Oracle Critical Patch Update Advisory - January 2019

Oracle Critical Patch Update Advisory - January 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 284 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 January 2019 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below. The product area is shown in the Patch Availability Document column. Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

Affected Products and Versions	Patch Availability Document
Enterprise Manager Base Platform, versions 12.1.0.5, 13.2, 13.3	Enterprise Manager

Affected Products and Versions	Patch Availability Document
Enterprise Manager for Virtualization, versions 13.2.2, 13.2.3, 13.3.1	Enterprise Manager
Enterprise Manager Ops Center, versions 12.2.2, 12.3.3	Enterprise Manager
Hyperion BI+, version 11.1.2.4	Fusion Middleware
Java Advanced Management Console, version 2.12	Java SE
JD Edwards EnterpriseOne Tools, version 9.2	JD Edwards
JD Edwards World Security, versions A9.3, A9.3.1, A9.4	JD Edwards
MySQL Connectors, versions 2.1.8 and prior, 8.0.13 and prior	MySQL
MySQL Enterprise Monitor, versions 4.0.7 and prior, 8.0.13 and prior	MySQL
MySQL Server, versions 5.6.42 and prior, 5.7.24 and prior, 8.0.13 and prior	MySQL
MySQL Workbench, versions 8.0.13 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 Product Lifecycle Management for Process, versions 6.2.0.0, 6.2.1.0, 6.2.2.0, 6.2.3.0, 6.2.3.1	Oracle Supply Chain Products
Oracle API Gateway, version 11.1.2.4.0	Fusion Middleware
Oracle Application Testing Suite, versions 12.5.0.3, 13.1.0.1, 13.2.0.1, 13.3.0.1	Enterprise Manager
Oracle Argus Safety, versions 8.1, 8.2	Health Sciences
Oracle Banking Platform, versions 2.5.0, 2.6.0, 2.6.1, 2.6.2	Oracle Banking Platform
Oracle Business Process Management Suite, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Communications Billing and Revenue Management, versions 7.5, 12.0	Oracle Communications Billing and Revenue Management
Oracle Communications Converged Application Server, versions prior to 7.0.0.1	Oracle Communications Converged Application Server
Oracle Communications Converged Application Server - Service Controller, version 6.1	Oracle Communications Converged Application Server - Service Controlle
Oracle Communications Diameter Signaling Router (DSR), versions prior to 8.3	Oracle Communications Diameter Signaling Router
Oracle Communications Online Mediation Controller, version 6.1	Oracle Communications Online Mediation Controller

Affected Products and Versions	Patch Availability Document
Oracle Communications Performance Intelligence Center (PIC) Software, versions prior to 10.2.1	Oracle Communications Performance Intelligence Center (PIC) Software
Oracle Communications Policy Management, versions prior to 12.5	Oracle Communications Policy Management
Oracle Communications Service Broker, version 6.0	Oracle Communications Service Brok
Oracle Communications Services Gatekeeper, versions prior to 6.1.0.4.0	Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller, versions SCz7.4.0, SCz7.4.1, SCz8.0.0, SCz8.1.0	Oracle Communications Session Bord Controller
Oracle Communications Unified Inventory Management, versions prior to 7.4.0	Oracle Communications Unified Inventory Management
Oracle Communications Unified Session Manager, version SCz7.3.5	Oracle Communications Unified Sess Manager
Oracle Communications WebRTC Session Controller, versions prior to 7.2	Oracle Communications WebRTC Session Controller
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c	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, 12.2.8	E-Business Suite
Oracle Endeca Server, version 7.7.0	Fusion Middleware
Oracle Enterprise Communications Broker, versions PCz2.1, PCz2.2, PCz3.0	Oracle Enterprise Communications Broker
Oracle Enterprise Repository, version 12.1.3.0.0	Fusion Middleware
Oracle Enterprise Session Border Controller, versions ECz7.4.0, ECz7.5.0, ECz8.0.0, ECz8.1.0	Oracle Enterprise Session Border Controller
Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3, 7.3.5, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.0.6, 8.0.7	Oracle Financial Services Analytical Applications Infrastructure
Oracle FLEXCUBE Direct Banking, version 12.0.2	Oracle Financial Services Applications
Oracle FLEXCUBE Investor Servicing, versions 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0	Oracle Financial Services Applications
Oracle Fusion Middleware MapViewer, version 12.2.1.3.0	Fusion Middleware
Oracle GoldenGate Application Adapters, version 12.3.2.1.1	Fusion Middleware
Oracle Health Sciences Information Manager, version 3.0	Health Sciences
Oracle Healthcare Foundation, versions 7.1, 7.2	Health Sciences
Oracle Healthcare Master Person Index, versions 3.0, 4.0	Health Sciences
Oracle Hospitality Cruise Fleet Management, version 9.0.10	Oracle Hospitality Cruise Fleet Management

