Oracle Critical Patch Update Advisory - January 2020

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 334 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 January 2020 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, 13.2.0.0, 13.3.0.0	Enterprise Manager
Enterprise Manager for Fusion Middleware, versions 13.2.0.0, 13.3.0.0	Enterprise Manager

Affected Products and Versions	Patch Availability Document
Enterprise Manager for Oracle Database, versions 12.1.0.5, 13.2.0.0, 13.3.0.0	Enterprise Manager
Enterprise Manager Ops Center, versions 12.3.3, 12.4.0	Enterprise Manager
Hyperion Financial Close Management, version 11.1.2.4	Fusion Middleware
Hyperion Planning, version 11.1.2.4	Fusion Middleware
Identity Manager, versions 11.1.2.3.0, 12.2.1.3.0	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineering Suite
JD Edwards EnterpriseOne Orchestrator, version 9.2	JD Edwards
JD Edwards EnterpriseOne Tools, version 9.2	JD Edwards
MySQL Client, versions 5.6.46 and prior, 5.7.28 and prior, 8.0.18 and prior	MySQL
MySQL Cluster, versions 7.3.27 and prior, 7.4.25 and prior, 7.5.15 and prior, 7.6.12 and prior	MySQL
MySQL Connectors, versions 5.3.13 and prior, 8.0.18 and prior	MySQL
MySQL Enterprise Backup, versions 3.12.4 and prior, 4.1.3 and prior	MySQL
MySQL Server, versions 5.6.46 and prior, 5.7.28 and prior, 8.0.18 and prior	MySQL
MySQL Workbench, versions 8.0.18 and prior	MySQL
Oracle Agile Engineering Data Management, versions 6.2.0, 6.2.1	Oracle Supply Chain Products
Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5, 9.3.6	Oracle Supply Chain Products
Oracle Agile PLM Framework, version 9.3.3	Oracle Supply Chain Products
Oracle Agile PLM MCAD Connector, versions 3.4, 3.5, 3.6	Oracle Supply Chain Products
Oracle Application Testing Suite, versions 12.5.0.3, 13.1.0.1, 13.2.0.1, 13.3.0.1	Enterprise Manager
Oracle AutoVue, version 21.0.2	Oracle Supply Chain Products
Oracle Banking Corporate Lending, versions 12.3.0-12.4.0, 14.0.0-14.3.0	Oracle Financial Services Applications
Oracle Banking Payments, versions 14.1.0-14.3.0	Oracle Financial Services Applications
Oracle Big Data Discovery, version 1.6	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Clinical, version 5.2	Health Sciences
Oracle Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Communications Design Studio, versions 7.3.4.3.0, 7.3.5.5.0, 7.4.0.4.0, 7.4.1.1.0	Oracle Communications Desig Studio
Oracle Communications Diameter Signaling Router (DSR), versions 8.0, 8.1, 8.2, 8.3, 8.4	Oracle Communications Diame Signaling Router
Oracle Communications Instant Messaging Server, version 10.0.1.3.0	Oracle Communications Instan Messaging Server
Oracle Communications Interactive Session Recorder, versions 6.0, 6.1, 6.2, 6.3	Oracle Communications Interactive Session Recorder
Oracle Communications IP Service Activator, versions 7.3.4, 7.4.0	Oracle Communications IP Ser Activator
Oracle Communications Session Border Controller, versions 7.4, 8.0, 8.1, 8.2, 8.3	Oracle Communications Sessic Border Controller
Oracle Communications Session Router, versions 7.4, 8.0, 8.1, 8.2, 8.3	Oracle Communications Sessic Router
Oracle Communications Subscriber-Aware Load Balancer, versions 7.3, 8.1, 8.3	Oracle Communications Subscriber-Aware Load Balanc
Oracle Communications Unified Inventory Management, versions 7.3, 7.4	Oracle Communications Unifie Inventory Management
Oracle Communications Unified Session Manager, versions 7.3.5, 8.2.5	Oracle Communications Unifie Session Manager
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c	Database
Oracle Demantra Demand Management, versions 12.2.4, 12.2.4.1, 12.2.5, 12.2.5.1	Oracle Supply Chain Products
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.9	E-Business Suite
Oracle Endeca Information Discovery Integrator, version 3.2.0	Fusion Middleware
Oracle Endeca Information Discovery Studio, version 3.2.0	Fusion Middleware
Oracle Enterprise Communications Broker, versions PCz3.0, PCz3.1, PCz3.2	Oracle Enterprise Communications Broker
Oracle Enterprise Repository, version 12.1.3.0.0	Fusion Middleware
Oracle Enterprise Session Border Controller, versions 7.5, 8.0, 8.1, 8.2, 8.3	Oracle Enterprise Session Bord Controller
Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3-7.3.5, 8.0.0-8.0.8	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Funds Transfer Pricing, versions 8.0.2-8.0.7	Oracle Financial Services Fund Transfer Pricing
Oracle Financial Services Revenue Management and Billing, versions 2.7.0.0, 2.7.0.1, 2.8.0.0	Oracle Financial Services Reve Management and Billing

