Oracle Critical Patch Update Advisory - July 2019

Oracle Critical Patch Update Advisory - July 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 319 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 2019 Critical Patch Update: Executive Summary and Analysis.

Please note that since the release of the April 2019 Critical Patch Update, Oracle has released two Security Alerts for Oracle WebLogic Server: CVE-2019-2725 (April 29, 2019) and CVE-2019-2729 (June 18, 2019). WebLogic Server customers are strongly advised to apply the fixes contained in this Critical Patch Update, which provides the fixes for the previously-released Alerts as well as additional fixes.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Application Express, versions 5.1, 18.2	Database
Diagnostic Assistant, versions prior to 2.12.36	Support Tools
Enterprise Manager Base Platform, versions 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0	Enterprise Manager
Enterprise Manager for Fusion Middleware, versions 13.2, 13.3	Enterprise Manager
Enterprise Manager for Virtualization, versions 13.1, 13.2, 13.3	Enterprise Manager
Enterprise Manager Ops Center, versions 12.3.3, 12.4.0	Enterprise Manager
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 Security, versions A9.3, A9.3.1, A9.4	JD Edwards
MICROS Retail XBRi Loss Prevention, versions 10.8.0 - 10.8.3	Retail Applications
MICROS Retail-J, versions 12.1.0, 12.1.1, 12.1.2, 13.1	Retail Applications
MySQL Enterprise Monitor, versions 4.0.9 and prior, 8.0.14 and prior	MySQL
MySQL Server, versions 5.6.44 and prior, 5.7.26 and prior, 8.0.16 and prior	MySQL
MySQL Workbench, versions 8.0.16 and prior	MySQL
Oracle Agile Engineering Data Management, versions 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 Application Testing Suite, versions 13.1, 13.2, 13.3	Enterprise Manager
Oracle Banking Platform, versions 2.4.0 - 2.7.1	Oracle Banking Platform
Oracle Berkeley DB, versions 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23, 12.1.6.2.32	Berkeley DB
Oracle BI Publisher, version 11.1.1.9.0	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 11.1.1.9.0, 12.2.1.4.0	Fusion Middleware
Oracle Clusterware, version 12.1.0.2.0	Support Tools

Affected Products and Versions	Patch Availability Document
Oracle Communications Application Session Controller, versions 3.7.1, 3.8.0	Oracle Communications Application Session Controller
Oracle Communications Billing and Revenue Management, versions 7.5, 12.0	Oracle Communications Billing and Revenue Management
Oracle Communications Converged Application Server, versions 5.1, 7.0, 7.1	Oracle Communications Converged Application Server
Oracle Communications Converged Application Server - Service Controller, versions 6.0, 6.1	Oracle Communications Converged Application Server - Service Controller
Oracle Communications Convergence, version 3.0.2	Oracle Communications Convergence
Oracle Communications Diameter Signaling Router (DSR), versions 8.0, 8.1, 8.2, 8.3	Oracle Communications Diameter Signaling Router
Oracle Communications EAGLE (Software), versions 46.5, 46.6, 46.7	Oracle Communications EAGLE (Software)
Oracle Communications Instant Messaging Server, version 10.0.1.2.0	Oracle Communications Instant Messaging Server
Oracle Communications Interactive Session Recorder, versions 6.0, 6.1, 6.2	Oracle Communications Interactive Session Recorder
Oracle Communications Messaging Server, versions 8.0.2, 8.1.0	Oracle Communications Messaging Server
Oracle Communications Online Mediation Controller, version 6.1	Oracle Communications Online Mediation Controller
Oracle Communications Unified, version 8.0.0.2.0	Oracle Communications Calendar Ser
Oracle Data Integrator, version 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 Demantra Demand Management, version 7.3.1.5.2	Oracle Supply Chain Products
Oracle E-Business Suite, versions 12.1.1 - 12.1.3, 12.2.3 - 12.2.8	E-Business Suite
Oracle Endeca Information Discovery Integrator, version 3.2.0	Fusion Middleware
Oracle Endeca Server, version 7.7.0	Fusion Middleware
Oracle Enterprise Manager Base Platform, versions 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0	Enterprise Manager
Oracle Enterprise Repository, version 12.1.3.0.0	Fusion Middleware
Oracle Financial Services - Regulatory Reporting for Reserve Bank of India - Lombard Risk Integration Pack, version 8.0.7	Oracle Financial Services - Regulatory Reporting for Reserve Bank of India
Oracle Financial Services - Regulatory Reporting for US Federal Reserve - Lombard Risk Integration Pack, versions 8.0.4 - 8.0.7	Oracle Financial Services Regulatory Reporting for US Federal Reserve

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3 - 7.3.5, 8.0.2 - 8.0.8	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Analytical Applications Reconciliation Framework, versions 8.0.4 - 8.0.7	Oracle Financial Services Analytical Applications Reconciliation Framewor
Oracle Financial Services Asset Liability Management, versions 8.0.4 - 8.0.7	Oracle Financial Services Asset Liabili Management
Oracle Financial Services Basel Regulatory Capital Basic, versions 8.0.4 - 8.0.7	Oracle Financial Services Basel Regulatory Capital Basic
Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, versions 8.0.4 - 8.0.7	Oracle Financial Services Basel Regulatory Capital Internal Ratings Ba Approach
Oracle Financial Services Data Foundation, versions 8.0.4 - 8.0.8	Oracle Financial Services Data Foundation
Oracle Financial Services Data Integration Hub, versions 8.0.5 - 8.0.7	Oracle Financial Services Data Integra Hub
Oracle Financial Services Funds Transfer Pricing, versions 8.0.4 - 8.0.7	Oracle Financial Services Funds Trans 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 Institutional Performance Analytics, versions 8.0.4 - 8.0.7	Oracle Financial Services Institutional Performance Analytics
Oracle Financial Services Liquidity Risk Management, versions 8.0.1, 8.0.2, 8.0.4, 8.0.5, 8.0.6	Oracle Financial Services Liquidity Ris Management
Oracle Financial Services Liquidity Risk Measurement and Management, versions 8.0.7, 8.0.8	Oracle Financial Services Liquidity Ris Measurement and 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, 8.0.8	Oracle Financial Services Market Risk Measurement and Management
Oracle Financial Services Price Creation and Discovery, versions 8.0.4 - 8.0.7	Oracle Financial Services Price Creatic And Discovery
Oracle Financial Services Profitability Management, versions 8.0.4 - 8.0.7	Oracle Financial Services Profitability Management
Oracle Financial Services Regulatory Reporting for European Banking Authority, versions 8.0.6, 8.0.7	Oracle Financial Services Regulatory Reporting for European Banking Authority
Oracle Financial Services Regulatory Reporting for European Banking Authority - Integration Pack for Lombard Risk, versions 8.0.6, 8.0.7	Oracle Financial Services Regulatory Reporting for European Banking Authority

