6.1	Network	Low	No
CVE-2018-2965	Primavera Unifier	Core	HTTP	Yes	6.1	Network	Low	No
CVE-2016-7103	Primavera Unifier	Core (jQueryUI)	HTTP	Yes	6.1	Network	Low	No
CVE-2018-2967	Primavera Unifier	Core	None	No	5.3	Physical	Low	No
CVE-2018-2962	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	No	4.4	Network	High	Lo
CVE-2018-2963	Primavera P6 Enterprise Project	Web Access	HTTP	No	4.3	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pri Re
	Portfolio Management							
CVE-2018-2969	Primavera Unifier	Core	HTTP	No	4.3	Network	Low	Lo

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 14 new security fixes for the Oracle E-Business Suite. 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.

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 July 2018 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 2018), My Oracle Support Note 2379675.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2993	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-3017	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2995	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-3018	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-3008	Oracle Marketing	User Interface	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-2953	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-2997	Oracle Scripting	Script Author	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-2991	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	Nc
CVE-2018-3012	Oracle Trade Management	User Interface	HTTP	Yes	8.2	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2996	Oracle Applications Manager	Oracle Diagnostics Interfaces	HTTP	Yes	7.5	Network	Low	Nc
CVE-2018-2954	Oracle Order Management	Product Diagnostic Tools	None	No	7.0	Local	High	Lc
CVE-2018-2988	Oracle Marketing	Products	HTTP	Yes	6.9	Network	High	Nc
CVE-2018-2934	Oracle Application Object Library	Attachments / File Upload	HTTP	Yes	5.3	Network	Low	Nc
CVE-2018-2994	Oracle iStore	Shopping Cart	HTTP	Yes	5.3	Network	Low	Nc

Oracle Enterprise Manager Products Suite Risk Matrix

This Critical Patch Update contains 16 new security fixes for the Oracle Enterprise Manager Products Suite. All 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 July 2018 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 2018 Patch Availability Document for Oracle Products, My Oracle Support Note 2394520.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pri Re
CVE-2017-5645	Enterprise Manager Base Platform	Installer (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2017-5645	Enterprise Manager Base Platform	Security Framework (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2017-5645	Enterprise Manager for Fusion Middleware	Application Replay (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2017-5645	Enterprise Manager for Fusion Middleware	FMW Plugin for CC (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2017-5645	Enterprise Manager for MySQL Database	EM Plugin: General (Apache Log4j)	Log4j	Yes	9.8	Network	Low	No
CVE-2017-5645	Enterprise Manager for Oracle Database	Provisioning (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2017-5645	Enterprise Manager for Peoplesoft	PSEM Plugin	HTTP	Yes	9.8	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pri Re
		(Apache Log4j)						
CVE-2018-7489	Enterprise Manager for Virtualization	Plug-In Lifecycle (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-1275	Enterprise Manager Ops Center	Networking (Spring Framework)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-1275	Oracle Application Testing Suite	Load Testing for Web Apps (Spring Framework)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-2976	Enterprise Manager Ops Center	Networking	HTTP	Yes	8.2	Network	Low	No
CVE-2016-1181	Enterprise Manager for Fusion Middleware	FMW Plugin for CC (Apache Struts 1)	HTTP	Yes	8.1	Network	High	No
CVE-2017-9798	Enterprise Manager Base Platform	Installer (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	No
CVE-2016-9878	Enterprise Manager Ops Center	Framework (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2017-9798	Enterprise Manager Ops Center	Networking (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-0739	Enterprise Manager Ops Center	Networking (OpenSSL)	HTTPS	Yes	6.5	Network	Low	No

Additional CVEs addressed are below:

- The fix for CVE-2016-1181 also addresses CVE-2014-0114 and CVE-2016-1182.