Affected Products and Versions	Patch Availability Document
Oracle Hospitality Cruise Shipboard Property Management System, version 8.0.8	Oracle Hospitality Cruise Shipboard Property Management System
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle Hospitality Simphony, version 2.10	Oracle Hospitality Simphony
Oracle HTTP Server, version 12.2.1.3	Fusion Middleware
Oracle Insurance Calculation Engine, version 10.2	Oracle Insurance Applications
Oracle Insurance Insbridge Rating and Underwriting, versions 5.2, 5.4, 5.5	Oracle Insurance Applications
Oracle Insurance Policy Administration J2EE, versions 10.0, 10.2	Oracle Insurance Applications
Oracle Insurance Rules Palette, versions 10.0, 10.2	Oracle Insurance Applications
Oracle Java SE, versions 7u201, 8u192, 11.0.1	Java SE
Oracle Java SE Embedded, version 8u191	Java SE
Oracle Managed File Transfer, versions 12.2.1.3.0, 19.1.0.0.0	Fusion Middleware
Oracle Outside In Technology, versions 8.5.3, 8.5.4	Fusion Middleware
Oracle Reports Developer, version 12.2.1.3	Fusion Middleware
Oracle Retail Back Office, versions 13.3, 13.4, 14.0, 14.1	Retail Applications
Oracle Retail Central Office, versions 13.3, 13.4, 14.0, 14.1	Retail Applications
Oracle Retail Convenience and Fuel POS Software, version 2.8.1	Retail Applications
Oracle Retail Customer Insights, versions 15.0, 16.0	Retail Applications
Oracle Retail Integration Bus, version 17.0	Retail Applications
Oracle Retail Merchandising System, version 14.1	Retail Applications
Oracle Retail Returns Management, versions 13.3, 13.4, 14.0, 14.1	Retail Applications
Oracle Retail Sales Audit, version 15.0	Retail Applications
Oracle Retail Service Backbone, versions 13.1, 13.2, 14.0, 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Workforce Management Software, versions 1.60.9, 1.64.0	Retail Applications
Oracle Retail Xstore Payment, version 3.3	Retail Applications
Oracle Secure Global Desktop (SGD), version 5.4	Virtualization
Oracle Service Architecture Leveraging Tuxedo, versions 12.1.3.0.0, 12.2.2.0.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle SOA Suite, versions 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Solaris, versions 10, 11	Systems
Oracle Transportation Management, versions 6.3.7, 6.4.1, 6.4.2, 6.4.3	Oracle Supply Chain Products
Oracle Utilities Framework, version 4.3.0.1-4.3.0.4	Oracle Utilities Applications
Oracle Utilities Network Management System, versions 1.12.0.3, 2.3.0.0, 2.3.0.1, 2.3.0.2	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 5.2.26, prior to 6.0.4	Virtualization
Oracle Web Cache, version 11.1.1.9.0	Fusion Middleware
Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0	Fusion Middleware
Oracle WebCenter Sites, version 11.1.1.8.0	Fusion Middleware
Oracle WebLogic Server, versions 10.3.6.0, 12.1.3.0, 12.2.1.3	Fusion Middleware
OSS Support Tools, versions prior to 19.1	Support Tools
PeopleSoft Enterprise CC Common Application Objects, version 9.2	PeopleSoft
PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2	PeopleSoft
PeopleSoft Enterprise HCM eProfile Manager Desktop, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56, 8.57	PeopleSoft
PeopleSoft Enterprise SCM eProcurement, version 9.2	PeopleSoft
Primavera P6 Enterprise Project Portfolio Management, versions 8.4, 15.1, 15.2, 16.1, 16.2, 17.7-17.12, 18.8	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.1, 16.2, 17.1-17.12, 18.8	Oracle Construction and Engineering Suite
Siebel Applications, versions 18.10, 18.11	Siebel
Sun ZFS Storage Appliance Kit (AK), versions prior to 8.8.2	Systems
Tape Library ACSLS, version 8.4	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:

- An Example working with Trend Micro Zero Day Initiative: CVE-2019-2554
- Andrej Simko of Accenture working with iDefense Labs: CVE-2019-2400, CVE-2019-2445, CVE-2019-2447, CVE-2019-2470, CVE-2019-2485, CVE-2019-2491, CVE-2019-2492, CVE-2019-2496, CVE-2019-2497
- Andres Georgieff of Sandia National Laboratories: CVE-2019-2419, CVE-2019-2439, CVE-2019-2442

- Anonymous Researcher: CVE-2019-2511
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2019-2524, CVE-2019-2525, CVE-2019-2526
- Behzad Najjarpour Jabbari, Secunia Research at Flexera Software: CVE-2016-9389, CVE-2016-9583, CVE-2017-14229, CVE-2019-2456, CVE-2019-2457, CVE-2019-2458, CVE-2019-2459, CVE-2019-2460, CVE-2019-2461, CVE-2019-2462, CVE-2019-2463, CVE-2019-2464, CVE-2019-2465, CVE-2019-2466, CVE-2019-2467, CVE-2019-2468, CVE-2019-2469
- Bui Thanh of Aalto University: CVE-2019-2503
- cPanel Security Team: CVE-2019-2537
- Daniel Kalinowski of LLama's Bytes: CVE-2019-2398
- Deapesh Misra of iDefense, Accenture: CVE-2019-2496
- E. Anonymous working with Trend Micro Zero Day Initiative: CVE-2019-2450
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2019-2444
- YongTao Wang & Sai Cheng of Qihoo360 PegasusTeam: CVE-2019-2426
- Ex Allocate Pool With Tag working with Trend Micro Zero Day Initiative: CVE-2019-2451
- Exhibit A working with Trend Micro Zero Day Initiative: CVE-2019-2555
- Guillaume Teissier of Orange CERT-CC: CVE-2019-2399
- Huy Ngo (Viettel Cyber Security) working with Trend Micro's Zero Day Initiative: CVE-2019-2520, CVE-2019-2521, CVE-2019-2522, CVE-2019-2523
- Huy Ngo of Viettel Cyber Security: CVE-2019-2509
- Ionel Cristinel Anichitei of Bit Defender: CVE-2019-2508
- Jason Matthyser of MWR Labs working with Trend Micro Zero Day Initiative: CVE-2019-2548
- Jayson Grace of Sandia National Laboratories: CVE-2019-2419, CVE-2019-2423
- Jonathan Jacobi: CVE-2019-2556
- Kamlapati Choubey of Trend Micro's Zero Day Initiative: CVE-2018-3147
- Karl Henselin: CVE-2019-2538
- Kasper Leigh Haabb, Secunia Research at Flexera: CVE-2016-9389, CVE-2016-9392, CVE-2017-13745, CVE-2019-2472, CVE-2019-2473, CVE-2019-2474, CVE-2019-2475, CVE-2019-2476, CVE-2019-2477, CVE-2019-2478, CVE-2019-2479, CVE-2019-2480
- Krzysztof Wrobel: CVE-2019-2439
- Lukasz Mikula: CVE-2019-2427
- Maciej Grabiec: CVE-2019-2414
- Marcin Wołoszyn of ING Services Polska: CVE-2019-2415
- Marios Gyftos: CVE-2019-2430, CVE-2019-2431, CVE-2019-2432

