Oracle Critical Patch Update Advisory - October 2019

Oracle Critical Patch Update Advisory - October 2019

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Please refer to:

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

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update security patches without delay.

This Critical Patch Update contains 219 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at October 2019 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Agile Recipe Management for Pharmaceuticals, versions 9.3.3, 9.3.4	Oracle Supply Chain Products
Diagnostic Assistant, version 2.12.36	Support Tools
Enterprise Manager Base Platform, versions 13.2, 13.3	Enterprise Manager
Enterprise Manager for Exadata, versions 12.1.0.5.0, 13.2.2.0.0, 13.3.1.0.0, 13.3.2.0.0	Enterprise Manager
Enterprise Manager Ops Center, versions 12.3.3, 12.4.0	Enterprise Manager
Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2361, prior to XCP3071	Systems
Hyperion Data Relationship Management, version 11.1.2.4	Fusion Middleware
Hyperion Enterprise Performance Management Architect, version 11.1.2.4	Fusion Middleware
Hyperion Financial Reporting, version 11.1.2.4	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineerir Suite
JD Edwards EnterpriseOne Tools, version 4.0.1.0	JD Edwards
MICROS Relate CRM Software, versions 7.1.0, 11.4, 15.0.0, 16.0.0, 17.0.0, 18.0.0	Retail Applications
MICROS Retail XBRi Loss Prevention, version 10.8.3	Retail Applications
MySQL Connectors, versions 5.3.13 and prior, 8.0.17 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.17 and prior	MySQL
MySQL Server, versions 5.6.45 and prior, 5.7.27 and prior, 8.17 and prior	MySQL
MySQL Workbench, versions 8.0.17 and prior	MySQL
Oracle Agile PLM, versions 9.3.3-9.3.6	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	Oracle Supply Chain Products
Oracle API Gateway, version 11.1.2.4.0	Fusion Middleware
Oracle Application Testing Suite, versions 13.2, 13.3	Enterprise Manager
Oracle Banking Digital Experience, versions 18.1, 18.2, 18.3, 19.1	Oracle Financial Services Applicatio
Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.7.0, 2.7.1	Oracle Banking Platform
Oracle BI Publisher, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Clusterware, version 19.0.0.0.0	Support Tools
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 E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.9	E-Business Suite
Oracle Enterprise Repository, version 12.1.3.0.0	Fusion Middleware
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.2-8.0.8	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Enterprise Financial Performance Analytics, versions 8.0.6, 8.0.7	Oracle Financial Services Enterprise Financial Performance Analytics
Oracle Financial Services Retail Performance Analytics, versions 8.0.6, 8.0.7	Oracle Financial Services Retail Performance Analytics
Oracle FLEXCUBE Direct Banking, versions 12.0.2, 12.0.3	Oracle Financial Services Applicatio
Oracle Forms, version 12.2.1.3.0	Fusion Middleware
Oracle GoldenGate Application Adapters, version 12.3.2.1.0	Fusion Middleware
Oracle GraalVM Enterprise Edition, version 19.2.0	Oracle GraalVM Enterprise Edition
Oracle Healthcare Foundation, versions 7.1.1, 7.2.2	Health Sciences
Oracle Healthcare Translational Research, versions 3.1.0, 3.2.1, 3.3.1	Health Sciences
Oracle Hospitality Cruise Dining Room Management, version 8.0.80	Oracle Hospitality Cruise Dining Ro Management
Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1	Oracle Hospitality Guest Access
Oracle Hospitality Materials Control, version 18.1	Oracle Hospitality Materials Control
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle Hospitality RES 3700, version 5.7	Oracle Hospitality RES
Oracle Java SE, versions 7u231, 8u221, 11.0.4, 13	Java SE
Oracle Java SE Embedded, version 8u221	Java SE
Oracle JDeveloper and ADF, versions 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle NoSQL Database, versions prior to 19.3.12	NoSQL Database
Oracle Outside In Technology, version 8.5.4	Fusion Middleware
Oracle Policy Automation, versions 10.4.7, 12.1.0, 12.1.1, 12.2.0-12.2.15	Oracle Policy Automation
Oracle Policy Automation Connector for Siebel, version 10.4.6	Oracle Policy Automation