- The fix for CVE-2016-9878 also addresses CVE-2018-1270, CVE-2018-1271, CVE-2018-1272 and CVE-2018-1275.
- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.
- The fix for CVE-2018-1275 also addresses CVE-2016-9878, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.
- The fix for CVE-2018-7489 also addresses CVE-2017-7525.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 56 new security fixes for Oracle Financial Services Applications. 21 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 "Oracle Financial Services Analytical Applications Infrastructure" is a component that is used by a number of Oracle Financial Services Applications. Customers should refer to the MOS Note (Doc ID 2380553.1) to determine the dependent products and refer Oracle Financial Services Analytical Applications Infrastructure MOS document to determine how to patch this component.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2017-5645	Oracle Banking Platform	Collections (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1275	Oracle Financial Services Analytical Applications Infrastructure	Inline Processing Engine (Spring Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1275	Oracle Financial Services Behavior	Admin Tool (Spring Framework)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
	Detection Platform							
CVE-2017-5645	Oracle Financial Services Behavior Detection Platform	Ingestion (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Financial Services Funds Transfer Pricing	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Financial Services Hedge Management and IFRS Valuations	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Financial Services Loan Loss Forecasting and Provisioning	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Financial Services Profitability Management	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-3050	Oracle Banking Corporate Lending	Core module	HTTP	No	8.1	Network	Low	I
CVE-2018-3027	Oracle Banking Payments	Payments Core	HTTP	No	8.1	Network	Low	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2018-3051	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	No	8.1	Network	Low	L
CVE-2018-3035	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	8.1	Network	Low	L
CVE-2018-3015	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	8.1	Network	Low	L
CVE-2018-8013	Oracle Financial Services Analytical Applications Infrastructure	Link Analysis and Metadata browser (Apache Batik)	HTTP	Yes	7.3	Network	Low	N
CVE-2018-3040	Oracle Banking Corporate Lending	Core module	HTTP	No	6.5	Network	Low	L
CVE-2018-3022	Oracle Banking Payments	Payments Core	HTTP	No	6.5	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2014-3577	Oracle Financial Services Revenue Management and Billing	External Message (HTTP Client)	HTTP	Yes	6.5	Network	Low	N
CVE-2018-3041	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	No	6.5	Network	Low	L
CVE-2018-3030	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	6.5	Network	Low	L
CVE-2018-2979	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.5	Network	Low	L
CVE-2018-3036	Oracle Banking Corporate Lending	Core module	HTTP	No	6.3	Network	Low	L
CVE-2018-3020	Oracle Banking Payments	Payments Core	HTTP	No	6.3	Network	Low	L
CVE-2018-3037	Oracle FLEXCUBE Enterprise Limits and	Infrastructure	HTTP	No	6.3	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
	Collateral Management							
CVE-2018-3028	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	6.3	Network	Low	I
CVE-2018-2974	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.3	Network	Low	I
CVE-2018-2895	Oracle Banking Corporate Lending	Core module	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2896	Oracle Banking Payments	Payments Core	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2897	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2898	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2899	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2018-3042	Oracle Banking Corporate Lending	Core module	HTTP	No	5.4	Network	Low	I
CVE-2018-3044	Oracle Banking Corporate Lending	Core module	HTTP	No	5.4	Network	Low	I
CVE-2018-3048	Oracle Banking Corporate Lending	Core module	HTTP	No	5.4	Network	Low	I
CVE-2018-3023	Oracle Banking Payments	Payments Core	HTTP	No	5.4	Network	Low	I
CVE-2018-3024	Oracle Banking Payments	Payments Core	HTTP	No	5.4	Network	Low	I
CVE-2018-3026	Oracle Banking Payments	Payments Core	HTTP	No	5.4	Network	Low	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2018-3043	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	No	5.4	Network	Low	I
CVE-2018-3045	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	No	5.4	Network	Low	I
CVE-2018-3049	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	No	5.4	Network	Low	I
CVE-2018-3031	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.4	Network	Low	I
CVE-2018-3032	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.4	Network	Low	I
CVE-2018-3034	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.4	Network	Low	I
CVE-2018-2980	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.4	Network	Low	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2018-2981	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.4	Network	Low	L
CVE-2018-3019	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.4	Network	Low	L
CVE-2018-3038	Oracle Banking Corporate Lending	Core module	HTTP	Yes	5.3	Network	Low	N
CVE-2018-3046	Oracle Banking Corporate Lending	Core module	HTTP	No	5.3	Network	High	L
CVE-2018-3021	Oracle Banking Payments	Payments Core	HTTP	Yes	5.3	Network	Low	N
CVE-2018-3025	Oracle Banking Payments	Payments Core	HTTP	No	5.3	Network	High	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2018-3039	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	Yes	5.3	Network	Low	N
CVE-2018-3047	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure	HTTP	No	5.3	Network	High	L
CVE-2018-3029	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	Yes	5.3	Network	Low	N
CVE-2018-3033	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.3	Network	High	L
CVE-2018-2975	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	Yes	5.3	Network	Low	N
CVE-2018-2982	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.3	Network	High	L