- Mark Haase: CVE-2019-2413
- Martin Doyhenard of Onapsis: CVE-2019-2546
- Michal Bazyli: CVE-2019-2414
- Mohamed M. Fouad of SecureMisr: CVE-2019-2413
- Mohamed Sayed of SecureMisr: CVE-2019-2453
- Mohamed Yusuf of SecureMisr: CVE-2019-2549, CVE-2019-2550
- Niklas Baumstark working with Trend Micro's Zero Day Initiative: CVE-2019-2446, CVE-2019-2448, CVE-2019-2525
- Philippe Arteau of GoSecure: CVE-2019-2438
- Piotr Madej of ING Tech Poland: CVE-2019-2395
- Quang Nguyen of Viettel Cyber Security: CVE-2019-2509
- rack911labs.com: CVE-2019-2537
- Rajesh Tv: CVE-2019-2396
- Reno Robert: CVE-2019-2552, CVE-2019-2553
- rgod of 9sg Security Team working with Trend Micro's Zero Day Initiative: CVE-2019-2449
- Root Object working with Trend Micro's Zero Day Initiative: CVE-2019-2500, CVE-2019-2501, CVE-2019-2504, CVE-2019-2505, CVE-2019-2506
- Saif ElSherei of Microsoft Corp: CVE-2019-2429
- Stamatis Kapiris: CVE-2019-2430, CVE-2019-2431, CVE-2019-2432
- Steven Seeley of Source Incite working with iDefense: CVE-2018-3304, CVE-2018-3305
- Zhiyi Zhang of 360 ESG Codesafe Team: CVE-2019-2398, CVE-2019-2452
- Zhouyuan Yang of Fortinet's FortiGuard Labs: CVE-2019-2527

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.:

- Amardeep Chana of MWR InfoSecurity
- George R of Advanced Information Security Corporation

- Jarrod Farncomb of TSS
- Lukasz Rupala
- Maksymilian Arciemowicz
- Martin Balao of Red Hat
- Michael Weissbacher of Northeastern University
- Zhiyi Zhang of 360 ESG Codesafe Team

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:

- Abhishek Misal
- Abu
- Arun Mishra
- Ben Murray
- Markus Pieton of Code White
- Mohit Kumar
- Nicolas Santiago Miguez of Deloitte Risk Advisory Pty Ltd
- Niraj Gautam of Light Pay Coin
- nullx0c0de
- Osman Ahmed Hassan
- Ranjeet Jaiswal
- Sarapremashish Butola
- Seth Duda
- Shoeb Patel (CaptainFreak)
- Srinivas M

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

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - January 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
2024-December-23	Rev 8. Updated EBS iStrore CVE-2019-2483
2020-February-13	Rev 7. Updated credit entry for CVE-2019-2442.
2019-April-18	Rev 6. Updated CVSS score for CVE-2019-2546.
2019-April-16	Rev 5. Updated credit entry for CVE-2018-3304 and CVE-2018-3305.
2019-March-12	Rev 4. Updated credit entry for CVE-2019-2438, CVE-2019-2439 and CVE-2019-2546.
2019-February-01	Rev 3. Updated credit entry for CVE-2019-2426.
2019-January-30	Rev 2. Updated affected versions of CVE-2019-2527 for Oracle Virtualization.
2019-January-15	Rev 1. Initial Release.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 3 new security fixes for the Oracle Database Server. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. None of these fixes are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2444	Core RDBMS	Local Logon	Local Logon	No	8.2	Local	Low	Low	R
CVE-2019-2406	Core RDBMS	Create Session, Execute Catalog Role	Oracle Net	No	7.2	Network	Low	High	
CVE-2019-2547	Java VM	Create Session, Create Procedure	Multiple	No	3.5	Network	Low	Low	R