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Regulatory Reporting for US Federal Reserve, versions 8.0.4 - 8.0.7	Oracle Financial Services Regulatory Reporting for US Federal Reserve
Oracle Financial Services Retail Customer Analytics, versions 8.0.4 - 8.0.6	Oracle Financial Services Retail Custo Analytics
Oracle Financial Services Revenue Management and Billing, versions 2.4.0.0, 2.4.0.1	Oracle Financial Services Revenue Management and Billing
Oracle FLEXCUBE Core Banking, versions 5.2.0, 11.6.0, 11.7.0, 11.8.0	Oracle Financial Services Applications
Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 12.0, 12.1	Oracle Financial Services Applications
Oracle FLEXCUBE Investor Servicing, versions 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0	Oracle Financial Services Applications
Oracle FLEXCUBE Private Banking, versions 12.0.1, 12.0.3, 12.1.0	Oracle Financial Services Applications
Oracle FLEXCUBE Universal Banking, versions 12.0.1 - 12.0.3, 12.1.0 - 12.4.0, 14.0.0 - 14.2.0	Oracle Financial Services Applications
Oracle Global Lifecycle Management OPatchAuto, versions prior to 12.2.0.1.14	Oracle Global Lifecycle Management OPatchAuto
Oracle GraalVM Enterprise Edition, version 19.0.0	Oracle GraalVM Enterprise Edition
Oracle Hospitality Gift and Loyalty, versions 9.0.0, 9.1.0	Oracle Hospitality Gift and Loyalty
Oracle Hospitality Guest Access, versions 4.2, 4.2.1	Oracle Hospitality Guest Access
Oracle Hospitality Simphony, version 18.2.1	Oracle Hospitality Simphony
Oracle Hospitality Suite8, versions 8.9.6, 8.10.2, 8.11 - 8.14	Oracle Hospitality Suite8
Oracle HTTP Server, versions 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Hyperion Planning, version 11.1.2.4	Fusion Middleware
Oracle Hyperion Workspace, version 11.1.2.4	Fusion Middleware
Oracle Identity Manager, versions 11.1.2.3.0, 12.2.1.3.0	Fusion Middleware
Oracle Insurance Allocation Manager for Enterprise Profitability, version 8.0.8	Oracle Insurance Allocation Manager Enterprise Profitability
Oracle Insurance Calculation Engine, versions 9.7, 10.0, 10.1, 10.2	Oracle Insurance Applications
Oracle Insurance Data Foundation, versions 8.0.4 - 8.0.7	Oracle Insurance Data Foundation
Oracle Insurance IFRS 17 Analyzer, versions 8.0.6, 8.0.7	Oracle Insurance IFRS 17 Analyzer
Oracle Insurance Performance Insight, version 8.0.7	Oracle Insurance Performance Insight
Oracle Insurance Policy Administration J2EE, versions 10.0, 10.1, 10.2, 11.0	Oracle Insurance Applications

Affected Products and Versions	Patch Availability Document
Oracle Insurance Rules Palette, versions 10.0, 10.1, 10.2, 11.0	Oracle Insurance Applications
Oracle Java SE, versions 7u221, 8u212, 11.0.3, 12.0.1	Java SE
Oracle Java SE Embedded, version 8u211	Java SE
Oracle Outside In Technology, version 8.5.4	Fusion Middleware
Oracle Retail Advanced Inventory Planning, version 15.0	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0	Retail Applications
Oracle Retail Financial Integration, versions 14.0, 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Integration Bus, versions 15.0, 16.0	Retail Applications
Oracle Retail Order Broker, versions 5.2, 15.0	Retail Applications
Oracle Retail Order Management System, version 5.0	Retail Applications
Oracle Retail Predictive Application Server, versions 14.0.3.26, 14.1.3.37, 15.0.3.100, 16.0	Retail Applications
Oracle Retail Service Backbone, version 16.0.1	Retail Applications
Oracle Retail Xstore Office, versions 7.0, 7.1	Retail Applications
Oracle Retail Xstore Point of Service, versions 7.0, 7.1, 15.0, 16.0, 17.0, 18.0	Retail Applications
Oracle Security Service, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle SOA Suite, version 12.2.1.3.0	Fusion Middleware
Oracle Solaris, versions 10, 11.3, 11.4	Systems
Oracle Transportation Management, version 6.3.7	Oracle Supply Chain Products
Oracle Utilities Advanced Spatial and Operational Analytics, version 2.7.0.1	Oracle Utilities Applications
Oracle Utilities Framework, versions 4.3.0.2.0 - 4.3.0.6.0, 4.4.0.0.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 5.2.32, prior to 6.0.10	Virtualization
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
PeopleSoft Enterprise FIN Project Costing, 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

Affected Products and Versions	Patch Availability Document
Primavera Analytics, version 18.8	Oracle Construction and Engineering Suite
Primavera Gateway, versions 15.2, 16.2, 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
Services Tools Bundle, version 19.2	Support Tools
Siebel Applications, versions 19.0 and prior	Siebel
StorageTek Tape Analytics SW Tool, version 2.3.0	Systems
Sun ZFS Storage Appliance Kit (AK), version 8.8.3	Systems
System Utilities, version 19.1	Support Tools
Tape Virtual Storage Manager GUI, version 6.2	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 and Alerts. An English text version of the risk matrices provided in this document is here.

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. Each vulnerability is identified by a CVE# which is 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:

- Abid Gul Shahid: CVE-2019-2809
- Alexander Kornbrust of Red Database Security: CVE-2019-2776
- Andrej Simko of Accenture: CVE-2019-2666, CVE-2019-2672, CVE-2019-2837
- Andrej Simko of Accenture working with iDefense Labs: CVE-2019-2668, CVE-2019-2672
- Andrzej Dyjak: CVE-2019-2756, CVE-2019-2759, CVE-2019-2764, CVE-2019-2792, CVE-2019-2835, CVE-2019-2852, CVE-2019-2853, CVE-2019-2854, CVE-2019-2855
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2019-2865
- Anthony Laou Hine Tsuei working with Trend Micro Zero Day Initiative: CVE-2019-2859
- Cornelius Aschermann of Ruhr-University Bochum: CVE-2019-2873, CVE-2019-2874, CVE-2019-2875, CVE-2019-2876, CVE-2019-2877
- Devin Rosenbauer of Identity Works LLC: CVE-2019-2858
- Ephem: CVE-2019-2848
- Fabio Pires of NCC Group: CVE-2019-2735
- Gaston Traberg of Onapsis: CVE-2019-2773, CVE-2019-2775, CVE-2019-2782, CVE-2019-2783, CVE-2019-2829
- Giuseppino Cadeddu of Quantum Leap: CVE-2019-2770
- Hanno Böck: CVE-2019-2760
- huyna of Viettel Cyber Security working with Trend Micro Zero Day Initiative: CVE-2019-2866, CVE-2019-2867