Notes:

1. Please refer MOS document (Doc ID 2380553.1) for applicability across other Oracle Financial Services products.

Additional CVEs addressed are below:

- The fix for CVE-2014-3577 also addresses CVE-2015-5262.
- The fix for CVE-2018-1275 also addresses CVE-2018-1258, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 44 new security fixes for Oracle Fusion Middleware. 38 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 July 2018 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 July 2018 Patch Availability Document for Oracle Products, My Oracle Support Note 2394520.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2017-5645	Oracle Enterprise Data Quality	General (Apache Log4j)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2018-1275	Oracle Enterprise Repository	Security Subsystem (Spring Framework)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2017-5645	Oracle Fusion Middleware MapViewer	Install (Apache Log4j)	HTTP	Yes	9.8	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-7489	Oracle WebCenter Portal	Security Framework (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-7489	Oracle WebLogic Server	Console (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-1275	Oracle WebLogic Server	Sample apps (Spring Framework)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-2894	Oracle WebLogic Server	WLS - Web Services	HTTP	Yes	9.8	Network	Low	No
CVE-2018-2893	Oracle WebLogic Server	WLS Core Components	T3	Yes	9.8	Network	Low	No
CVE-2018-3100	Oracle Business Process Management Suite	Process Analysis & Discovery	HTTP	Yes	9.1	Network	Low	No
CVE-2018-3007	Oracle Tuxedo	Core	Jolt	Yes	8.6	Network	Low	No
CVE-2018-2935	Oracle WebLogic Server	JSF	HTTP	Yes	8.3	Network	Low	No
CVE-2018-2958	BI Publisher	BI Publisher Security	HTTP	Yes	8.2	Network	Low	No
CVE-2018-2900	BI Publisher	Layout Tools	HTTP	Yes	8.2	Network	Low	No
CVE-2017-12617	FMW Platform	Common Components (Apache Tomcat)	HTTP	Yes	8.1	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2015-7940	Oracle JDeveloper	None (Bouncy Castle Java package)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-8013	Oracle Fusion Middleware MapViewer	Install (Apache Batik)	HTTP	Yes	7.3	Network	Low	No
CVE-2018-2943	Oracle Fusion Middleware MapViewer	Map Builder	HTTP	No	7.2	Network	Low	Hi
CVE-2018-3102	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-2992	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3009	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3010	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3092	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3103	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3093	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3094	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3095	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-3096	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3097	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3104	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3098	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-3099	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	No
CVE-2018-2925	BI Publisher	Web Server	HTTP	No	6.5	Network	Low	Lo
CVE-2018-0739	Oracle API Gateway	Oracle API Gateway (OpenSSL)	HTTPS	Yes	6.5	Network	Low	No
CVE-2018-3109	Oracle Fusion Middleware MapViewer	Map Builder	HTTP	No	6.5	Network	Low	Lo
CVE-2018-0739	Oracle Tuxedo	SSL/TLS (OpenSSL)	HTTPS	Yes	6.5	Network	Low	No
CVE-2016-9843	Oracle Outside In Technology	Outside In Search Export SDK (zlib)	HTTP	Yes	6.3	Network	Low	No
CVE-2018-2987	Oracle WebLogic Server	Console	HTTP	Yes	6.1	Network	Low	No
CVE-2015-0204	Oracle Internet Directory	SSL/TLS	HTTPS	Yes	5.9	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2998	Oracle WebLogic Server	SAML	HTTP	No	5.4	Network	Low	L
CVE-2011-4461	Oracle Endeca Information Discovery Studio	Studio (Jetty)	HTTP	Yes	5.3	Network	Low	N
CVE-2018-3108	Oracle Fusion Middleware	Oracle Notification Service	HTTPS	No	5.3	Network	High	L
CVE-2018-3101	Oracle WebCenter Portal	Portlet Services	HTTP	Yes	5.3	Network	Low	N
CVE-2018-2933	Oracle WebLogic Server	WLS Core Components	HTTP	No	4.9	Network	High	L
CVE-2018-3105	Oracle SOA Suite	Health Care FastPath	HTTP	No	4.3	Network	Low	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.

2. Please refer to MOS document (Doc ID 2420947.1) for instructions on how to address this issue.

3. Please refer to MOS document (Doc ID 2421480.1) for instructions on how to address this issue.

Additional CVEs addressed are below:

- The fix for CVE-2016-9843 also addresses CVE-2014-8157, CVE-2014-9029, CVE-2014-9746, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2016-0718, CVE-2016-5300, CVE-2016-9841 and CVE-2017-10989.