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 33 new security fixes for Oracle Communications Applications. 29 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-2017-5645	Oracle Communications Converged Application Server - Service Controller	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications Diameter Signaling Router (DSR)	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-2017-5645	Oracle Communications Online Mediation Controller	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2018-11776	Oracle Communications Policy Management	Security (Apache Struts 2)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Communications Service Broker	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Communications Services Gatekeeper	Security (Apache Commons Collections Fileupload)	HTTP	Yes	9.8	Network	Low
CVE-2018-9206	Oracle Communications Services Gatekeeper	Security (jQuery)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Communications WebRTC Session Controller	Security (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-6814	Oracle Communications Unified Inventory Management	Security (Apache Groovy)	HTTP	Yes	9.6	Network	Low
CVE-2016-0635	Oracle Communications Converged Application Server	Security (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2018-1258	Oracle Communications Diameter Signaling Router (DSR)	Security (Spring Framework)	HTTP	No	8.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-1258	Oracle Communications Performance Intelligence Center (PIC) Software	Security (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2018-1258	Oracle Communications Services Gatekeeper	Security (Spring Framework)	HTTP	No	8.8	Network	Low
CVE-2018-14718	Oracle Communications Billing and Revenue Management	Billing Operations Center, Billing Care (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2016-1181	Oracle Communications Converged Application Server	Security (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2017-15095	Oracle Communications Diameter Signaling Router (DSR)	Security (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2016-1181	Oracle Communications WebRTC Session Controller	Security (Apache Struts 1)	HTTP	Yes	8.1	Network	High
CVE-2018-1000180	Oracle Communications Converged Application Server	Security (Bouncy Castle)	HTTP	Yes	7.5	Network	Low
CVE-2017-9798	Oracle Communications Diameter Signaling Router (DSR)	Security (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-5390	Oracle Communications Session Border Controller	Security (Kernel)	TCP	Yes	7.5	Network	Low
CVE-2018-1000180	Oracle Communications WebRTC Session Controller	Security (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low
CVE-2018-1000300	Oracle Communications WebRTC Session Controller	Security (cURL)	HTTP	Yes	7.5	Network	High
CVE-2017-0379	Oracle Communications WebRTC Session Controller	Security (libgcrypt)	TLS	Yes	7.5	Network	Low
CVE-2018-8013	Oracle Communications Diameter Signaling Router (DSR)	Security (Apache Batik)	HTTP	Yes	7.3	Network	Low
CVE-2018-8013	Oracle Communications WebRTC Session Controller	Security (Apache Batik)	HTTP	Yes	7.3	Network	Low
CVE-2019-2399	Oracle Communications Diameter Signaling Router (DSR)	Security	HTTP	Yes	6.5	Network	Low
CVE-2015-9251	Oracle Communications Converged Application Server	Security (JQuery)	HTTP	Yes	6.1	Network	Low
CVE-2015-9251	Oracle Communications WebRTC Session Controller	Security (jQuery)	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-0732	Oracle Communications Session Border Controller	Security (OpenSSL)	TLS	Yes	4.3	Network	Low
CVE-2018-0732	Oracle Communications Unified Session Manager	Security (OpenSSL)	TLS	Yes	4.3	Network	Low
CVE-2018-0732	Oracle Communications WebRTC Session Controller	Security (OpenSSL)	TLS	Yes	4.3	Network	Low
CVE-2018-0732	Oracle Enterprise Communications Broker	Security (OpenSSL)	TLS	Yes	4.3	Network	Low
CVE-2018-0732	Oracle Enterprise Session Border Controller	Security (OpenSSL)	TLS	Yes	4.3	Network	Low

Additional CVEs addressed are below:

- The fix for CVE-2016-0635 also addresses CVE-2018-1258.
- The fix for CVE-2016-1181 also addresses CVE-2014-0114 and CVE-2016-1182.
- The fix for CVE-2017-0379 also addresses CVE-2017-9526.
- The fix for CVE-2017-15095 also addresses CVE-2017-7525.
- The fix for CVE-2018-0732 also addresses CVE-2017-3735, CVE-2017-3736, CVE-2017-3738, CVE-2018-0733, CVE-2018-0737 and CVE-2018-0739.
- The fix for CVE-2018-1000180 also addresses CVE-2015-7940 and CVE-2018-1000613.
- 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-2018-11776 also addresses CVE-2016-1000031.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257, CVE-2018-1270, CVE-2018-1271, CVE-2018-1272 and CVE-2018-1275.
- The fix for CVE-2018-14718 also addresses CVE-2017-15095, CVE-2017-7525, CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721 and CVE-2018-7489.

- The fix for CVE-2018-5390 also addresses CVE-2018-6922.
- The fix for CVE-2018-9206 also addresses CVE-2015-9251.

Oracle Construction and Engineering Suite Risk Matrix

This Critical Patch Update contains 4 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 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2018-9206	Primavera Unifier	Core (jQuery FileUpload)	HTTP	Yes	9.8	Network	Low	None
CVE-2018-14718	Primavera Unifier	Core (jackson-databind)	HTTP	Yes	8.1	Network	High	None
CVE-2018-0732	Primavera P6 Enterprise Project Portfolio Management	Project Manager (OpenSSL)	HTTPS	Yes	7.5	Network	Low	None
CVE-2019-2512	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	Yes	4.7	Network	High	None

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- The fix for CVE-2018-14718 also addresses CVE-2018-14719, CVE-2018-14720 and CVE-2018-14721.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 16 new security fixes for the Oracle E-Business 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.

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 January 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 (January 2019), My Oracle Support Note 2480398.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2489	Oracle One-to-One Fulfillment	OCM Query	HTTP	Yes	9.1	Network	Low	No
CVE-2019-2453	Oracle Performance Management	Performance Management Plan	HTTP	Yes	9.1	Network	Low	No
CVE-2019-2445	Oracle Content Manager	Cover Letter	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2497	Oracle CRM Technical Foundation	Messages	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2483	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2400	Oracle iStore	User Registration	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2440	Oracle Marketing	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2498	Oracle Partner Management	Partner Dash board	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2447	Oracle Partner Management	Partner Detail	HTTP	Yes	8.2	Network	Low	No
CVE-2019-2470	Oracle Partner Management	Partner Detail	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2546	Oracle Applications Manager	SQL Extensions	HTTP	Yes	8.1	Network	Low	No
CVE-2019-2488	Oracle CRM Technical Foundation	Session Management	HTTP	Yes	5.3	Network	Low	No
CVE-2019-2396	Oracle CRM Technical Foundation	Messages	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2496	Oracle CRM Technical Foundation	Messages	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2491	Oracle Email Center	Message Display	HTTP	Yes	4.7	Network	Low	No
CVE-2019-2492	Oracle Email Center	Message Display	HTTP	Yes	4.7	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-2485	Oracle Mobile Field Service	Administration	HTTP	Yes	4.7	Network	Low	No