Affected Products and Versions	Patch Availability Document
Oracle FLEXCUBE Investor Servicing, versions 12.1.0-12.4.0, 14.0.0-14.1.0	Oracle Financial Services Applications
Oracle FLEXCUBE Universal Banking, versions 12.0.1-12.4.0, 14.0.0-14.3.0	Oracle Financial Services Applications
Oracle GraalVM Enterprise Edition, version 19.3.0.2	Oracle GraalVM Enterprise Edit
Oracle Health Sciences Data Management Workbench, versions 2.4, 2.5	Health Sciences
Oracle Healthcare Master Person Index, version 3.0	Health Sciences
Oracle Hospitality Cruise Materials Management, version 7.30.567	Oracle Hospitality Cruise Mater Management
Oracle Hospitality Guest Access, version 4.2	Oracle Hospitality Guest Acces
Oracle Hospitality OPERA 5, versions 5.5, 5.6	Oracle Hospitality OPERA 5 Property Services
Oracle Hospitality Suites Management, versions 3.7, 3.8	Oracle Hospitality Suites Management
Oracle HTTP Server, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle iLearning, version 6.1	iLearning
Oracle Java SE, versions 7u241, 8u231, 11.0.5, 13.0.1	Java SE
Oracle Java SE Embedded, version 8u231	Java SE
Oracle Outside In Technology, version 8.5.4	Fusion Middleware
Oracle Real-Time Scheduler, versions 2.3.0.1-2.3.0.3	Oracle Utilities Applications
Oracle Reports Developer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Retail Assortment Planning, versions 15.0.3, 16.0.3	Retail Applications
Oracle Retail Clearance Optimization Engine, versions 13.4, 14.0, 14.0.3, 14.0.5	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0	Retail Applications
Oracle Retail Markdown Optimization, versions 13.4, 13.4.4	Retail Applications
Oracle Retail Order Broker, versions 5.2, 15.0, 16.0, 18.0	Retail Applications
Oracle Retail Predictive Application Server, versions 15.0.3, 16.0.3	Retail Applications
Oracle Retail Sales Audit, version 15.0.3.16.0.2	Retail Applications
Oracle Secure Global Desktop, versions 5.4, 5.5	Virtualization
Oracle Security Service, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0	Fusion Middleware
Oracle Solaris, versions 10, 11	Systems

Affected Products and Versions	Patch Availability Document
Oracle Tuxedo, versions 12.1.1.0.0, 12.1.3.0.0	Fusion Middleware
Oracle Utilities Framework, versions 4.2.0.2-4.2.0.3, 4.3.0.1-4.3.0.4	Oracle Utilities Applications
Oracle Utilities Mobile Workforce Management, versions 2.3.0.1-2.3.0.3	Oracle Utilities Applications
Oracle Utilities Work and Asset Management (v1), version 1.9.1.2	Oracle Utilities Applications
Oracle VM Server for SPARC, version 3.6	Systems
Oracle VM VirtualBox, versions prior to 5.2.36, prior to 6.0.16, prior to 6.1.2	Virtualization
Oracle WebCenter Sites, version 12.2.1.3.0	Fusion Middleware
Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
PeopleSoft Enterprise CC Common Application Objects, versions 9.1, 9.2	PeopleSoft
PeopleSoft Enterprise HCM Human Resources, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft
PeopleSoft PeopleTools, versions 8.56, 8.57	PeopleSoft
Primavera Gateway, versions 15.2.18, 16.2.11, 17.12.6, 18.8.8.1	Oracle Construction and Engineering Suite
Primavera P6 Enterprise Project Portfolio Management, versions 15.1.0.0-15.2.18.7, 16.1.0.0-16.2.19.0, 17.1.0.0-17.12.16.0, 18.1.0.0-18.8.16.0, 19.12.0.0, 20.1.0.0	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12	Oracle Construction and Engineering Suite
Siebel Applications, versions 19.10 and prior	Siebel
Sun ZFS Storage Appliance Kit, version 8.8.6	Systems
Tape Library ACSLS, versions 8.5, 8.5.1	Systems

Note:

- Vulnerabilities affecting either Oracle Database or 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:

- Add of STAR labs: CVE-2020-2674
- Afanti of North China Electric Power University: CVE-2020-2550
- Alexander Kornbrust of Red Database Security: CVE-2020-2511, CVE-2020-2516, CVE-2020-2527, CVE-2020-2572, CVE-2020-2608, CVE-2020-2609, CVE-2020-2610, CVE-2020-2611, CVE-2020-2612, CVE-2020-2613, CVE-2020-2614, CVE-2020-2615, CVE-2020-2616, CVE-2020-2617, CVE-2020-2618, CVE-2020-2619, CVE-2020-2620, CVE-2020-2621, CVE-2020-2622, CVE-2020-2623, CVE-2020-2624, CVE-2020-2625, CVE-2020-2626, CVE-2020-2628, CVE-2020-2629, CVE-2020-2630, CVE-2020-2631, CVE-2020-2632, CVE-2020-2633, CVE-2020-2634, CVE-2020-2635, CVE-2020-2636, CVE-2020-2637, CVE-2020-2638, CVE-2020-