- The fix for CVE-2018-0739 also addresses CVE-2017-3735, CVE-2017-3736, CVE-2017-3738 and CVE-2018-0733.
- The fix for CVE-2018-1275 also addresses CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.
- The fix for CVE-2018-7489 also addresses CVE-2017-7525.

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 24 new security fixes for Oracle Hospitality Applications. 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 Complexity	
CVE-2018-2984	Oracle Hospitality Cruise Fleet Management System	Gangway Activity Web App	HTTP	No	8.1	Network	Low	
CVE-2016-1181	Oracle Hospitality Gift and Loyalty	Report (Struts 1)	HTTP	Yes	8.1	Network	High	I
CVE-2016-1181	Oracle Hospitality Gift and Loyalty	iCard.net (Struts 1)	HTTP	Yes	8.1	Network	High	I
CVE-2018-2956	Oracle Hospitality OPERA 5 Property Services	Integration	None	No	8.1	Local	High	I
CVE-2016-1181	Oracle Hospitality Reporting and Analytics	Configuration (Struts 1)	HTTP	Yes	8.1	Network	High	I
CVE-2016-1181	Oracle Hospitality Reporting and Analytics	Report (Struts 1)	HTTP	Yes	8.1	Network	High	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complexity	
CVE-2016-1181	Oracle Hospitality Reporting and Analytics	Report (Struts 1)	HTTP	Yes	8.1	Network	High	
CVE-2018-2957	Oracle Hospitality OPERA 5 Property Services	Logging	HTTP	Yes	7.5	Network	Low	
CVE-2018-3002	Oracle Hospitality Cruise Fleet Management System	Fleet Management System Suite	None	No	7.1	Local	Low	
CVE-2018-3000	Oracle Hospitality Cruise Shipboard Property Management System	SPMS Suite	None	No	7.1	Local	Low	
CVE-2018-2978	Oracle Hospitality Simphony	Import/Export	HTTP	No	7.1	Network	High	
CVE-2018-3013	Oracle Hospitality OPERA 5 Property Services	Report Server Config	HTTP	No	6.5	Network	Low	
CVE-2018-3014	Oracle Hospitality OPERA 5 Property Services	Reports	HTTP	No	6.5	Network	Low	
CVE-2017-0785	MICROS Handheld Terminal	MC40 Zebra Handheld unit (WiFi)	None	No	6.2	Local	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complexity	
CVE-2018-3003	Oracle Hospitality Cruise Fleet Management System	Fleet Management System Suite	None	No	6.2	Local	Low	
CVE-2018-3001	Oracle Hospitality Cruise Shipboard Property Management System	SPMS Suite	None	No	6.2	Local	Low	
CVE-2017-5715	MICROS 700 Series Tablet	MICROS Tablet 720 (BIOS)	None	No	5.6	Local	High	
CVE-2017-5715	MICROS 700 Series Tablet	MICROS Tablet 721 (BIOS)	None	No	5.6	Local	High	
CVE-2017-5715	MICROS Kitchen Display Controller	Kitchen Display System 210 (BIOS)	None	No	5.6	Local	High	
CVE-2017-5715	MICROS Workstation 6	Workstation 610 (BIOS 32 Bit)	None	No	5.6	Local	High	
CVE-2017-5715	MICROS Workstation 6	Workstation 610 (BIOS 64 Bit)	None	No	5.6	Local	High	
CVE-2017-5715	MICROS Workstation 6	Workstation 620 (BIOS)	None	No	5.6	Local	High	
CVE-2017-5715	MICROS Workstation 6	Workstation 650 (BIOS)	None	No	5.6	Local	High	
CVE-2018-2955	Oracle Hospitality OPERA 5	Integration	HTTP	Yes	5.3	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complexity	
	Property Services							

Additional CVEs addressed are below:

- The fix for CVE-2016-1181 also addresses CVE-2014-0114, CVE-2015-6420 and CVE-2016-1182.
- The fix for CVE-2017-0785 also addresses CVE-2017-13088 and CVE-2017-13218.