Affected Products and Versions	Patch Availability Document
Oracle Policy Automation for Mobile Devices, versions 12.2.0-12.2.15	Oracle Policy Automation
Oracle Retail Customer Insights, versions 15.0, 16.0	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, version 17.0	Retail Applications
Oracle Retail Integration Bus, versions 15.0, 16.0	Retail Applications
Oracle Retail Xstore Office, version 7.1	Retail Applications
Oracle Retail Xstore Point of Service, versions 7.1, 15.0, 16.0, 17.0, 17.0.3, 18.0, 18.0.1, 19.0.0	Retail Applications
Oracle Service Bus, 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	Systems
Oracle Virtual Directory, version 11.1.1.9.0	Fusion Middleware
Oracle VM VirtualBox, versions prior to 5.2.34, prior to 6.0.14	Virtualization
Oracle Web Services, version 12.2.1.3.0	Fusion Middleware
Oracle WebCenter Portal, 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, 12.2.1.4.0	Fusion Middleware
PeopleSoft Enterprise HCM Human Resources, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57	PeopleSoft
PeopleSoft Enterprise SCM eProcurement, version 9.2	PeopleSoft
Primavera Gateway, versions 15.2, 16.2, 17.12, 18.8	Oracle Construction and Engineerir Suite
Primavera P6 Enterprise Project Portfolio Management, versions 15.1.0-15.2.18, 16.1.0-16.2.18, 17.1.0-17.12.14, 18.1.0-18.8.13	Oracle Construction and Engineerir Suite
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8	Oracle Construction and Engineerir Suite
Siebel Applications, versions 19.8 and prior	Siebel

Note:

- Vulnerabilities affecting Oracle Database and Oracle Fusion Middleware may affect Oracle Fusion Applications, so Oracle customers should refer to Oracle Fusion Applications Critical Patch Update Knowledge Document, My Oracle Support Note 1967316.1 for information on patches to be applied to Fusion Application environments.
- Vulnerabilities affecting Oracle Solaris may affect Oracle ZFSSA so Oracle customers should refer to the Oracle and Sun Systems Product Suite Critical Patch Update Knowledge

Document, My Oracle Support Note 2160904.1 for information on minimum revisions of security patches 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 addressed by the patches associated with this advisory. Risk matrices for previous security patches can be found in previous Critical Patch Update advisories and Alerts. An English text version of the risk matrices provided in this document is here.

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. Each vulnerability is identified by a CVE# which is 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 security patches as soon as possible. Until you apply the Critical Patch Update patches, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or

access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

Oracle strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Critical Patch Update Supported Products and Versions

Patches released through the Critical Patch Update program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the Lifetime Support Policy. Oracle recommends that customers plan product upgrades to ensure that patches released through the Critical Patch Update program are available for the versions they are currently running.

Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, it is likely that earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

Database, Fusion Middleware, and Oracle Enterprise Manager products are patched in accordance with the Software Error Correction Support Policy explained in My Oracle Support Note 209768.1. Please review the Technical Support Policies for further guidelines regarding support policies and phases of support.

Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Critical Patch Update to Oracle:

- Alaa Kachouh of Bankmed: CVE-2019-3019
- Alexander Kornbrust of Red Database Security: CVE-2018-2875, CVE-2019-2895, CVE-2019-2939
- Alpha66647777: CVE-2019-2978
- Amaal Khalid of SecureMisr: CVE-2019-2979, CVE-2019-2980

- Andrej Simko of Accenture: CVE-2019-2930, CVE-2019-2990, CVE-2019-2994, CVE-2019-2995, CVE-2019-3000, CVE-2019-3022, CVE-2019-3024
- Andrej Simko of Accenture working with iDefense Labs: CVE-2019-2930
- Andrzej Dyjak of sigsegv.pl: CVE-2019-2901, CVE-2019-2902, CVE-2019-2903, CVE-2019-2970, CVE-2019-2971, CVE-2019-2972
- anhdaden of STAR Labs: CVE-2019-2984, CVE-2019-3002, CVE-2019-3005
- Anhdaden of StarLabs working with Trend Micro's Zero Day Initiative: CVE-2019-3026, CVE-2019-3031
- Badcode of Knownsec 404 Team: CVE-2019-2888
- Bartlomiej Stasiek: CVE-2019-2941
- Dimitrios - Georgios Karetsos of COSMOTE - Mobile Telecommunications S.A.: CVE-2019-2959
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2019-2954, CVE-2019-2955
- Ehsan Nikavar: CVE-2019-2898
- Emad Al-Mousa of Saudi Aramco: CVE-2019-2940
- Huyna of Viettel Cyber Security working with Trend Micro Zero Day Initiative: CVE-2019-3017
- Imre Rad: CVE-2019-2996
- Jakub Palaczynski: CVE-2019-2927
- Jakub Palaczynski of ING Tech Poland: CVE-2019-2886
- Jan Jancar of Masaryk University: CVE-2019-2894
- Jean-Benjamin Rousseau of SEC Consult Vulnerability Lab: CVE-2019-17091
- Krzysztof Bednarski of ING Tech Poland: CVE-2019-2886
- Kyle Stiemann of Liferay: CVE-2019-17091
- Laura Rowieska: CVE-2019-2897
- Lewei Qu of Baidu, Inc.: CVE-2019-3021
- lofiboy of infiniti Team, VinCSS (a member of Vingroup): CVE-2019-2926, CVE-2019-2944
- Longofo of Knownsec 404 Team: CVE-2019-2888
- Lukasz Mikula: CVE-2019-2932
- Lukasz Rupala of ING Tech Poland: CVE-2019-2900, CVE-2019-3012
- Marco Ivaldi of Media Service: CVE-2019-3010
- Marek Cybul: CVE-2019-3014, CVE-2019-3015
- Michal Skowron: CVE-2019-2897
- MitAh of Tencent Security Xuanwu Lab: CVE-2019-2999