Oracle Enterprise Manager Products Suite Risk Matrix

This Critical Patch Update contains 11 new security fixes for the Oracle Enterprise Manager Products Suite. 9 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 January 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 January 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2466391.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2016-4000	Enterprise Manager Base Platform	Agent Next Gen (Jython)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1258	Oracle Application Testing Suite	Load Testing for Web Apps (Spring Framework)	HTTP	No	8.8	Network	Low	L
CVE-2018-12023	Enterprise Manager for Virtualization	Plug-In Lifecycle (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2018-14718	Enterprise Manager for Virtualization	Plug-In Lifecycle (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2018-0732	Enterprise Manager Base Platform	Discovery Framework (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-1000300	Enterprise Manager Ops Center	Networking (cURL)	HTTP	Yes	7.5	Network	High	N
CVE-2018-0732	Enterprise Manager Ops Center	Networking (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-3303	Enterprise Manager Base Platform	EM Console	HTTP	Yes	6.5	Network	Low	N
CVE-2018-3304	Oracle Application Testing Suite	Load Testing for Web Apps	HTTP	Yes	6.5	Network	Low	N
CVE-2018-3305	Oracle Application Testing Suite	Load Testing for Web Apps	HTTP	No	6.3	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P Re
CVE-2015-9251	Enterprise Manager Ops Center	Networking (jQuery)	HTTP	Yes	6.1	Network	Low	N

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- 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-2018-12023 also addresses CVE-2018-11307, CVE-2018-12022 and CVE-2018-14718.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-14718 also addresses CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-14719, CVE-2018-14720 and CVE-2018-14721.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 9 new security fixes for Oracle Financial Services 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-2016-4000	Oracle Banking Platform	Patching (Jython)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2017-5645	Oracle FLEXCUBE	Infrastructure (Apache Log4j)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Investor Servicing							
CVE-2018-14718	Oracle Banking Platform	Infrastructure (jackson-databind)	HTTP	Yes	8.1	Network	High	
CVE-2018-14718	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (jackson-databind)	HTTP	Yes	8.1	Network	High	
CVE-2018-1000632	Oracle FLEXCUBE Investor Servicing	Infrastructure (dom4j)	HTTP	Yes	7.5	Network	Low	
CVE-2017-14735	Oracle Banking Platform	Infrastructure (AntiSamy)	HTTP	Yes	6.1	Network	Low	
CVE-2019-2549	Oracle FLEXCUBE Direct Banking	Logoff Page	HTTP	Yes	6.1	Network	Low	
CVE-2019-2550	Oracle FLEXCUBE Direct Banking	Logoff Page	HTTP	Yes	4.3	Network	Low	

Additional CVEs addressed are below:

- The fix for CVE-2018-14718 also addresses CVE-2018-12023, CVE-2018-14719, CVE-2018-14720 and CVE-2018-14721.

Oracle Food and Beverage Applications Risk Matrix

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

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2401	Oracle Hospitality Reporting and Analytics	Admin	HTTP	No	8.1	Network	Low	Low
CVE-2019-2402	Oracle Hospitality Simphony	Client Application Loader	HTTP	Yes	7.7	Network	High	None
CVE-2019-2425	Oracle Hospitality Reporting and Analytics	Report	HTTP	Yes	6.5	Network	Low	None
CVE-2019-2403	Oracle Hospitality Simphony	Enterprise Management Console	HTTP	Yes	6.5	Network	Low	None
CVE-2019-2407	Oracle Hospitality Reporting and Analytics	Report	None	No	6.1	Local	Low	Low
CVE-2019-2397	Oracle Hospitality Reporting and Analytics	Report	None	No	4.4	Local	Low	Low

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 62 new security fixes for Oracle Fusion Middleware. 57 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 January 2019 Critical Patch Update to

the Oracle Database components of Oracle Fusion Middleware products. For information on what patches need to be applied to your environments, refer to Critical Patch Update January 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2466391.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2016-1000031	Oracle Fusion Middleware MapViewer	Install (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle GoldenGate Application Adapters	Application Adapters (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1275	Oracle Service Architecture Leveraging Tuxedo	Internal Operations (Spring Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2017-5645	Oracle SOA Suite	Installation & Templates (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2015-1832	Oracle WebLogic Server	Third Party Tools (Apache Derby)	HTTP	Yes	9.1	Network	Low	N
CVE-2018-14718	Oracle WebCenter Portal	Security Framework (jackson-databind)	HTTP	Yes	8.1	Network	High	N
CVE-2019-2414	Oracle HTTP Server	Web Listener	None	No	7.8	Local	Low	L
CVE-2018-0732	Oracle API Gateway	Oracle API Gateway (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle Business Process Management Suite	Runtime Engine (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2018-0732	Oracle Endeca Server	Third Party (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle Enterprise Repository	Security Subsystem - 12c (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2467	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2468	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2473	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2474	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2475	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2476	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2477	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2479	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N
CVE-2016-9389	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	7.5	Network	Low	N
CVE-2017-13745	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
		(Jasper Project)						
CVE-2016-9392	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle WebCenter Portal	Security Framework (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	N
CVE-2018-1000180	Oracle WebLogic Server	WLS Core Components (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-2462	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.2	Network	Low	N
CVE-2019-2538	Oracle Managed File Transfer	MFT Runtime Server	HTTP	No	7.1	Network	Low	L
CVE-2019-2429	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.1	Network	Low	N
CVE-2019-2438	Oracle Web Cache	ESI/Partial Page Caching	HTTP	Yes	6.9	Network	High	N
CVE-2018-11775	Oracle Enterprise Repository	Security Subsystem (Apache ActiveMQ)	HTTP	Yes	6.8	Network	High	N
CVE-2019-2452	Oracle WebLogic Server	WLS Core Components	HTTP	No	6.7	Network	Low	H
CVE-2019-2456	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2463	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	Low	N
CVE-2019-2469	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network	High	N
CVE-2019-2418	Oracle WebLogic Server	WLS Core Components	T3	Yes	6.5	Network	High	N
CVE-2015-9251	Oracle Business Process Management Suite	Runtime Engine (JQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-2413	Oracle Reports Developer	Valid Session	HTTP	Yes	6.1	Network	Low	N
CVE-2017-14735	Oracle WebCenter Sites	Third Party Tools (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2015-9251	Oracle WebLogic Server	Sample apps (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-2395	Oracle WebLogic Server	WLS - Web Services	HTTP	No	5.4	Network	Low	L
CVE-2019-2457	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2458	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2459	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2460	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2461	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2464	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2465	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2466	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2472	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2478	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2480	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low	N
CVE-2016-9389	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	5.3	Network	Low	N
CVE-2016-9389	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	5.3	Network	Low	N
CVE-2016-9389	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	5.3	Network	Low	N
CVE-2016-9583	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	5.3	Network	Low	N
CVE-2016-9389	Oracle Outside In	Outside In Filters	HTTP	Yes	5.3	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Technology	(Jasper Project)						
CVE-2016-9392	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	5.3	Network	Low	N
CVE-2016-9389	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2427	Oracle WebCenter Portal	WebCenter Spaces Application	HTTP	Yes	5.3	Network	Low	N
CVE-2019-2441	Oracle WebLogic Server	Application Container - JavaEE	HTTP	Yes	5.3	Network	Low	N
CVE-2018-3147	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	4.3	Network	Low	N
CVE-2019-2398	Oracle WebLogic Server	WLS - Deployment	HTTP	No	4.3	Network	Low	L
CVE-2017-14229	Oracle Outside In Technology	Outside In Filters (Jasper Project)	HTTP	Yes	3.1	Network	High	N