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle Hyperion. Both 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 Complexity	
CVE-2018-2907	Hyperion Financial Reporting	Security Models	HTTP	Yes	8.6	Network	Low	No
CVE-2018-2915	Hyperion Data Relationship Management	Access and security	HTTPS	Yes	5.8	Network	Low	No

Oracle iLearning Risk Matrix

This Critical Patch Update contains 1 new security fix 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 3.0 R			
					Base Score	Attack Vector	Attack Complexity	
CVE-2018-2989	Oracle iLearning	Learner Administration	HTTP	Yes	8.2	Network	Low	Non

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle Insurance Applications. Both 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 Complexity
CVE-2017-5645	Oracle Insurance Policy Administration	Policy Administration (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2018-1275	Oracle Insurance Policy Administration	Policy Administration (Spring Framework)	HTTP	Yes	9.8	Network	Low

Oracle Java SE Risk Matrix

This Critical Patch Update contains 8 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.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complexity	Priv Req'
CVE-2018-2938	Java SE	Java DB	Multiple	Yes	9.0	Network	High	Non
CVE-2018-2964	Java SE	Deployment	Multiple	Yes	8.3	Network	High	Non
CVE-2018-2941	Java SE	JavaFX	Multiple	Yes	8.3	Network	High	Non
CVE-2018-2942	Java SE	Windows DLL	Multiple	Yes	8.3	Network	High	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complexity	Privs Req'
CVE-2018-2972	Java SE	Security	Multiple	Yes	5.9	Network	High	Non
CVE-2018-2973	Java SE, Java SE Embedded	JSSE	SSL/TLS	Yes	5.9	Network	High	Non
CVE-2018-2940	Java SE, Java SE Embedded	Libraries	Multiple	Yes	4.3	Network	Low	Non
CVE-2018-2952	Java SE, Java SE Embedded, JRockit	Concurrency	Multiple	Yes	3.7	Network	High	Non

Notes:

1. 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. CVE-2018-2938 addresses CVE-2018-1313.

2. 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).

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 Products Risk Matrix

This Critical Patch Update contains 10 new security fixes for Oracle JD Edwards Products. 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 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2944	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics	HTTP	Yes	7.5	Network	Low	N
CVE-2018-2947	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	No	6.5	Network	Low	L
CVE-2018-2945	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2946	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2948	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2949	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2950	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2999	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N
CVE-2018-3006	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2017-3736	JD Edwards World Security	GUI / World Vision (OpenSSL)	HTTP	Yes	5.9	Network	High	N

Additional CVEs addressed are below:

- The fix for CVE-2017-3736 also addresses CVE-2017-3735.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 31 new security fixes for Oracle MySQL. 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 VERSIC		
					Base Score	Attack Vector	Attack Complexi
CVE-2017-5645	MySQL Enterprise Monitor	Service Manager (Apache Log4j)	Log4j	Yes	9.8	Network	Low
CVE-2017-0379	MySQL Workbench	Workbench: Security: Encryption (libgcrypt)	MySQL Protocol	Yes	7.5	Network	Low
CVE-2018-3064	MySQL Server	InnoDB	MySQL Protocol	No	7.1	Network	Low
CVE-2018-0739	MySQL Connectors	Connector/ODBC (OpenSSL)	HTTPS	Yes	6.5	Network	Low
CVE-2018-0739	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	HTTPS	Yes	6.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complexi
CVE-2018-3070	MySQL Server	Client mysqldump	MySQL Protocol	No	6.5	Network	Low
CVE-2018-3060	MySQL Server	InnoDB	MySQL Protocol	No	6.5	Network	Low
CVE-2018-3065	MySQL Server	Server: DML	MySQL Protocol	No	6.5	Network	Low
CVE-2018-0739	MySQL Server	Server: Installing (OpenSSL)	MySQL Protocol	Yes	6.5	Network	Low
CVE-2018-3073	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low
CVE-2018-0739	MySQL Workbench	Workbench: Security: Encryption (OpenSSL)	MySQL Protocol	Yes	6.5	Network	Low
CVE-2018-3074	MySQL Server	Server: Security: Roles	MySQL Protocol	No	5.3	Network	High
CVE-2018-3062	MySQL Server	Server: Memcached	memcached	No	5.3	Network	High
CVE-2018-3081	MySQL Client	Client programs	MySQL Protocol	No	5.0	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complexi
CVE-2018-3071	MySQL Server	Audit Log	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3079	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3054	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3077	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3078	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3080	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3061	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3067	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3063	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3075	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low
CVE-2018-3058	MySQL Server	MyISAM	MySQL Protocol	No	4.3	Network	Low
CVE-2018-3056	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.3	Network	Low
CVE-2018-2598	MySQL Workbench	Workbench: Security: Encryption	MySQL Protocol	Yes	3.7	Network	High
CVE-2018-3066	MySQL Server	Server: Options	MySQL Protocol	No	3.3	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complexi
CVE-2018-2767	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	3.1	Network	High
CVE-2018-3084	MySQL Server	Shell: Core / Client	None	No	2.8	Local	Low
CVE-2018-3082	MySQL Server	Server: DDL	MySQL Protocol	No	2.7	Network	Low