- TSM_007 of TSM: CVE-2019-3012
- Owais Zaman of Sabic: CVE-2019-3020
- Philippe Antoine, Christopher Alves, Zouhair Janatil-Idrissi, Julien Zhan (Telecom Nancy): CVE-2019-2993, CVE-2019-3011
- Ramnath Shenoy of NCC Group: CVE-2019-3015
- Resecurity, Inc.: CVE-2019-3028
- Rob Hamm of sas.com: CVE-2019-2949
- RunningSnail: CVE-2019-2889
- Saeed Shiravi: CVE-2019-3012
- Spyridon Chatzimichail of OTE Hellenic Telecommunications Organization S.A.: CVE-2019-2959
- Steven Danneman of Security Innovation: CVE-2019-2922, CVE-2019-2923, CVE-2019-2924
- tint0 of Viettel Cyber Security working with Trend Micro Zero Day Initiative: CVE-2019-2904
- Tomasz Wisniewski: CVE-2019-2906
- Vahagn Vardanyan: CVE-2019-2905, CVE-2019-2907
- Venustech ADLab: CVE-2019-2887, CVE-2019-2890
- Vladimir Egorov: CVE-2019-2905, CVE-2019-2907
- Walid Faour: CVE-2019-3025
- Zohaib Tasneem of Sabic: CVE-2019-3020

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.:

- Amit Kaplan of GE
- An Trinh
- Bartlomiej Zogala
- Ben Heimerdinger of Code White GmbH
- Cornelius Aschermann of Ruhr-University Bochum

- George R
- Joshua Graham of TSS
- Lucas Fink
- Markus Wulftange of Code White GmbH
- Roberto Suggi Liverani of NATO Communications and Information Agency
- Roy Haroush of GE
- Sergej Schumilo of Ruhr-University Bochum
- Simon Worner
- Tin Duong of Fortinet's FortiGuard Labs
- voidfyoo of Chaitin Tech

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:

- Arun Babu
- Ben Stock of CISPA Helmholtz Center for Information Security (Germany)
- Dudy Shaul
- Khiem Tran
- Malavika SK
- Nick Nikiforakis
- Pooja B Sen
- Ronak Nahar
- Sajjad Hashemian
- Shubham Garg [nullb0t] of JMIETI
- Stefano Calzavara
- 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:

- 14 January 2020
- 14 April 2020
- 14 July 2020
- 20 October 2020

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - October 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
- Oracle Lifetime support Policy

Modification History

Date	Note
2019-October-15	Rev 1. Initial Release.
2019-November-26	Rev 2. Update Entry for CVE-2019-2941
2020-January-22	Rev 3. Update affected version Entry for CVE-2019-2888

Oracle Database Server Risk Matrix

This Critical Patch Update contains 11 new security patches for the Oracle Database Server divided as follows:

- 10 new security patches for the Oracle Database Server. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

- 1 new security patch for Oracle NoSQL Database. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2909	Java VM	None	Multiple	Yes	6.8	Network	High	N
CVE-2019-2956	Core RDBMS (jackson-databind)	Create Session	Multiple	No	5.7	Network	Low	L
CVE-2019-2913	Core RDBMS	Create Session	OracleNet	No	5.0	Network	Low	L
CVE-2019-2939	Core RDBMS	Create Session	OracleNet	No	5.0	Network	Low	L
CVE-2018-2875	Core RDBMS	Create Session	OracleNet	No	5.0	Network	Low	L
CVE-2019-2734	Core RDBMS	Create Session, Execute on DBMS_ADVISOR	OracleNet	No	4.3	Network	Low	L
CVE-2018-11784	WLM (Apache Tomcat)	None	HTTP	Yes	4.3	Network	Low	N
CVE-2019-2954	Core RDBMS	Create Session, Create Procedure	Multiple	No	3.9	Local	Low	L
CVE-2019-2955	Core RDBMS	Local Logon	Multiple	No	3.9	Local	Low	L
CVE-2019-2940	Core RDBMS	Create Session	OracleNet	No	2.3	Local	Low	H

Additional CVEs addressed are below:

- The patch for CVE-2018-11784 also addresses CVE-2018-8034.
- The patch for CVE-2019-2956 also addresses CVE-2018-1000873, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361 and CVE-2018-19362.