- Jason Matthyser of MWR Labs working with Trend Micro Zero Day Initiative: CVE-2019-2863
- Jayson Grace of Sandia National Laboratories: CVE-2019-2484
- Jonathan Birch of Microsoft Corp.: CVE-2019-2816
- Kamlapati Choubey of Trend Micro working with Trend Micro's Zero Day Initiative: CVE-2019-2827
- Keegan Ryan of NCC Group: CVE-2019-2745
- Lionel Debroux: CVE-2019-2760, CVE-2019-2868, CVE-2019-2869, CVE-2019-2870, CVE-2019-2871
- lofiboy of VinCSS (Vingroup) working with Trend Micro Zero Day Initiative: CVE-2019-2864
- Luca Moro of Synacktiv: CVE-2019-5597, CVE-2019-5598
- Lucas Dinucci: CVE-2019-2861
- Lukasz Mikula: CVE-2019-2599
- Manuel Rigger of Eth Zurich: CVE-2019-2879
- Martin Doyhenard of Onapsis: CVE-2019-2828
- Mathew Nash of NCC Group: CVE-2019-2735
- Matthias Kaiser of Apple Information Security: CVE-2019-2856
- Minle Chen of PingAn Galaxy Lab: CVE-2019-2824
- Mirza Burhan Baig of Dig8Labs: CVE-2019-2823
- Nati Nimni of Microsoft Corp.: CVE-2019-2842
- Or Hanuka of Motorola Solutions: CVE-2019-2732, CVE-2019-2733
- rgod of 9sg Security Team working with Trend Micro's Zero Day Initiative: CVE-2019-2799
- Sarath Nair: CVE-2019-2857
- Sergej Schumilo of Ruhr-University Bochum: CVE-2019-2873, CVE-2019-2874, CVE-2019-2875, CVE-2019-2876, CVE-2019-2877
- Simon Wörner of Ruhr-University Bochum: CVE-2019-2873, CVE-2019-2874, CVE-2019-2875, CVE-2019-2876, CVE-2019-2877
- Steven Seeley of Source Incite working with iDefense: CVE-2019-2727
- Tzachy Horesh of Motorola Solutions: CVE-2019-2732, CVE-2019-2733
- Ubais PK: CVE-2019-2850
- Vahagn Vardanyan: CVE-2019-2767, CVE-2019-2768, CVE-2019-2771
- Vladimir Egorov: CVE-2019-2767, CVE-2019-2768, CVE-2019-2771

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.:

- Abbas Mamoun
- Andres Georgieff of Sandia National Laboratories
- Brian Healy of Sandia National Laboratories
- Dasari Narendra
- George R
- Harold Fang
- Juraj Somorovsky of Ruhr-University Bochum
- Marcin Wołoszyn of ING Services Polska
- Mateusz Jurczyk of Google Project Zero (4 reports)
- Narendra Singh
- Nimrod Aviram
- Peter Dettman of cryptoworkshop.com (2 reports)
- Raju Mogulapalli of Rheem
- Robert Merget of Ruhr-University Bochum
- Tilman Hausherr
- William Bonnaventure of University of Luxembourg (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:

- 162187647

- Bartlomiej Bergier
- Bibek Shah
- Jan Kopriva of Alef Nula (2 reports)
- Jonathan Leitschuh
- Markus Wulftange of Code White GmbH
- Naveen Kumar
- Patrick Samuel
- Suhas Nayak
- Wai Yan Aung

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:

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

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - July 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
2020-October-12	Rev 6. Updated affected versions for CVE-2019-2767

Date	Note
2019-August-16	Rev 5. Added note for CVE-2018-11058
2019-July-19	Rev 4. Updated component for CVE-2018-12022 and CVE-2018-1000873
2019-July-17	Rev 3. Updated Security-In-Depth Contributors Section.
2019-July-17	Rev 2. Updated affected versions for CVE-2019-2856.
2019-July-16	Rev 1. Initial Release.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 9 new security fixes for the Oracle Database Server divided as follows:

- 8 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. 3 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 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			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2018-11058	Core RDBMS	None	TCPS/HTTPS	Yes	9.8	Network	Low	Nor
CVE-2019-2776	Core RDBMS	Create Any Index	OracleNet	No	7.6	Network	Low	Hig
CVE-2019-2799	Oracle ODBC Driver	None	Multiple	No	7.5	Network	High	Lov
CVE-2019-2749	Java VM	Create Session, Create Procedure	Multiple	No	6.8	Network	High	Lov
CVE-2019-2484	Application Express	Valid Account	HTTP	No	5.4	Network	Low	Lov

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-2753	Oracle Text	Create Session	OracleNet	No	4.6	Network	Low	Lov
CVE-2019-2569	Core RDBMS	Local Logon	Local Logon	No	4.0	Local	High	Hig
CVE-2016-9572	Spatial	Create Session	OracleNet	No	3.5	Network	Low	Lov

Notes:

1. Client Score for CVE-2018-11058 is 8.1 with Attack Complexity as High.

2. The vulnerability affects Windows platforms only.

Additional CVEs addressed are below:

- The update for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.

Oracle Database Server Client-Only Installations

The following Oracle Database Server vulnerabilities included in this Critical Patch Update affect client-only installations: CVE-2018-11058, CVE-2019-2799 and CVE-2019-2569.

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Global Lifecycle Management. This vulnerability is not remotely exploitable without authentication, i.e., may not be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2018-7489	Oracle Global Lifecycle Management OPatchAuto	OPatch Auto Binary (jackson-databind)	Local Logon	No	7.2	Local	High	High	

Additional CVEs addressed are below:

- The update for CVE-2018-7489 also addresses CVE-2017-15095 and CVE-2017-7525.