Additional CVEs addressed are below:

- The fix for CVE-2017-0379 also addresses CVE-2017-9526.
- The fix for CVE-2018-0739 also addresses CVE-2017-3737 and CVE-2017-3738.

Oracle PeopleSoft Products Risk Matrix

This Critical Patch Update contains 15 new security fixes for Oracle PeopleSoft Products. 11 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 Complexity	Pr Re
CVE-2017-5645	PeopleSoft Enterprise FIN Install	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1275	PeopleSoft Enterprise FIN Install	Security (Spring Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-2990	PeopleSoft Enterprise PeopleTools	Integration Broker	HTTP	Yes	7.4	Network	High	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2977	PeopleSoft Enterprise PeopleTools	Integration Broker	HTTP	Yes	6.5	Network	Low	N
CVE-2018-0739	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTP	Yes	6.5	Network	Low	N
CVE-2018-2951	PeopleSoft Enterprise PeopleTools	Configuration Manager	None	No	6.2	Local	Low	N
CVE-2018-3068	PeopleSoft Enterprise HCM Human Resources	Compensation	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2929	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2919	PeopleSoft Enterprise PeopleTools	Unified Navigation	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2985	PeopleSoft Enterprise PeopleTools	Workflow	HTTP	Yes	6.1	Network	Low	N
CVE-2018-2986	PeopleSoft Enterprise PeopleTools	Workflow	HTTP	Yes	6.1	Network	Low	N
CVE-2018-3016	PeopleSoft Enterprise PeopleTools	Integration Broker	HTTP	No	5.4	Network	Low	L
CVE-2018-3072	PeopleSoft HRMS	Candidate Gateway	HTTP	Yes	5.3	Network	Low	N
CVE-2018-2970	PeopleSoft Enterprise PeopleTools	PIA Search Functionality	HTTP	No	4.3	Network	Low	L
CVE-2018-3076	PeopleSoft Enterprise CS Financial Aid	ISIR Processing	HTTP	No	2.7	Network	Low	H

Additional CVEs addressed are below:

- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.
- The fix for CVE-2018-1275 also addresses CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.

Oracle Policy Automation Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	P R
CVE-2017-5645	Oracle Policy Automation	Determinations Engine (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Policy Automation Connector for Siebel	Core (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle Policy Automation for Mobile Devices	Core (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	P R