Oracle NoSQL Database Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle NoSQL Database. 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	U Int
CVE-2018-14721	Oracle NoSQL Database	NoSQL (jackson-databind)	HTTP	Yes	10.0	Network	Low	None	N

Additional CVEs addressed are below:

- The patch for CVE-2018-14721 also addresses CVE-2018-1000873, CVE-2018-11798, CVE-2018-1320, CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-19360, CVE-2018-19361, CVE-2018-19362, CVE-2019-12086, CVE-2019-12384 and CVE-2019-12814.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 13 new security patches for Oracle Construction and Engineering. 11 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2017-6056	Instantis EnterpriseTrack	Core (Apache Tomcat)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-14379	Primavera Gateway	Admin (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-14379	Primavera Unifier	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-3020	Primavera P6 Enterprise	Web Access	HTTP	Yes	9.3	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
	Project Portfolio Management							
CVE-2019-0232	Instantis EnterpriseTrack	Generic (Apache Tomcat)	HTTP	Yes	8.1	Network	High	No
CVE-2019-0211	Instantis EnterpriseTrack	Generic (Apache HTTP Server)	None	No	7.8	Local	Low	Lo
CVE-2019-0227	Instantis EnterpriseTrack	Generic (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	No
CVE-2017-12626	Instantis EnterpriseTrack	Generic (Apache POI)	HTTP	Yes	7.5	Network	Low	No
CVE-2017-12626	Primavera Gateway	Admin (Apache POI)	HTTP	Yes	7.5	Network	Low	No
CVE-2017-12626	Primavera P6 Enterprise Project Portfolio Management	Web Access (Apache POI)	HTTP	Yes	7.5	Network	Low	No
CVE-2017-12626	Primavera Unifier	Core (Apache POI)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-2976	Primavera P6 Enterprise Project Portfolio Management	Web Access	HTTP	No	6.8	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-11358	Primavera Unifier	Core (jQuery)	HTTP	Yes	6.1	Network	Low	No

Additional CVEs addressed are below:

- The patch for CVE-2017-6056 also addresses CVE-2016-5425.
- The patch for CVE-2019-0211 also addresses CVE-2019-0196, CVE-2019-0197, CVE-2019-0215, CVE-2019-0217 and CVE-2019-0220.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-0232 also addresses CVE-2019-10072.
- The patch for CVE-2019-14379 also addresses CVE-2019-12086, CVE-2019-14439, CVE-2019-14540 and CVE-2019-16335.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 10 new security patches 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 updates are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that customers apply the October 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 (October 2019), My Oracle Support Note 2586423.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2942	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2990	Oracle iStore	Order Tracker	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2994	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	None
CVE-2019-2995	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	None
CVE-2019-3000	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	None
CVE-2019-3022	Oracle Content Manager	Content	HTTP	Yes	5.8	Network	Low	None
CVE-2019-3027	Oracle Application Object Library	Login Help	HTTP	Yes	5.3	Network	Low	None
CVE-2019-2930	Oracle Field Service	Wireless	HTTP	Yes	4.7	Network	Low	None
CVE-2019-3024	Oracle Installed Base	Engineering Change Order	HTTP	Yes	4.7	Network	Low	None
CVE-2019-2925	Oracle Workflow	Worklist	HTTP	Yes	4.3	Network	Low	None

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Enterprise Manager. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found here.

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the October 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 October 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2568292.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2016-4000	Enterprise Manager Base Platform	Command Line Interface (Jython)	HTTP	Yes	9.8	Network	Low	None	
CVE-2019-5443	Enterprise Manager Ops Center	Networking (cURL)	None	No	7.8	Local	Low	Low	
CVE-2019-2895	Enterprise Manager for Exadata	Exadata Plug-In Deploy and Ins	HTTP	No	7.5	Network	High	Low	
CVE-2019-9517	Enterprise Manager Ops Center	OS Provisioning (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	None	
CVE-2019-11358	Enterprise Manager Ops Center	Networking (jQuery)	HTTP	Yes	6.1	Network	Low	None	
CVE-2019-11358	Oracle Application Testing Suite	Load Testing for Web Apps (jQuery)	HTTP	Yes	6.1	Network	Low	None	
CVE-2019-10247	Enterprise Manager	Agent Next Gen (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
	Base Platform								

Additional CVEs addressed are below:

- The patch for CVE-2019-10247 also addresses CVE-2019-10246.
- The patch for CVE-2019-11358 also addresses CVE-2015-9251.
- The patch for CVE-2019-5443 also addresses CVE-2019-5435 and CVE-2019-5436.
- The patch for CVE-2019-9517 also addresses CVE-2019-10081, CVE-2019-10082, CVE-2019-10092, CVE-2019-10097 and CVE-2019-10098.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Financial Services Applications. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-14379	Oracle Banking Platform	Infrastructure (jackson-databind)	HTTP	Yes	9.8	Network	Low	Non
CVE-2019-14379	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (jackson-databind)	HTTP	Yes	9.8	Network	Low	Non
CVE-2019-2980	Oracle FLEXCUBE Direct Banking	eMail	HTTP	No	6.5	Network	Low	Lov
CVE-2019-11358	Oracle Financial Services Enterprise Financial	UI (jQuery)	HTTP	Yes	6.1	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Performance Analytics							
CVE-2019-11358	Oracle Financial Services Retail Performance Analytics	UI (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-2979	Oracle FLEXCUBE Direct Banking	Payments	HTTP	No	5.7	Network	Low	Lov
CVE-2019-3019	Oracle Banking Digital Experience	Loan Calculator	HTTP	No	5.4	Network	Low	Lov

Additional CVEs addressed are below:

- The patch for CVE-2019-14379 also addresses CVE-2019-14439.

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 7 new security patches 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-3025	Oracle Hospitality RES 3700	Interface	HTTP	Yes	9.0	Network	High	None
CVE-2019-2934	Oracle Hospitality Reporting and Analytics	Admin - Configuration	HTTP	No	8.1	Network	Low	Low

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-2019-2937	Oracle Hospitality Reporting and Analytics	Admin - Configuration	HTTP	No	8.1	Network	Low	Low
CVE-2019-2947	Oracle Hospitality Reporting and Analytics	Inventory Integration	HTTP	No	7.1	Network	Low	Low
CVE-2019-2936	Oracle Hospitality Reporting and Analytics	Admin - Configuration	HTTP	No	6.8	Network	High	Low
CVE-2019-11358	Oracle Hospitality Materials Control	Core (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2019-2952	Oracle Hospitality Reporting and Analytics	Admin- Configuration	HTTP	Yes	6.1	Network	Low	None

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 37 new security patches for Oracle Fusion Middleware. 31 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security updates are not listed in the Oracle Fusion Middleware risk matrix. However, since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the Critical Patch Update October 2019 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 October 2019 Patch Availability Document for Oracle Products, My Oracle Support Note 2568292.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2019-2904	Oracle JDeveloper and ADF	ADF Faces	HTTP	Yes	9.8	Network	Low	Non
CVE-2016-1000031	Oracle Virtual Directory	Virtual Directory Server (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	Non
CVE-2019-2905	Oracle Business Intelligence Enterprise Edition	Installation	HTTP	Yes	8.6	Network	Low	Non
CVE-2019-2906	BI Publisher (formerly XML Publisher)	Mobile Service	HTTP	Yes	8.2	Network	Low	Non
CVE-2019-2891	Oracle WebLogic Server	Console	HTTP	Yes	8.1	Network	High	Non
CVE-2019-2900	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-0188	Oracle Enterprise Repository	Security Subsystem - 12c (Apache Camel)	HTTP	Yes	7.5	Network	Low	Non
CVE-2017-12626	Oracle Enterprise Repository	Security Subsystem - 12c (Apache POI)	HTTP	Yes	7.5	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2018-15756	Oracle GoldenGate Application Adapters	3rd Party (Spring Framework)	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-12086	Oracle WebCenter Portal	Security Framework (jackson-databind)	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-2970	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2901	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2902	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2903	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2971	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2972	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	Non
CVE-2016-1000031	Oracle SOA Suite	BPEL Service Engine and Fabric Layer (Apache Commons FileUpload)	HTTP	Yes	7.3	Network	Low	Non
CVE-2019-2907	Oracle Web Services	SOAP with Attachments API for Java	HTTP	Yes	7.2	Network	Low	Non
CVE-2019-2890	Oracle WebLogic Server	Web Services	T3	No	7.2	Network	Low	Higl

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2019-2943	Oracle Data Integrator	Studio	HTTP	No	6.5	Network	Low	Low
CVE-2019-2897	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	No	6.4	Network	Low	Low
CVE-2016-7103	Oracle Business Intelligence Enterprise Edition	BI Platform Security (JQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-2886	Oracle Forms	Services	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-11358	Oracle JDeveloper and ADF	ADF Faces (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-11358	Oracle Service Bus	Web Container (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-11358	Oracle WebLogic Server	Console (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-2889	Oracle WebLogic Server	Sample apps	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-11358	Oracle WebLogic Server	Sample apps (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-17091	Oracle WebLogic Server	Web Container (JavaServer Faces)	HTTP	Yes	6.1	Network	Low	Non
CVE-2015-9251	Oracle WebLogic Server	Web Services (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-1559	Oracle API Gateway	Oracle API Gateway (OpenSSL)	HTTPS	Yes	5.9	Network	High	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2019-1559	Oracle Business Intelligence Enterprise Edition	Secure Store (OpenSSL)	HTTPS	Yes	5.9	Network	High	Non
CVE-2019-3012	Oracle Business Intelligence Enterprise Edition	BI Platform Security	HTTP	Yes	5.3	Network	Low	Non
CVE-2019-2888	Oracle WebLogic Server	EJB Container	HTTP	Yes	5.3	Network	Low	Non
CVE-2019-2898	BI Publisher (formerly XML Publisher)	BI Publisher Security	HTTP	No	4.3	Network	Low	Low
CVE-2019-2887	Oracle WebLogic Server	Web Services	HTTP	No	4.3	Network	Low	Low
CVE-2019-2899	Oracle JDeveloper and ADF	OAM	HTTP	No	2.4	Network	Low	Higl

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

Additional CVEs addressed are below:
- The patch for CVE-2016-7103 also addresses CVE-2015-9251.
- The patch for CVE-2019-11358 also addresses CVE-2015-9251.