Oracle Berkeley DB Risk Matrix

This Critical Patch Update contains 5 new security fixes for Oracle Berkeley DB. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Inte
CVE-2019-2760	Data Store	Local Logon	Local Logon	No	7.0	Local	High	None	Req
CVE-2019-2868	Data Store	Local Logon	Local Logon	No	7.0	Local	High	None	Req
CVE-2019-2869	Data Store	Local Logon	Local Logon	No	7.0	Local	High	None	Req
CVE-2019-2870	Data Store	Local Logon	Local Logon	No	7.0	Local	High	None	Req
CVE-2019-2871	Data Store	Local Logon	Local Logon	No	7.0	Local	High	None	Req

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 24 new security fixes for Oracle Communications 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.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2016-1000031	Oracle Communications Application Session Controller	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2019-2729	Oracle Communications Converged Application Server	Security (Oracle WebLogic Server)	HTTP	Yes	9.8	Network	Low
CVE-2018-1275	Oracle Communications Converged Application Server - Service Controller	Security (Spring Framework)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications Convergence	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Communications Interactive Session Recorder	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications Online Mediation Controller	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications Unified	Security (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-2018-19362	Oracle Communications Unified	Security (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2018-18311	Oracle Communications Billing and Revenue Management	Billing and Revenue Management Server (Perl)	HTTP	Yes	8.1	Network	High
CVE-2018-8039	Oracle Communications Diameter Signaling Router (DSR)	Security (Apache cxf)	HTTP	Yes	8.1	Network	High
CVE-2018-12023	Oracle Communications Instant Messaging Server	Security (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2018-1000120	Oracle Communications Application Session Controller	Security (cURL)	HTTP	Yes	7.5	Network	High
CVE-2019-12086	Oracle Communications Billing and Revenue Management	Billing Care, Business Operations Center (jackson-databind)	HTTP	Yes	7.5	Network	Low
CVE-2018-1000180	Oracle Communications Convergence	Security (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low
CVE-2018-0732	Oracle Communications Diameter Signaling Router (DSR)	Signaling (OpenSSL)	TLS	Yes	7.5	Network	Low
CVE-2017-5664	Oracle Communications Interactive	Security (Apache Tomcat)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Session Recorder						
CVE-2018-15756	Oracle Communications Online Mediation Controller	Security (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2018-8013	Oracle Communications Application Session Controller	Security (Apache Batik)	HTTP	Yes	7.3	Network	Low
CVE-2017-3736	Oracle Communications EAGLE (Software)	Security (OpenSSL)	TLS	No	6.5	Network	Low
CVE-2018-1305	Oracle Communications Instant Messaging Server	Security (Apache Tomcat)	HTTP	No	6.5	Network	Low
CVE-2018-17197	Oracle Communications Messaging Server	Security (Apache Tika)	HTTP	Yes	6.5	Network	Low
CVE-2015-9251	Oracle Communications Application Session Controller	Security (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-11358	Oracle Communications Billing and Revenue Management	Billing Care, Business Operations Center (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2017-5715	Oracle Communications Diameter Signaling Router (DSR)	Security (Kernel)	None	No	5.6	Local	High

Additional CVEs addressed are below:

- The update for CVE-2017-3736 also addresses CVE-2017-3735, CVE-2017-3737, CVE-2017-3738, CVE-2018-0732, CVE-2018-0734, CVE-2018-0737, CVE-2018-0739 and CVE-2018-5407.
- The update for CVE-2017-5664 also addresses CVE-2016-8735 and CVE-2017-5647.
- The update for CVE-2018-0732 also addresses CVE-2017-3738, CVE-2018-0733, CVE-2018-0734, CVE-2018-0737 and CVE-2018-0739.
- The update for CVE-2018-1000120 also addresses CVE-2018-1000121, CVE-2018-1000122 and CVE-2018-1000301.
- The update for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The update for CVE-2018-12023 also addresses CVE-2018-11307 and CVE-2018-12022.
- The update for CVE-2018-1275 also addresses CVE-2018-1258, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.
- The update for CVE-2018-1305 also addresses CVE-2018-1304.
- The update for CVE-2018-15756 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257, CVE-2018-1258, CVE-2018-1270, CVE-2018-1271, CVE-2018-1272 and CVE-2018-1275.
- The update for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.
- The update for CVE-2019-12086 also addresses CVE-2018-19360, CVE-2018-19361 and CVE-2018-19362.
- The update for CVE-2019-2729 also addresses CVE-2019-2725.

Oracle Construction and Engineering Suite Risk Matrix

This Critical Patch Update contains 8 new security fixes for the Oracle Construction and Engineering 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 3.(			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2018-19362	Primavera Gateway	Admin (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-0192	Primavera Unifier	Core (solr)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-0190	Instantis EnterpriseTrack	Core (Apache	HTTP	Yes	7.5	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
		HTTP Server)						
CVE-2019-0199	Instantis EnterpriseTrack	Core (Tomcat)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-15756	Primavera Analytics	Admin (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-15756	Primavera Gateway	Admin (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-17197	Primavera Unifier	Core (Apache Tika)	HTTP	Yes	6.5	Network	Low	No
CVE-2015-9251	Primavera Unifier	Core (jQuery)	HTTP	Yes	6.1	Network	Low	No

Additional CVEs addressed are below:

- The update for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.
- The update for CVE-2019-0190 also addresses CVE-2018-17189 and CVE-2018-17199.
- The update for CVE-2019-0192 also addresses CVE-2017-3164.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 13 new security fixes for the Oracle E-Business Suite. 12 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

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 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 (July 2019), My Oracle Support Note 2555452.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2828	Oracle Field Service	Wireless	HTTP	Yes	9.6	Network	Low	None
CVE-2019-2775	Oracle Payments	File Transmission	HTTP	Yes	9.1	Network	Low	None
CVE-2019-2782	Oracle Payments	File Transmission	HTTP	Yes	8.6	Network	Low	None
CVE-2019-2837	Oracle CRM Technical Foundation	User Interface	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2829	Oracle iSupport	Service Requests	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2666	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2668	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2672	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2825	Oracle Applications Manager	Oracle Diagnostics Interfaces	HTTP	No	6.5	Network	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2773	Oracle Payments	File Transmission	HTTP	Yes	5.8	Network	Low	None
CVE-2019-2783	Oracle Payments	File Transmission	HTTP	Yes	5.8	Network	Low	None
CVE-2019-2809	Oracle iRecruitment	Password Reset	HTTP	Yes	5.3	Network	Low	None
CVE-2019-2761	Oracle Application Object Library	Attachments / File Upload	HTTP	Yes	3.7	Network	High	None