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 31 new security fixes for Oracle Retail 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 Complexity
CVE-2017-5533	MICROS Lucas	Security (JasperReports)	HTTP	Yes	9.8	Network	Low
CVE-2017-5533	MICROS Relate CRM Software	Internal Operations (JasperReports)	HTTP	Yes	9.8	Network	Low
CVE-2018-1275	Oracle Retail Back Office	Security (Spring Framework)	HTTP	Yes	9.8	Network	Low
CVE-2018-1275	Oracle Retail Central Office	Security (Spring Framework)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Retail Clearance Optimization Engine	General Application (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Retail Integration Bus	RIB Kernal (Apache Log4j)	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complexity
CVE-2017-5533	Oracle Retail Order Broker	Order Broker Foundation (JasperReports)	HTTP	Yes	9.8	Network	Low
CVE-2018-1275	Oracle Retail Point-of-Service	Infrastructure (Spring Framework)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2018-1275	Oracle Retail Returns Management	Security (Spring Framework)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Retail Service Backbone	Install (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Retail Service Layer	Installation (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-6814	Oracle Retail Integration Bus	RIB Kernal (Apache Groovy)	HTTP	Yes	9.6	Network	Low
CVE-2016-6814	Oracle Retail Service Backbone	Install (Apache Groovy)	HTTP	Yes	9.6	Network	Low
CVE-2016-1181	MICROS XBR	Retail (Apache Struts 1)	HTTP	Yes	8.1	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complexity
CVE-2017-12617	Oracle Retail Convenience and Fuel POS Software	OPT Server (Apache Tomcat)	HTTP	Yes	8.1	Network	High
CVE-2016-3506	Oracle Retail Convenience and Fuel POS Software	Point of Sale	HTTP	Yes	8.1	Network	High
CVE-2018-2882	MICROS Retail-J	Interfaces	HTTP	No	7.7	Network	Low
CVE-2016-9878	Oracle Retail Back Office	Security (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2016-9878	Oracle Retail Central Office	Security	HTTP	Yes	7.5	Network	Low
CVE-2017-5664	Oracle Retail Convenience and Fuel POS Software	OPT Server (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2015-7940	Oracle Retail Convenience and Fuel POS Software	OPT Server (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low
CVE-2016-9878	Oracle Retail Integration Bus	Install (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2016-9878	Oracle Retail Point-of-Sale	Transaction (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2016-9878	Oracle Retail Returns Management	Security (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2018-2888	MICROS Retail-J	Back Office	none	No	6.7	Physical	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complexity
CVE-2018-3052	MICROS Relate CRM Software	Internal Operations	HTTP	No	6.4	Network	Low
CVE-2018-3053	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations	HTTP	No	6.4	Network	Low
CVE-2018-2881	MICROS Retail-J	Database	HTTP	No	6.3	Network	Low
CVE-2018-2891	Oracle Retail Bulk Data Integration	BDI Job Scheduler	HTTP	Yes	6.1	Network	Low

Additional CVEs addressed are below:

- The fix for CVE-2016-1181 also addresses CVE-2014-0114 and CVE-2016-1182.
- The fix for CVE-2017-5533 also addresses CVE-2017-5529.
- The fix for CVE-2017-5664 also addresses CVE-2016-8735.
- The fix for CVE-2018-1275 also addresses CVE-2016-9878, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Siebel CRM. 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 RIS			
					Base Score	Attack Vector	Attack Complexity	Privs Req'd
CVE-2018-2959	Siebel UI Framework	UIF Open UI	HTTP	Yes	4.3	Network	Low	None

Oracle Sun Systems Products Suite Risk Matrix

This Critical Patch Update contains 22 new security fixes for the Oracle Sun Systems Products Suite. 10 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 Complexity	Pr Re
CVE-2018-2930	Solaris Cluster	NAS device addition	RPC	Yes	9.8	Network	Low	No
CVE-2015-7501	Tape Library ACSLS	Software (Apache Commons Collections)	Multiple	No	8.8	Network	Low	Lo
CVE-2018-3057	Sun ZFS Storage Appliance Kit (AK)	API frameworks	None	No	8.2	Local	Low	Hi
CVE-2018-2928	Solaris	RAD	Multiple	Yes	8.1	Network	Low	No
CVE-2018-2892	Solaris	Availability Suite Service	None	No	7.8	Local	Low	Lo
CVE-2018-2908	Solaris	Kernel	RPC	No	7.7	Network	Low	Lo
CVE-2018-2926	Solaris	NVIDIA-GFX Kernel driver	ISCSI	No	7.6	Network	Low	Lo
CVE-2018-2918	Sun ZFS Storage Appliance Kit (AK)	API frameworks	Multiple	Yes	7.5	Network	High	No
CVE-2018-2920	Sun ZFS Storage Appliance Kit (AK)	API frameworks	Multiple	No	7.4	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-2932	Oracle SuperCluster Specific Software	SuperCluster Virtual Assistant	Multiple	Yes	7.1	Network	High	No
CVE-2018-1171	Solaris	Kernel	None	No	7.0	Local	High	Lo
CVE-2018-2921	Sun ZFS Storage Appliance Kit (AK)	User Interface	HTTP	Yes	5.8	Network	Low	No
CVE-2018-2924	Sun ZFS Storage Appliance Kit (AK)	API frameworks	None	No	5.7	Local	Low	Hi
CVE-2018-2937	Sun ZFS Storage Appliance Kit (AK)	User Interface	HTTP	Yes	5.3	Network	Low	No
CVE-2018-2917	Sun ZFS Storage Appliance Kit (AK)	API frameworks	Multiple	Yes	5.3	Network	Low	No
CVE-2018-2905	Sun ZFS Storage Appliance Kit (AK)	Core Services	SSL/TLS	Yes	5.3	Network	Low	No
CVE-2018-2903	Solaris	Kernel	None	No	4.4	Local	Low	Hi
CVE-2018-2927	Sun ZFS Storage Appliance Kit (AK)	HTTP data path subsystems	HTTP	No	4.3	Network	Low	Lo
CVE-2018-2906	Hardware Management Pack	Ipmitool	IPMI	Yes	3.7	Network	High	No
CVE-2018-2901	Solaris	Kernel	DHCP	Yes	3.7	Network	High	No
CVE-2018-2916	Sun ZFS Storage	API frameworks	Multiple	No	2.7	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
	Appliance Kit (AK)							
CVE-2018-2923	Sun ZFS Storage Appliance Kit (AK)	Core Services	None	No	2.3	Local	Low	Hi