Oracle GraalVM Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2019-2986	Oracle GraalVM Enterprise Edition	LLVM Interpreter	Multiple	No	7.7	Network	Low	Low	N
CVE-2019-9511	Oracle GraalVM Enterprise Edition	JavaScript (Node.js)	Multiple	Yes	7.5	Network	Low	None	N
CVE-2019-2989	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	6.8	Network	High	None	N

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Health Sciences 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-11358	Oracle Healthcare Foundation	Security (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2019-11358	Oracle Healthcare Translational Research	Cohort Explorer (jQuery)	HTTP	Yes	6.1	Network	Low	None

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Hospitality 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-0227	Oracle Hospitality Guest Access	Base (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	None
CVE-2019-2953	Oracle Hospitality Cruise Dining Room Management	Web Service	HTTP	No	7.1	Network	Low	Low
CVE-2019-10247	Oracle Hospitality Guest Access	Base (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	None

Additional CVEs addressed are below:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10247 also addresses CVE-2019-10246.

Oracle Hyperion Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2927	Hyperion Data Relationship Management	Access and Security	HTTP	No	6.4	Network	High	High
CVE-2019-2959	Hyperion Financial Reporting	Security Models	HTTP	No	4.2	Network	High	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2941	Hyperion Profitability and Cost Management	Modeling	HTTP	No	4.0	Network	High	High

Oracle Java SE Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2949	Java SE, Java SE Embedded	Kerberos	Kerberos	Yes	6.8	Network	High	None
CVE-2019-2989	Java SE, Java SE Embedded	Networking	Multiple	Yes	6.8	Network	High	None
CVE-2019-2958	Java SE, Java SE Embedded	Libraries	Multiple	Yes	5.9	Network	High	None
CVE-2019-11068	Java SE	JavaFX (libxslt)	Multiple	Yes	5.6	Network	High	None
CVE-2019-2977	Java SE	Hotspot	Multiple	Yes	4.8	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-2975	Java SE, Java SE Embedded	Scripting	Multiple	Yes	4.8	Network	High	None	
CVE-2019-2999	Java SE	Javadoc	Multiple	Yes	4.7	Network	High	None	F
CVE-2019-2996	Java SE, Java SE Embedded	Deployment	Multiple	Yes	4.2	Network	High	None	F
CVE-2019-2987	Java SE	2D	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2962	Java SE, Java SE Embedded	2D	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2988	Java SE, Java SE Embedded	2D	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2992	Java SE, Java SE Embedded	2D	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2964	Java SE, Java SE Embedded	Concurrency	Multiple	Yes	3.7	Network	High	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-2973	Java SE, Java SE Embedded	JAXP	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2981	Java SE, Java SE Embedded	JAXP	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2978	Java SE, Java SE Embedded	Networking	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2894	Java SE, Java SE Embedded	Security	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2983	Java SE, Java SE Embedded	Serialization	Multiple	Yes	3.7	Network	High	None	
CVE-2019-2933	Java SE, Java SE Embedded	Libraries	Multiple	Yes	3.1	Network	High	None	F

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-2945	Java SE, Java SE Embedded	Networking	Multiple	Yes	3.1	Network	High	None	F

Notes:

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

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

3. This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle JD Edwards. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2017-5645	JD Edwards EnterpriseOne	Deployment (Log4j)	HTTP	Yes	9.8	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	Tools							