Oracle Enterprise Manager Products Suite Risk Matrix

This Critical Patch Update contains 12 new security fixes for the Oracle Enterprise Manager Products Suite. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these 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 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 July 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2534806.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2018-19362	Enterprise Manager for Virtualization	Plug-In Lifecycle (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-3822	Enterprise Manager Ops Center	Networking (cURL)	HTTP	Yes	9.8	Network	Low	No
CVE-2016-1000031	Oracle Application Testing Suite	Load Testing for Web Apps (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-8039	Enterprise Manager Base Platform	Connector Framework (Apache CXF)	HTTP	Yes	8.1	Network	High	No
CVE-2019-0211	Enterprise Manager Ops Center	Compliance Test Suite (Apache HTTP Server)	none	No	7.8	Local	Low	L
CVE-2018-1000180	Enterprise Manager for Fusion Middleware	Application Replay (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-0222	Oracle Enterprise Manager Base Platform	Valid Session (Apache ActiveMQ)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-2727	Oracle Application Testing Suite	Load Testing for Web Apps	HTTP	Yes	7.3	Network	Low	No
CVE-2018-11775	Oracle Enterprise Manager Base Platform	Reporting Framework (Apache ActiveMQ)	HTTP	Yes	6.8	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-1559	Enterprise Manager Base Platform	Discovery Framework (OpenSSL)	HTTPS	Yes	5.9	Network	High	N
CVE-2019-1559	Enterprise Manager Ops Center	Networking (OpenSSL)	HTTPS	Yes	5.9	Network	High	N
CVE-2019-2728	Enterprise Manager Ops Center	Networking	HTTP	No	4.3	Network	Low	L

Additional CVEs addressed are below:

- The update for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The update for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.
- The update for CVE-2018-8039 also addresses CVE-2018-1258.
- The update for CVE-2019-0211 also addresses CVE-2019-0196, CVE-2019-0197, CVE-2019-0215, CVE-2019-0217 and CVE-2019-0220.
- The update for CVE-2019-0222 also addresses CVE-2018-11775.
- The update for CVE-2019-3822 also addresses CVE-2018-16890 and CVE-2019-3823.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 60 new security fixes for Oracle Financial Services Applications. 50 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-2018-19362	Oracle Banking Platform	Infrastructure (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Financial Services	Infrastructure (Jackson-databind)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Analytical Applications Infrastructure							
CVE-2018-19362	Oracle Financial Services Funds Transfer Pricing	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Financial Services Institutional Performance Analytics	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Financial Services Price Creation and Discovery	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Financial Services Profitability Management	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Financial Services Retail Customer Analytics	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle FLEXCUBE Core Banking	Securities (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2016-1000031	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Insurance Allocation Manager for Enterprise Profitability	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2018-19362	Oracle Insurance Performance Insight	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2019-2841	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	8.1	Network	Low	
CVE-2018-8039	Oracle FLEXCUBE Private Banking	Core (cxf)	HTTP	Yes	8.1	Network	High	
CVE-2019-2754	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	8.1	Network	Low	
CVE-2018-15756	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Spring Framework)	HTTP	Yes	7.5	Network	Low	
CVE-2018-15756	Oracle FLEXCUBE	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Private Banking							
CVE-2014-0114	Oracle Insurance IFRS 17 Analyzer	UI (Beanutils)	HTTP	Yes	7.3	Network	Low	
CVE-2018-17197	Oracle FLEXCUBE Private Banking	Core (Apache Tika)	HTTP	Yes	6.5	Network	Low	
CVE-2019-11358	Oracle Banking Platform	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services - Regulatory Reporting for Reserve Bank of India - Lombard Risk Integration Pack	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services - Regulatory Reporting for US Federal Reserve - Lombard Risk Integration Pack	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services	UI (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Analytical Applications Reconciliation Framework							
CVE-2019-11358	Oracle Financial Services Asset Liability Management	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Basel Regulatory Capital Basic	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Data Foundation	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Data Integration Hub	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Funds Transfer Pricing	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial	UI (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Services Hedge Management and IFRS Valuations							
CVE-2019-11358	Oracle Financial Services Institutional Performance Analytics	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Liquidity Risk Management	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Liquidity Risk Measurement and Management	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Loan Loss Forecasting and Provisioning	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Market Risk Measurement and Management	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Price Creation and Discovery	UI (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-11358	Oracle Financial Services Profitability Management	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Regulatory Reporting for European Banking Authority	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Regulatory Reporting for European Banking Authority - Integration Pack for Lombard Risk	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Regulatory Reporting for US Federal Reserve	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Financial Services Retail Customer Analytics	UI (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-11358	Oracle Financial Services Revenue Management and Billing	Core (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2017-14735	Oracle FLEXCUBE Core Banking	Security (AntiSamy)	HTTP	Yes	6.1	Network	Low	
CVE-2019-2736	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	Yes	6.1	Network	Low	
CVE-2019-2744	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Insurance Allocation Manager for Enterprise Profitability	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Insurance Data Foundation	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Insurance IFRS 17 Analyzer	UI (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-11358	Oracle Insurance	UI (jQuery)	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Performance Insight							
CVE-2019-2847	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.7	Network	Low	
CVE-2019-2840	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.7	Network	Low	
CVE-2019-2823	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	No	5.4	Network	Low	
CVE-2019-2843	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.4	Network	Low	
CVE-2019-2790	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.4	Network	Low	
CVE-2019-2846	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	Yes	5.3	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-2794	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	Yes	5.3	Network	Low	
CVE-2019-2839	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.3	Network	High	
CVE-2019-2845	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	3.5	Network	Low	
CVE-2019-2793	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	3.5	Network	Low	

Additional CVEs addressed are below:

- The update for CVE-2018-19362 also addresses CVE-2018-19360, CVE-2018-19361 and CVE-2019-12086.

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle Food and Beverage Applications. 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#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2763	Oracle Hospitality Gift and Loyalty	iCard	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2833	Oracle Hospitality Simphony	Import/Export	HTTP	No	7.7	Network	Low	Low
CVE-2019-2836	Oracle Hospitality Simphony	Engagement	HTTP	Yes	7.5	Network	Low	None

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 33 new security fixes for Oracle Fusion Middleware. 28 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.