Notes:

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

Additional CVEs addressed are below:

- The fix for CVE-2015-1832 also addresses CVE-2018-1313.
- The fix for CVE-2016-9392 also addresses CVE-2016-9389.
- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613 and CVE-2018-3246.

- The fix for CVE-2018-1275 also addresses CVE-2018-1258, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.
- The fix for CVE-2018-14718 also addresses CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-14719, CVE-2018-14720 and CVE-2018-14721.

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 6 new security fixes for Oracle Health Sciences 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#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2018-1258	Oracle Health Sciences Information Manager	Health Policy Engine (Spring Framework)	HTTP	No	8.8	Network	Low	Low	
CVE-2018-1258	Oracle Healthcare Master Person Index	Core (Spring Framework)	HTTP	No	8.8	Network	Low	Low	
CVE-2019-2430	Oracle Argus Safety	Console	HTTP	No	6.5	Network	Low	Low	
CVE-2019-2431	Oracle Argus Safety	Console	HTTP	Yes	6.1	Network	High	None	
CVE-2015-9251	Oracle Healthcare Foundation	Install (jQuery)	HTTP	Yes	6.1	Network	Low	None	
CVE-2019-2432	Oracle Argus Safety	Login	HTTP	No	4.9	Network	High	Low	

Additional CVEs addressed are below:

- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257, CVE-2018-1270, CVE-2018-1271, CVE-2018-1272 and CVE-2018-1275.

Oracle Hospitality Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2016-5684	Oracle Hospitality Cruise Fleet Management	Corporate Access Module (Freeimage)	None	No	7.8	Local	Low	None
CVE-2016-5684	Oracle Hospitality Cruise Shipboard Property Management System	SPMS Shared Libraries (Freeimage)	None	No	7.8	Local	Low	None
CVE-2019-2411	Oracle Hospitality Cruise Shipboard Property Management System	SPMS Suite	TCP	No	7.6	Network	Low	Low
CVE-2019-2409	Oracle Hospitality Cruise Shipboard Property Management System	SPMS Suite	None	No	7.3	Local	Low	Low
CVE-2019-2410	Oracle Hospitality Cruise Shipboard Property Management System	DGS RES Online, FMS Sender, FMS Receiver, OHC WPF Security	None	No	5.1	Local	Low	None

Additional CVEs addressed are below:

- The fix for CVE-2016-5684 also addresses CVE-2015-0852.

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Hyperion. 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 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2019-2415	Hyperion BI+	Foundation UI & Servlets	HTTP	No	4.3	Network	Low	High	Rec

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 5 new security fixes for Oracle Insurance 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			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2018-1258	Oracle Insurance Calculation Engine	Core (Spring Framework)	HTTP	No	8.8	Network	Low	Lov
CVE-2018-1258	Oracle Insurance Rules Palette	Core (Spring Framework)	HTTP	No	8.8	Network	Low	Lov
CVE-2018-8013	Oracle Insurance Policy Administration J2EE	User Interface (Apache Batik)	HTTP	Yes	7.3	Network	Low	Nor
CVE-2015-9251	Oracle Insurance Insbridge Rating and Underwriting	Framework (jQuery)	HTTP	Yes	6.1	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2017-14735	Oracle Insurance Policy Administration J2EE	Core (AntiSamy)	HTTP	Yes	6.1	Network	Low	Nor

Additional CVEs addressed are below:

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

Oracle Java SE Risk Matrix

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

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2540	Java Advanced Management Console	Server	Multiple	Yes	6.1	Network	Low	None
CVE-2018-11212	Java SE	ImageIO (libjpeg)	Multiple	Yes	5.3	Network	Low	None
CVE-2019-2426	Java SE	Networking	Multiple	Yes	3.7	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2449	Java SE	Deployment	Multiple	Yes	3.1	Network	High	None
CVE-2019-2422	Java SE	Libraries	Multiple	Yes	3.1	Network	High	None

Notes:

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

2. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

Oracle JD Edwards Products Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle JD Edwards Products. 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2018-8013	JD Edwards EnterpriseOne Tools	Web Runtime SEC (Apache Batik)	HTTP	Yes	9.8	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2018-0732	JD Edwards World Security	Security (OpenSSL)	HTTPS	Yes	7.5	Network	Low	None