Oracle MySQL Risk Matrix

This Critical Patch Update contains 34 new security patches for Oracle MySQL. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-8457	MySQL Workbench	MySQL Workbench (SQLite)	MySQL Workbench	Yes	9.8	Network	Low	
CVE-2019-5443	MySQL Server	Server: Compiling (cURL)	MySQL Protocol	No	7.8	Local	Low	
CVE-2019-10072	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	
CVE-2019-1543	MySQL Connectors	Connector/ODBC (OpenSSL)	TLS	Yes	7.4	Network	High	
CVE-2019-3011	MySQL Server	Server: C API	MySQL Protocol	No	6.5	Network	Low	
CVE-2019-2966	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	
CVE-2019-2967	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	
CVE-2019-2974	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-2946	MySQL Server	Server: PS	MySQL Protocol	No	6.5	Network	Low
CVE-2019-3004	MySQL Server	Server: Parser	MySQL Protocol	No	6.5	Network	Low
CVE-2019-2914	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	6.5	Network	Low
CVE-2019-2969	MySQL Server	Client programs	MySQL Protocol	No	6.2	Local	Low
CVE-2019-2991	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2019-2920	MySQL Connectors	Connector/ODBC	MySQL Protocol	Yes	5.3	Network	Low
CVE-2019-2993	MySQL Server	Server: C API	MySQL Protocol	No	5.3	Network	High
CVE-2019-2922	MySQL Server	Server: Security: Encryption	MySQL Protocol	Yes	5.3	Network	Low
CVE-2019-2923	MySQL Server	Server: Security: Encryption	MySQL Protocol	Yes	5.3	Network	Low
CVE-2019-2924	MySQL Server	Server: Security: Encryption	MySQL Protocol	Yes	5.3	Network	Low
CVE-2019-1549	MySQL Workbench	Workbench: Security:	MySQL Workbench	Yes	5.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
		Encryption (OpenSSL)					
CVE-2019-2963	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2968	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2019-3003	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2997	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2948	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2950	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2982	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2998	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2960	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2957	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	4.9	Network	Low
CVE-2019-2938	MySQL Server	InnoDB	MySQL Protocol	No	4.4	Network	High
CVE-2019-3018	MySQL Server	InnoDB	MySQL Protocol	No	4.4	Network	High
CVE-2019-3009	MySQL Server	Server: Connection	MySQL Protocol	No	4.4	Network	High
CVE-2019-2910	MySQL Server	Server: Security: Encryption	MySQL Protocol	Yes	3.7	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-2911	MySQL Server	Information Schema	MySQL Protocol	No	2.7	Network	Low

Additional CVEs addressed are below:

- The patch for CVE-2019-1549 also addresses CVE-2019-1547, CVE-2019-1552 and CVE-2019-1563.
- The patch for CVE-2019-5443 also addresses CVE-2019-5435 and CVE-2019-5436.
- The patch for CVE-2019-8457 also addresses CVE-2019-9936 and CVE-2019-9937.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 13 new security patches for Oracle PeopleSoft. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2016-0729	PeopleSoft Enterprise PeopleTools	Integration Broker (Apache Xerces)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-3862	PeopleSoft Enterprise PeopleTools	File Processing (libssh2)	HTTP	Yes	9.1	Network	Low	Nor
CVE-2019-2932	PeopleSoft Enterprise PeopleTools	Tree Manager	HTTP	No	7.7	Network	Low	Lo
CVE-2019-2915	PeopleSoft Enterprise PeopleTools	Fluid Core	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-2985	PeopleSoft Enterprise	Fluid Core	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
	PeopleTools							
CVE-2019-3014	PeopleSoft Enterprise PeopleTools	Performance Monitor	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-2929	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-2931	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-11358	PeopleSoft Enterprise PeopleTools	Portal, Charting (jQuery)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-3001	PeopleSoft Enterprise SCM eProcurement	eProcurement	HTTP	Yes	5.3	Network	Low	Nor
CVE-2019-3023	PeopleSoft Enterprise PeopleTools	Stylesheet	HTTP	Yes	4.7	Network	Low	Nor
CVE-2019-2951	PeopleSoft Enterprise HCM Human Resources	US Federal Specific	HTTP	No	4.3	Network	Low	Lo
CVE-2019-3015	PeopleSoft Enterprise PeopleTools	Integration Broker	HTTP	No	4.3	Network	Low	Lo

Additional CVEs addressed are below:

- The patch for CVE-2019-3862 also addresses CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861 and CVE-2019-3863.

Oracle Policy Automation Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-0227	Oracle Policy Automation Connector for Siebel	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Non
CVE-2019-11358	Oracle Policy Automation	Determinations Engine (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-11358	Oracle Policy Automation Connector for Siebel	Core (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-11358	Oracle Policy Automation for Mobile Devices	Core (jQuery)	HTTP	Yes	6.1	Network	Low	Non

Additional CVEs addressed are below:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Retail Applications. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2018-19362	MICROS Retail XBRi Loss Prevention	Retail (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-2019-14379	Oracle Retail Xstore Point of Service	Xenvironment (jackson-databind)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-0232	MICROS Relate CRM Software	Internal Operations (Apache Tomcat)	HTTP	Yes	8.1	Network	High	No
CVE-2018-15756	Oracle Retail Integration Bus	RIB Kernal (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-12086	Oracle Retail Xstore Point of Service	Xenvironment (jackson-databind)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-11358	Oracle Retail Customer Insights	Retail Science Engine (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2019-2896	MICROS Relate CRM Software	Internal Operations	HTTP	Yes	5.9	Network	High	No
CVE-2019-2884	Oracle Retail Customer Management and Segmentation Foundation	Segment	HTTP	Yes	5.9	Network	High	No
CVE-2018-3300	Oracle Retail Xstore Office	Internal Operations	HTTP	No	5.4	Network	Low	Lo
CVE-2019-10247	Oracle Retail Xstore Point of Service	Dataloader (jackson-databind)	HTTP	Yes	5.3	Network	Low	No
CVE-2019-2883	Oracle Retail Customer Management and Segmentation Foundation	Segment	HTTP	No	4.6	Network	Low	Lo
CVE-2019-2872	Oracle Retail Xstore Point	Point of Sale	None	No	2.7	Physical	High	Hi