Please note that the recently-released Security Alert patches for WebLogic Server, CVE-2019-2725 and CVE-2019-2729, are included in this Critical Patch Update. Customers are strongly advised to apply this Critical Patch Update on all WebLogic Server systems.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2018-11058	Oracle Security Service	SSL API (RSA BSAFE)	Multiple	Yes	9.8	Network	Low	No
CVE-2017-5645	Oracle SOA Suite	Installation & Templates (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2016-1000031	Oracle WebCenter Sites	Advanced UI (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-2856	Oracle WebLogic Server	Application Container - JavaEE	T3	Yes	9.8	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2016-6814	Oracle WebCenter Sites	Advanced UI (Apache Groovy)	HTTP	Yes	9.6	Network	Low	No
CVE-2019-2771	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	No	8.2	Network	Low	Lo
CVE-2019-0211	Oracle HTTP Server	Web Listener (Apache httpd)	None	No	7.8	Local	Low	Lo
CVE-2019-2768	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	Yes	7.5	Network	Low	No
CVE-2018-1000180	Oracle Data Integrator	Runtime Java agent for ODI (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-15756	Oracle Endeca Information Discovery Integrator	Other Issues (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-0222	Oracle Enterprise Repository	Security Subsystem - 12c (Apache ActiveMQ)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-15756	Oracle WebCenter Sites	Advanced UI (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-15756	Oracle WebLogic Server	Sample apps (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-2852	Oracle Outside In	Outside In Filters	HTTP	Yes	7.3	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
	Technology							
CVE-2019-2853	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2756	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2759	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2854	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2764	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2792	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2835	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2855	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No
CVE-2018-8013	Oracle WebCenter Sites	Third Party Tools (Apache Batik)	HTTP	Yes	7.3	Network	Low	No
CVE-2019-2767	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	Yes	7.2	Network	Low	No
CVE-2019-2742	Oracle BI Publisher	Web Service API	HTTP	Yes	7.2	Network	Low	No
CVE-2015-9251	Oracle Business Intelligence	BI Platform Security (jQuery)	HTTP	Yes	6.1	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
	Enterprise Edition							
CVE-2016-7103	Oracle WebLogic Server	Console (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2018-0734	Oracle Endeca Server	Product Code (OpenSSL)	HTTPS	Yes	5.9	Network	High	No
CVE-2019-1559	Oracle Endeca Server	Product Code (OpenSSL)	HTTPS	Yes	5.9	Network	High	No
CVE-2019-2751	Oracle HTTP Server	OHS Config MBeans	HTTPS	Yes	5.9	Network	High	No
CVE-2019-2824	Oracle WebLogic Server	WLS Core Components	HTTP	No	5.5	Network	Low	Hig
CVE-2019-2827	Oracle WebLogic Server	WLS Core Components	HTTP	No	5.5	Network	Low	Hig
CVE-2019-2858	Oracle Identity Manager	Advanced Console	HTTP	No	4.3	Network	Low	Lo

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 update for CVE-2018-0734 also addresses CVE-2018-0735 and CVE-2018-5407.
- The update for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The update for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.
- The update for CVE-2019-2742 also addresses CVE-2016-3473.

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle Hospitality 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 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2781	Oracle Hospitality Suite8	XML Interface	TCP/IP	No	6.5	Network	Low	Low	
CVE-2019-11358	Oracle Hospitality Guest Access	Base (jQuery)	HTTP	Yes	6.1	Network	Low	None	F

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle Hyperion. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2770	Oracle Hyperion Planning	Smart View	HTTP	No	4.5	Network	Low	High	F
CVE-2019-2861	Oracle Hyperion Planning	Security	HTTP	No	4.2	Network	High	High	F
CVE-2019-2735	Oracle Hyperion Workspace	UI and Visualization	HTTP	No	2.4	Network	Low	High	F

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 7 new security fixes for Oracle Insurance Applications. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2016-1000031	Oracle Insurance Calculation Engine	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Insurance Policy Administration J2EE	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Insurance Rules Palette	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2018-15756	Oracle Insurance Calculation Engine	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	
CVE-2018-15756	Oracle Insurance Policy Administration J2EE	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	
CVE-2018-15756	Oracle Insurance Rules Palette	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	
CVE-2017-14735	Oracle Insurance Calculation Engine	Core (AntiSamy)	HTTP	Yes	6.1	Network	Low	

Additional CVEs addressed are below:

- The update for CVE-2018-15756 also addresses CVE-2016-5007 and CVE-2016-9878.

Oracle Java SE Risk Matrix

This Critical Patch Update contains 10 new security fixes for Oracle Java SE. 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.

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-2019-7317	Java SE, Java SE Embedded	AWT (libpng)	Multiple	Yes	6.8	Network	High	None	R
CVE-2019-2821	Java SE	JSSE	TLS	Yes	5.3	Network	High	None	R
CVE-2019-2762	Java SE, Java SE Embedded	Utilities	Multiple	Yes	5.3	Network	Low	None	
CVE-2019-2769	Java SE, Java SE Embedded	Utilities	Multiple	Yes	5.3	Network	Low	None	
CVE-2019-2745	Java SE	Security	None	No	5.1	Local	High	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-2019-2816	Java SE, Java SE Embedded	Networking	Multiple	Yes	4.8	Network	High	None	
CVE-2019-2842	Java SE	JCE	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2786	Java SE, Java SE Embedded	Security	Multiple	Yes	3.4	Network	High	None	R
CVE-2019-2818	Java SE	Security	Multiple	Yes	3.1	Network	High	None	R
CVE-2019-2766	Java SE, Java SE Embedded	Networking	Multiple	Yes	3.1	Network	High	None	R

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 does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

2. This vulnerability 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.

Additional CVEs addressed are below:

- The update for CVE-2019-7317 also addresses CVE-2019-6129.

Oracle GraalVM Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle GraalVM. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2019-2813	Oracle GraalVM Enterprise Edition	GraalVM	Multiple	No	7.7	Network	Low	Low	
CVE-2019-2862	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	6.8	Network	High	None	Re

Oracle JD Edwards Products Risk Matrix

This Critical Patch Update contains 5 new security fixes for Oracle JD Edwards Products. 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	Pri Re
CVE-2017-5645	JD Edwards EnterpriseOne Tools	Installation SEC (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2018-19362	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics (jackson-databind)	HTTP	Yes	9.8	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2018-19362	JD Edwards EnterpriseOne Tools	Web Runtime (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-1559	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure SEC (OpenSSL)	JDENET	Yes	5.9	Network	High	No
CVE-2019-1559	JD Edwards World Security	Security Vulnerability (OpenSSL)	HTTPS	Yes	5.9	Network	High	No

Additional CVEs addressed are below:

- The update for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.
- The update for CVE-2019-1559 also addresses CVE-2018-0734, CVE-2018-0735 and CVE-2018-5407.