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2017-3738, CVE-2018-0733, CVE-2018-0737 and CVE-2018-0739.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 30 new security fixes for Oracle MySQL. 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 VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2018-10933	MySQL Workbench	MySQL Workbench (libssh)	MySQL Workbench	Yes	9.1	Network	Low
CVE-2019-2435	MySQL Connectors	Connector/Python	TLS	Yes	8.1	Network	Low
CVE-2018-0732	MySQL Workbench	MySQL Workbench (OpenSSL)	MySQL Workbench	Yes	7.5	Network	Low
CVE-2019-2534	MySQL Server	Server: Replication	MySQL Protocol	No	7.1	Network	Low
CVE-2019-2533	MySQL Server	Server : Security : Privileges	MySQL Protocol	No	6.5	Network	Low
CVE-2019-2529	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2019-2482	MySQL Server	Server: PS	MySQL Protocol	No	6.5	Network	Low
CVE-2019-2434	MySQL Server	Server: Parser	MySQL Protocol	No	6.5	Network	Low
CVE-2019-2455	MySQL Server	Server: Parser	MySQL Protocol	No	6.5	Network	Low
CVE-2019-2503	MySQL Server	Server: Connection Handling	MySQL Protocol	No	6.4	Adjacent Network	High
CVE-2019-2436	MySQL Server	Server: Replication	MySQL Protocol	No	5.5	Network	Low
CVE-2018-0734	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	No	5.1	Local	High
CVE-2019-2536	MySQL Server	Server: Packaging	MySQL Protocol	No	5.0	Local	High
CVE-2019-2502	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2019-2510	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2539	MySQL Server	Server: Connection	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2494	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2495	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2537	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2420	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2481	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2507	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2530	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2528	MySQL Server	Server: Partition	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2531	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2019-2486	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2532	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2535	MySQL Server	Server: Options	MySQL Protocol	No	4.1	Local	High
CVE-2019-2513	MySQL Server	Shell	None	No	2.5	Local	High
CVE-2018-0732	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	None	No	0.0	Local	Low

Notes:

1. MySQL Enterprise Monitor is not vulnerable to this CVE because it does not use the TLS functionality included in OpenSSL. The CVSS v3.0 Base Score for this CVE in the National Vulnerability Database (NVD) is 7.5.

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- The fix for CVE-2018-0734 also addresses CVE-2018-5407.

Oracle PeopleSoft Products Risk Matrix

This Critical Patch Update contains 20 new security fixes for Oracle PeopleSoft Products. 15 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-2416	PeopleSoft Enterprise PeopleTools	Application Server	HTTP	No	8.8	Network	Low	
CVE-2018-1000300	PeopleSoft Enterprise PeopleTools	File Processing (cURL)	HTTP	Yes	7.5	Network	High	
CVE-2019-2405	PeopleSoft Enterprise PeopleTools	Security	HTTP	No	7.5	Network	High	
CVE-2018-0732	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	7.5	Network	Low	
CVE-2019-2433	PeopleSoft Enterprise PeopleTools	XML Publisher	HTTP	No	7.2	Network	Low	
CVE-2019-2443	PeopleSoft Enterprise PeopleTools	XML Publisher	HTTP	No	7.2	Network	Low	
CVE-2019-2417	PeopleSoft Enterprise PeopleTools	Performance Monitor	HTTP	Yes	6.5	Network	Low	
CVE-2019-2421	PeopleSoft Enterprise HCM eProfile Manager Desktop	Guided Self Service	HTTP	Yes	6.1	Network	Low	
CVE-2019-2442	PeopleSoft Enterprise PeopleTools	Fluid Core	HTTP	Yes	6.1	Network	Low	
CVE-2015-9251	PeopleSoft Enterprise PeopleTools	Mobile Application Platform (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2019-2423	PeopleSoft Enterprise PeopleTools	PIA Search	HTTP	Yes	6.1	Network	Low	
CVE-2019-2499	PeopleSoft Enterprise PeopleTools	PIA Search Functionality	HTTP	Yes	6.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-2439	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	
CVE-2019-2471	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	
CVE-2019-2519	PeopleSoft Enterprise SCM ePROCUREMENT	Manage Requisition Status	HTTP	Yes	6.1	Network	Low	
CVE-2019-2419	PeopleSoft Enterprise CC Common Application Objects	Form and Approval Builder	HTTP	No	5.4	Network	Low	
CVE-2019-2404	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	5.3	Network	Low	
CVE-2019-2490	PeopleSoft Enterprise PeopleTools	Panel Processor	HTTP	Yes	4.7	Network	Low	
CVE-2019-2408	PeopleSoft Enterprise PeopleTools	Feeds	HTTP	Yes	4.3	Network	Low	
CVE-2019-2493	PeopleSoft Enterprise CS Campus Community	Frameworks	HTTP	Yes	3.1	Network	High	

Notes:

1. This Enterprise Common Component is used by all PeopleSoft Application products. Please refer to the MOS Note Doc ID 2493366.1 for patch information.

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- The fix for CVE-2018-1000300 also addresses CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122 and CVE-2018-1000301.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 16 new security fixes for Oracle Retail Applications. 15 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2016-1000031	Oracle Retail Back Office	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Retail Central Office	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Retail Returns Management	Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Retail Service Backbone	Install (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2017-7658	Oracle Retail Xstore Payment	Security (Jetty)	HTTP	Yes	9.8	Network	Low	
CVE-2018-1258	Oracle Retail Customer Insights	Other (Spring Framework)	HTTP	No	8.8	Network	Low	
CVE-2018-3311	Oracle Retail Xstore Payment	Security	HTTP	Yes	8.6	Network	Low	
CVE-2018-1000180	Oracle Retail Convenience and Fuel POS Software	Point of Sale (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	
CVE-2018-8013	Oracle Retail Integration Bus	RIB Kernel (Apache Batik)	HTTP	Yes	7.3	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2018-3125	Oracle Retail Merchandising System	Security (SQL Logger)	HTTP	Yes	6.5	Network	Low	
CVE-2017-14735	Oracle Retail Back Office	Security (AntiSamy)	HTTP	Yes	6.1	Network	Low	
CVE-2017-14735	Oracle Retail Central Office	Security (AntiSamy)	HTTP	Yes	6.1	Network	Low	
CVE-2015-9251	Oracle Retail Customer Insights	Other (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2017-14735	Oracle Retail Returns Management	Security (AntiSamy)	HTTP	Yes	6.1	Network	Low	
CVE-2015-9251	Oracle Retail Sales Audit	Operational Insights (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2015-9251	Oracle Retail Workforce Management Software	Framework (jQuery)	HTTP	Yes	6.1	Network	Low	

Additional CVEs addressed are below:

- The fix for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-3311 also addresses CVE-2015-4760.