Oracle Supply Chain Products Suite Risk Matrix

This Critical Patch Update contains 8 new security fixes for the Oracle Supply Chain Products Suite. 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		
					Base Score	Attack Vector	Attack Complexity
CVE-2017-5645	Oracle AutoVue VueLink Integration	Installation Issues (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-6814	Oracle Agile PLM	Event Java PX (Apache Groovy)	HTTP	Yes	9.6	Network	Low
CVE-2016-1181	Agile Recipe Management for Pharmaceuticals	UI Components-Framework (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2016-1181	Oracle Transportation Management	Install (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2017-5662	Oracle Agile PLM MCAD Connector	CAX Client (Apache Batik)	HTTP	No	7.3	Network	Low
CVE-2018-0739	Oracle Agile Engineering Data Management	Install (OpenSSL)	HTTP	Yes	6.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complexity
CVE-2018-0739	Oracle Transportation Management	Install (OpenSSL)	HTTP	Yes	6.5	Network	Low
CVE-2018-3069	Oracle Agile Product Lifecycle Management for Process	Installation	HTTP	No	2.7	Network	Low

Additional CVEs addressed are below:

- The fix for CVE-2016-1181 also addresses CVE-2014-0114 and CVE-2016-1182.
- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.

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 R			
					Base Score	Attack Vector	Attack Complexity	Priv Req
CVE-2018-1000300	OSS Support Tools	Services Tools Bundle (curl)	HTTP	Yes	7.5	Network	High	Non

Additional CVEs addressed are below:

- The fix for CVE-2018-1000300 also addresses CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122 and CVE-2018-1000301.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 4 new security fixes for Oracle Utilities Applications. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 I			
					Base Score	Attack Vector	Attack Complexity	Pri Rec
CVE-2017-5645	Oracle Utilities Network Management System	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2017-5645	Oracle Utilities Work and Asset Management	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2016-5019	Oracle Utilities Framework	Help (Apache Trinidad)	HTTP	Yes	7.5	Network	Low	No
CVE-2017-5662	Oracle Utilities Network Management System	Install (Apache Batik)	HTTP	No	7.3	Network	Low	Lo

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 12 new security fixes for Oracle Virtualization. 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			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-3086	Oracle VM VirtualBox	Core	None	No	8.6	Local	Low	N
CVE-2018-3087	Oracle VM VirtualBox	Core	None	No	8.6	Local	Low	N
CVE-2018-3088	Oracle VM VirtualBox	Core	None	No	8.6	Local	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complexity	Pr Re
CVE-2018-3089	Oracle VM VirtualBox	Core	None	No	8.6	Local	Low	N
CVE-2018-3090	Oracle VM VirtualBox	Core	None	No	8.6	Local	Low	N
CVE-2018-3085	Oracle VM VirtualBox	Core	None	No	8.5	Local	Low	N
CVE-2018-1000300	Oracle Secure Global Desktop	Core (curl)	Multiple	Yes	7.5	Network	High	N
CVE-2018-3055	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	N
CVE-2018-1305	Oracle Secure Global Desktop	Application Server (Apache Tomcat)	HTTP	No	6.5	Network	Low	L
CVE-2018-0739	Oracle Secure Global Desktop	Core (OpenSSL)	TLS	Yes	6.5	Network	Low	N
CVE-2018-3091	Oracle VM VirtualBox	Core	None	No	6.3	Local	Low	N
CVE-2018-3005	Oracle VM VirtualBox	Core	None	No	4.0	Local	Low	N

Additional CVEs addressed are below:

- The fix for CVE-2018-1000300 also addresses CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122 and CVE-2018-1000301.
- The fix for CVE-2018-1305 also addresses CVE-2018-1304.