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

Additional CVEs addressed are below:

- The patch for CVE-2019-10247 also addresses CVE-2017-7656, CVE-2017-7657, CVE-2017-7658, CVE-2017-9735, CVE-2018-12536, CVE-2018-12538, CVE-2018-12545, CVE-2019-10241 and CVE-2019-10246.
- The patch for CVE-2019-14379 also addresses CVE-2019-12086 and CVE-2019-14439.

Oracle Siebel CRM Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-2965	Siebel Core - DB Deployment and Configuration	Install - Configuration	HTTP	Yes	7.5	Network	Low	
CVE-2019-11358	Siebel Mobile Applications	CG Mobile Connected (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2018-8037	Siebel UI Framework	Customizable Prod/Configurator (Apache Tomcat)	HTTP	Yes	5.9	Network	High	
CVE-2019-2935	Siebel UI Framework	EAI	HTTP	Yes	5.3	Network	Low	

Oracle Systems Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Systems . 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2018-1000007	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (cURL)	Multiple	Yes	9.8	Network	Low	None
CVE-2019-3010	Oracle Solaris	XScreenSaver	None	No	8.8	Local	Low	Low
CVE-2015-5180	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (glibc)	Multiple	Yes	7.5	Network	Low	None
CVE-2018-7185	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (NTP)	NTP	Yes	7.5	Network	Low	None
CVE-2018-18066	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (Net SNMP)	SNMP	Yes	7.5	Network	Low	None
CVE-2018-0732	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (OpenSSL)	TLS	Yes	7.5	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-6109	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (OpenSSH)	SSH	Yes	6.8	Network	High	None
CVE-2017-17558	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (USB Driver)	None	No	6.6	Physical	Low	Low
CVE-2018-12404	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (NSS)	TLS	Yes	5.9	Network	High	None
CVE-2019-2765	Oracle Solaris	Filesystem	None	No	5.3	Local	High	Low
CVE-2019-2961	Oracle Solaris	SMF services & legacy daemons	None	No	3.6	Local	High	Low
CVE-2019-3008	Oracle Solaris	LDAP Library	None	No	1.8	Local	High	High

Additional CVEs addressed are below:

- The patch for CVE-2017-17558 also addresses CVE-2017-16531.
- The patch for CVE-2018-0732 also addresses CVE-2016-8610 and CVE-2019-1559.
- The patch for CVE-2018-1000007 also addresses CVE-2018-1000120 and CVE-2018-16842.
- The patch for CVE-2018-12404 also addresses CVE-2018-12384.
- The patch for CVE-2018-18066 also addresses CVE-2018-18065.
- The patch for CVE-2019-6109 also addresses CVE-2018-20685 and CVE-2019-6111.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Supply Chain. 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 Req
CVE-2016-6814	Agile Recipe Management for Pharmaceuticals	Recipe (Apache Groovy)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-0232	Oracle Agile PLM	Security (Apache Tomcat)	HTTP	Yes	8.1	Network	High	No
CVE-2019-11358	Oracle Agile Product Lifecycle Management for Process	Supplier Portal (jQuery)	HTTP	Yes	6.1	Network	Low	No

Oracle Support Tools Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Support Tools. 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 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-11358	Diagnostic Assistant	Libraries (jQuery)	HTTP	Yes	6.1	Network	Low	None	
CVE-2019-12814	Oracle Clusterware	Trace File Analyzer (TFA) Collector (jackson-databind)	HTTP	Yes	5.9	Network	High	None	

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle Virtualization. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Inte
CVE-2019-3028	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	No
CVE-2019-3017	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	No
CVE-2019-2944	Oracle VM VirtualBox	Core	None	No	7.3	Local	Low	High	No
CVE-2019-3026	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	No
CVE-2019-3021	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	No
CVE-2019-2984	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	No
CVE-2019-3002	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	No
CVE-2019-3005	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2019-3031	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	No
CVE-2019-1547	Oracle VM VirtualBox	Core (OpenSSL)	None	No	4.7	Local	High	Low	No
CVE-2019-2926	Oracle VM VirtualBox	Core	None	No	2.3	Local	Low	High	No

Additional CVEs addressed are below:

- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.

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