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 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-3822	MySQL Server	Server: Packaging (cURL)	MySQL Protocol	Yes	9.8	Network	Low	Nor
CVE-2018-15756	MySQL Enterprise Monitor	Monitoring: General (Spring Framework)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-2822	MySQL Server	Shell: Admin / InnoDB Cluster	MySQL Protocol	Yes	7.5	Network	High	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-2800	MySQL Server	Server: Replication	MySQL Protocol	No	7.1	Network	Low	Lov
CVE-2019-2795	MySQL Server	Server: Charsets	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2019-2746	MySQL Server	Server: Data Dictionary	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2019-2812	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2019-2834	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2019-2805	MySQL Server	Server: Parser	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2019-2740	MySQL Server	Server: XML	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2019-1559	MySQL Workbench	MySQL Workbench (OpenSSL)	MySQL Workbench	Yes	5.9	Network	High	Nor
CVE-2019-2758	MySQL Server	InnoDB	MySQL Protocol	No	5.5	Network	Low	Hig
CVE-2019-2819	MySQL Server	Server: Security: Audit	MySQL Protocol	No	5.5	Network	Low	Hig
CVE-2019-2731	MySQL Server	Server: Replication	MySQL Protocol	No	5.4	Network	Low	Lov
CVE-2019-2778	MySQL Server	Server: Security:	MySQL Protocol	No	5.4	Network	Low	Lov

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
		Privileges						
CVE-2019-2741	MySQL Server	Server: Audit Log	MySQL Protocol	No	5.3	Network	High	Lov
CVE-2019-2743	MySQL Server	Server: Security: Roles	MySQL Protocol	No	5.3	Network	High	Lov
CVE-2019-2739	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	5.1	Local	Low	Hig
CVE-2019-2785	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2798	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2879	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2737	MySQL Server	Server : Pluggable Auth	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2780	MySQL Server	Server: Components / Services	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2784	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2801	MySQL Server	Server: FTS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2747	MySQL Server	Server: GIS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2757	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-2774	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2796	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2802	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2803	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2808	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2810	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2815	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2830	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2752	MySQL Server	Server: Options	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2755	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2811	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2826	MySQL Server	Server: Security: Roles	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2019-2797	MySQL Server	Client programs	MySQL Protocol	No	4.2	Adjacent Network	High	Hig
CVE-2019-2791	MySQL Server	Server: Audit Plug-in	MySQL Protocol	No	3.8	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-2738	MySQL Server	Server : Compiling	MySQL Protocol	No	3.1	Network	High	Lo
CVE-2019-2730	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	2.7	Network	Low	Hig
CVE-2019-2789	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	2.7	Network	Low	Hig
CVE-2019-2814	MySQL Server	InnoDB	MySQL Protocol	No	2.2	Network	High	Hig

Additional CVEs addressed are below:

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

Oracle PeopleSoft Products Risk Matrix

This Critical Patch Update contains 8 new security fixes for Oracle PeopleSoft Products. 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 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2015-0226	PeopleSoft Enterprise PeopleTools	Security (Apache WSS4J)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-2748	PeopleSoft Enterprise PT PeopleTools	Application Server	HTTP	No	7.1	Network	High	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2599	PeopleSoft Enterprise PT PeopleTools	Pagelet Wizard	HTTP	No	6.5	Network	Low	Low
CVE-2019-2831	PeopleSoft Enterprise FIN Project Costing	Projects	HTTP	No	6.4	Network	Low	Low
CVE-2019-2772	PeopleSoft Enterprise PeopleTools	Activity Guide	HTTP	Yes	6.1	Network	Low	None
CVE-2019-11358	PeopleSoft Enterprise PeopleTools	Mobile Application Platform (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2018-17960	PeopleSoft Enterprise PeopleTools	Rich Text Editor (CKEditor)	HTTP	Yes	6.1	Network	Low	None
CVE-2019-1559	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	5.9	Network	High	None

Additional CVEs addressed are below:

- The update for CVE-2015-0226 also addresses CVE-2015-0227.
- The update for CVE-2018-17960 also addresses CVE-2018-9861.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 21 new security fixes for Oracle Retail Applications. 14 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	MICROS Retail XBRi Loss Prevention	Retail (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Retail Integration Bus	RIB Kernal (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2018-19362	Oracle Retail Xstore Point of Service	Xenvironment (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2018-1258	Oracle Retail Predictive Application Server	RPAS Fusion Client (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2018-1258	Oracle Retail Predictive Application Server	RPAS Fusion Client (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2018-1258	Oracle Retail Service Backbone	Install (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2019-2750	MICROS Retail-J	Internal Operations	HTTP	Yes	8.6	Network	Low
CVE-2018-3315	Oracle Retail Customer Management and Segmentation Foundation	Customer	HTTP	No	8.2	Network	High
CVE-2019-2561	Oracle Retail Xstore Office	Internal Operations	HTTP	Yes	8.2	Network	Low
CVE-2018-19362	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2018-8039	Oracle Retail Order Broker	Order Broker Foundation	HTTP	Yes	8.1	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
		(Apache CXF)					
CVE-2019-0232	Oracle Retail Order Broker	Upgrade Install (Apache Tomcat)	HTTP	Yes	8.1	Network	High
CVE-2016-1181	Oracle Retail Order Management System	Upgrade Install (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2019-0211	Oracle Retail Xstore Point of Service	Xenvironment (Apache HTTP Server)	none	No	7.8	Local	Low
CVE-2018-3316	Oracle Retail Customer Management and Segmentation Foundation	Segment	HTTP	No	7.6	Network	Low
CVE-2018-3111	Oracle Retail Xstore Office	Internal Operations	HTTP	Yes	7.6	Network	Low
CVE-2018-15756	Oracle Retail Advanced Inventory Planning	Operations & Maintenance (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2019-0190	Oracle Retail Xstore Point of Service	Xstore Office (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low
CVE-2018-2883	Oracle Retail Xstore Office	Internal Operations	HTTP	No	5.5	Network	Low
CVE-2018-11784	MICROS Retail XBRi Loss Prevention	Retail (Apache Tomcat)	HTTP	Yes	4.3	Network	Low

Additional CVEs addressed are below:

- The update for CVE-2016-1181 also addresses CVE-2016-1182.
- The update for CVE-2018-11784 also addresses CVE-2018-8034.
- The update for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257 and CVE-2018-15756.
- The update for CVE-2018-15756 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257 and CVE-2018-1258.
- The update for CVE-2018-19362 also addresses CVE-2018-19360 and CVE-2018-19361.
- The update for CVE-2019-0190 also addresses CVE-2018-17189 and CVE-2018-17199.
- The update for CVE-2019-0211 also addresses CVE-2019-0196, CVE-2019-0197, CVE-2019-0215, CVE-2019-0217 and CVE-2019-0220.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle Siebel CRM. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2777	Siebel Core - Server Framework	Search	HTTP	Yes	6.1	Network	Low	None
CVE-2019-2857	Siebel UI Framework	UIF Open UI	HTTP	No	5.4	Network	Low	Low
CVE-2019-2779	Siebel Core - Common Components	Email	HTTP	No	4.2	Network	High	High