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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2018-9206	Siebel UI Framework	UIF Open UI (jQuery FileUpload)	HTTP	Yes	9.8	Network	Low	None	

Oracle Sun Systems Products Suite Risk Matrix

This Critical Patch Update contains 11 new security fixes for the Oracle Sun Systems Products Suite. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2017-5645	Tape Library ACSLS	Software (Apache Log4j)	HTTP	Yes	9.8	Network	Low	None	
CVE-2018-1275	Tape Library ACSLS	Software (Spring Framework)	HTTP	Yes	9.8	Network	Low	None	
CVE-2016-0635	Tape Library ACSLS	Software (Spring Framework)	HTTP	No	8.8	Network	Low	Low	
CVE-2019-2541	Oracle Solaris	DHCP Client	DHCP	Yes	7.5	Adjacent Network	High	None	
CVE-2019-2437	Oracle Solaris	Kernel	TCP	Yes	7.5	Network	Low	None	
CVE-2019-2412	Sun ZFS Storage Appliance Kit (AK)	Object Store	None	No	6.4	Local	High	High	
CVE-2018-3646	Oracle Solaris	Kernel	None	No	5.6	Local	High	Low	
CVE-2018-3639	Oracle Solaris	Kernel	None	No	5.5	Local	Low	Low	
CVE-2019-2543	Oracle Solaris	Kernel	KSSL	Yes	5.3	Network	Low	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2019-2544	Oracle Solaris	Kernel	None	No	4.0	Local	Low	None	
CVE-2019-2545	Oracle Solaris	LDoms IO	None	No	4.0	Local	Low	None	

Additional CVEs addressed are below:

- The fix for CVE-2018-1275 also addresses CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.

Oracle Supply Chain Products Suite Risk Matrix

This Critical Patch Update contains 5 new security fixes for the Oracle Supply Chain Products Suite. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2015-8965	Oracle Agile PLM	Gantt Chart (JViews)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2018-0732	Oracle Agile Engineering Data Management	Install (OpenSSL)	HTTPS	Yes	7.5	Network	Low	Nc
CVE-2019-2487	Oracle Transportation Management	UI Infrastructure	HTTP	No	6.5	Network	Low	Lc
CVE-2017-14735	Oracle Agile PLM	Security (AntiSamy)	HTTP	Yes	6.1	Network	Low	Nc
CVE-2015-9251	Oracle Agile Product Lifecycle Management for Process	Supplier Portal (jQuery)	HTTP	Yes	6.1	Network	Low	Nc

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.

Oracle Support Tools Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2018-0732	OSS Support Tools	Services Tools Bundle (OpenSSL)	HTTPS	Yes	7.5	Network	Low	None	Nc

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle Utilities 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 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'c
CVE-2016-4000	Oracle Utilities Network Management System	System wide (Jython)	HTTP	Yes	9.8	Network	Low	None
CVE-2015-9251	Oracle Utilities Framework	User Interface (jQuery)	HTTP	Yes	6.1	Network	Low	None

Additional CVEs addressed are below:

- The fix for CVE-2016-4000 also addresses CVE-2018-1000180 and CVE-2018-1000613.

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 30 new security fixes for Oracle Virtualization. 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 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2500	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2524	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2019-2552	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2018-3309	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2019-2520	Oracle VM VirtualBox	Core	None	No	7.8	Local	High	Low	
CVE-2019-2521	Oracle VM VirtualBox	Core	None	No	7.8	Local	High	Low	
CVE-2019-2522	Oracle VM VirtualBox	Core	None	No	7.8	Local	High	Low	
CVE-2019-2523	Oracle VM VirtualBox	Core	None	No	7.8	Local	High	Low	
CVE-2019-2526	Oracle VM VirtualBox	Core	None	No	7.8	Local	High	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2548	Oracle VM VirtualBox	Core	None	No	7.8	Local	Low	Low	
CVE-2018-11763	Oracle Secure Global Desktop (SGD)	Web Server (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	None	
CVE-2019-2511	Oracle VM VirtualBox	Core	SOAP	Yes	7.5	Network	Low	None	
CVE-2019-2508	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2509	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2527	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2450	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2451	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2555	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2554	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2019-2556	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2018-11784	Oracle Secure Global Desktop (SGD)	Application Server (Apache Tomcat)	HTTP	Yes	6.1	Network	Low	None	R
CVE-2018-0734	Oracle VM VirtualBox	Core (OpenSSL)	TLS	Yes	5.9	Network	High	None	
CVE-2019-2525	Oracle VM VirtualBox	Core	None	No	5.6	Local	High	Low	
CVE-2019-2446	Oracle VM VirtualBox	Core	None	No	5.5	Local	Low	Low	
CVE-2019-2448	Oracle VM VirtualBox	Core	None	No	5.5	Local	Low	Low	
CVE-2019-2501	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	
CVE-2019-2504	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	
CVE-2019-2505	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-2506	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	
CVE-2019-2553	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	

Additional CVEs addressed are below:

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

© 2026 Oracle | Privacy / Do Not Sell My Info Cookie Preferences Ad Choices Careers
Integrity Helpline Contact Us