Oracle Sun Systems Products Suite Risk Matrix

This Critical Patch Update contains 14 new security fixes for the Oracle Sun Systems Products Suite. 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 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-2725	StorageTek Tape Analytics SW Tool	Application Server (WebLogic)	HTTP	Yes	9.8	Network	Low	None	
CVE-2019-2729	StorageTek Tape Analytics SW Tool	Application Server (WebLogic)	HTTP	Yes	9.8	Network	Low	None	
CVE-2019-2725	Tape Virtual Storage Manager GUI	Application Server (WebLogic)	HTTP	Yes	9.8	Network	Low	None	
CVE-2019-5597	Oracle Solaris	Kernel	IPv6	Yes	9.1	Network	Low	None	
CVE-2019-2832	Oracle Solaris	Common Desktop Environment	None	No	8.8	Local	Low	Low	
CVE-2019-2844	Oracle Solaris	LDAP Client Tools	None	No	8.8	Local	Low	Low	
CVE-2019-5598	Oracle Solaris	Kernel	ICMPv6	Yes	7.5	Network	Low	None	
CVE-2019-2838	Oracle Solaris	Kernel	NFS	Yes	7.5	Network	Low	None	
CVE-2019-2804	Oracle Solaris	Filesystem	None	No	7.3	Local	Low	Low	
CVE-2019-2820	Oracle Solaris	Gnuplot	None	No	7.3	Local	Low	Low	
CVE-2019-2788	Oracle Solaris	Open Fabrics Tools	None	No	6.3	Local	High	None	
CVE-2019-2878	Sun ZFS Storage Appliance Kit (AK)	HTTP data path subsystems	HTTP	Yes	6.1	Network	Low	None	
CVE-2019-2787	Oracle Solaris	Automount	NFS	Yes	4.2	Network	High	None	
CVE-2019-2807	Oracle Solaris	Zones	None	No	3.9	Local	Low	Low	

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 Complex	
CVE-2016-1000031	Oracle Agile Engineering Data Management	Installation Issues (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2019-2725	Oracle Agile PLM	Application Server (Oracle WebLogic Server)	HTTP	Yes	9.8	Network	Low	
CVE-2019-0232	Oracle Transportation Management	Install (Apache Tomcat)	HTTP	Yes	8.1	Network	High	
CVE-2018-15756	Oracle Agile PLM	Security (Spring Framework)	HTTP	Yes	7.5	Network	Low	
CVE-2019-2817	Oracle Agile PLM	Folders, Files & Attachments	HTTP	No	5.4	Network	High	
CVE-2019-2732	Oracle Demantra Demand Management	Product Security	HTTP	Yes	5.3	Network	Low	
CVE-2018-11784	Oracle Agile Engineering Data Management	Installation Issues (Apache Tomcat)	HTTP	Yes	4.3	Network	Low	
CVE-2019-2733	Oracle Demantra Demand Management	Product Security	HTTP	No	4.3	Network	Low	

Additional CVEs addressed are below:

- The update for CVE-2018-11784 also addresses CVE-2018-8034.
- The update for CVE-2019-0232 also addresses CVE-2018-11784 and CVE-2018-8034.

Oracle Support Tools Risk Matrix

This Critical Patch Update contains 7 new security fixes for Oracle Support Tools. 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-2019-3822	Services Tools Bundle	Utilities (cURL)	Multiple	Yes	9.8	Network	Low	Nor
CVE-2018-12022	Oracle Clusterware	Trace File Analyzer (TFA) Collector (jackson-databind)	Multiple	Yes	7.5	Network	High	Nor
CVE-2018-1000873	Oracle Clusterware	Trace File Analyzer (TFA) Collector (jackson-databind)	Multiple	Yes	6.5	Network	Low	Nor
CVE-2015-9251	Diagnostic Assistant	Libraries (Jsch and jQuery)	Multiple	Yes	6.1	Network	Low	Nor
CVE-2019-11358	System Utilities	One Command Installation Tool (jQuery)	Multiple	Yes	6.1	Network	Low	Nor
CVE-2019-1559	Services Tools Bundle	Utilities (OpenSSL)	HTTPS	Yes	5.9	Network	High	Nor
CVE-2019-2860	Oracle Clusterware	Trace File Analyzer (TFA) Collector	Multiple	Yes	5.6	Network	High	Nor

Additional CVEs addressed are below:

- The update for CVE-2018-1000873 also addresses CVE-2018-12022, CVE-2018-12023, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361 and CVE-2019-12814.
- The update for CVE-2018-12022 also addresses CVE-2018-12023 and CVE-2019-12086.
- The update for CVE-2019-11358 also addresses CVE-2015-9251.
- The update for CVE-2019-3822 also addresses CVE-2018-16890 and CVE-2019-3823.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle Utilities 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 3.0 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2017-5645	Oracle Utilities Advanced Spatial and Operational Analytics	Install (Apache Log4j)	HTTP	Yes	9.8	Network	Low	None
CVE-2016-6814	Oracle Utilities Framework	Scripting (Groovy)	HTTP	Yes	9.8	Network	Low	None
CVE-2018-12023	Oracle Utilities Advanced Spatial and Operational Analytics	Install (jackson-databind)	HTTP	Yes	8.1	Network	High	None

Additional CVEs addressed are below:

- The update for CVE-2016-6814 also addresses CVE-2016-6497.
- The update for CVE-2018-12023 also addresses CVE-2017-7525, CVE-2018-11307, CVE-2018-12022 and CVE-2018-7489.

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 14 new security fixes for Oracle Virtualization. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2859	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2867	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2019-2866	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2019-2864	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2019-2865	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2019-1543	Oracle VM VirtualBox	Core (OpenSSL)	TLS	Yes	7.4	Network	High	None	
CVE-2019-2863	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2848	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2877	Oracle VM VirtualBox	Core	None	No	5.5	Local	Low	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2873	Oracle VM VirtualBox	Core	None	No	3.3	Local	Low	Low	
CVE-2019-2874	Oracle VM VirtualBox	Core	None	No	3.3	Local	Low	Low	
CVE-2019-2875	Oracle VM VirtualBox	Core	None	No	3.3	Local	Low	Low	
CVE-2019-2876	Oracle VM VirtualBox	Core	None	No	3.3	Local	Low	Low	
CVE-2019-2850	Oracle VM VirtualBox	Core	None	No	2.8	Local	Low	Low	R

Notes:

1. The vulnerability affects Windows platforms only.