2639, CVE-2020-2640, CVE-2020-2641, CVE-2020-2642, CVE-2020-2643, CVE-2020-2644, CVE-2020-2645

- ALVES Christopher: CVE-2020-2570, CVE-2020-2573, CVE-2020-2574
- An Trinh: CVE-2020-6950
- Andrej Simko of Accenture: CVE-2020-2582, CVE-2020-2596, CVE-2020-2597, CVE-2020-2657, CVE-2020-2658, CVE-2020-2661, CVE-2020-2662, CVE-2020-2665, CVE-2020-2667, CVE-2020-2668, CVE-2020-2669, CVE-2020-2670, CVE-2020-2671, CVE-2020-2672
- Andres Georgieff of Sandia National Laboratories: CVE-2020-2561
- André Lenoir of Tehtris: CVE-2020-2651, CVE-2020-2652, CVE-2020-2653
- anhdaden of StarLabs working with Trend Micro's Zero Day Initiative: CVE-2020-2682
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2020-2698, CVE-2020-2701, CVE-2020-2726, CVE-2020-2727
- Bengt Jonsson of Uppsala University: CVE-2020-2655
- Bo Zhang: CVE-2020-2654
- Daniel Le Souef of Trustwave Hivint: CVE-2020-2675, CVE-2020-2676, CVE-2020-2677
- Daniel Martinez Adan (aDoN90): CVE-2020-2538, CVE-2020-2539
- Davide Berardi: CVE-2020-2703
- Devin Rosenbauer of Identity Works LLC: CVE-2020-2729
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2020-2568, CVE-2020-2569, CVE-2020-2731
- Ehsan Nikavar: CVE-2020-2531
- elasticheart from ICC working with Trend Micro Zero Day Initiative: CVE-2020-2681, CVE-2020-2689, CVE-2020-2690, CVE-2020-2691, CVE-2020-2692, CVE-2020-2704, CVE-2020-2705
- Giuseppino Cadeddu of Quantum Leap: CVE-2020-2599
- Harold Zang of Trustwave Hivint: CVE-2020-2675, CVE-2020-2676, CVE-2020-2677
- Harrison Neal: CVE-2020-2510, CVE-2020-2512, CVE-2020-2515, CVE-2020-2517
- Instructor working with Trend Micro Zero Day Initiative: CVE-2020-2693
- Janatildrissi Zouhair: CVE-2020-2570, CVE-2020-2573, CVE-2020-2574
- Jang from VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2020-2555
- Jonas Mattsson of Outpost24 Ghost Labs: CVE-2020-2533, CVE-2020-2534
- Juraj Somorovsky of Ruhr-University Bochum: CVE-2020-2655
- Kasper Leigh Haabb, Secunia Research at Flexera: CVE-2020-2540, CVE-2020-2541, CVE-2020-2542, CVE-2020-2543, CVE-2020-2576
- Kirtikumar Anandrao Ramchandani: CVE-2020-2545

- Kostis Sagonas of Uppsala University: CVE-2020-2655
- Kylinking of NSFocus Security Team: CVE-2020-2551
- Long Kuan: CVE-2020-2654
- Looke of PingAn Galaxy Lab: CVE-2020-2547, CVE-2020-2548, CVE-2020-2549, CVE-2020-2552
- Lucas Leong of Trend Micro Zero Day Initiative: CVE-2020-2702
- Lukasz Mikula: CVE-2020-2563
- Lukasz Plonka of ING Tech Poland: CVE-2020-2663
- Lukasz Rupala of ING Tech Poland: CVE-2020-2663
- Marco Ivaldi of Media Service: CVE-2020-2656, CVE-2020-2696
- Martin Doyhenard of Onapsis: CVE-2020-2586, CVE-2020-2587
- Matthias Kaiser of Apple Information Security: CVE-2020-2546
- Michal Skowron: CVE-2020-2537
- Microsoft Vulnerability Research of Microsoft Corp.: CVE-2020-2536
- Mohammad Sedghi: CVE-2020-2535
- Nicolas Verdier of Tehtris: CVE-2020-2651, CVE-2020-2652, CVE-2020-2653
- Or Hanuka of Motorola Solutions: CVE-2020-2557
- Owais Zaman of Sabic: CVE-2020-2592, CVE-2020-2707
- Paul Fiterau Brostean of Uppsala University: CVE-2020-2655
- Philippe Antoine, Christopher Alves, Zouhair Janatil-Idrissi, Julien Zhan (Telecom Nancy): CVE-2020-2570, CVE-2020-2573, CVE-2020-2574
- RACV Information Security Team: CVE-2020-2675, CVE-2020-2676, CVE-2020-2677
- Reno Robert: CVE-2020-2698
- Robert Merget of Ruhr-University Bochum: CVE-2020-2655
- Rémi Badonnel: CVE-2020-2570, CVE-2020-2573, CVE-2020-2574
- Sravya Nandimandalam: CVE-2020-2519
- Stefano Ciccone of Aon's Cyber Labs: CVE-2020-2551
- Tom Tran: CVE-2020-2559, CVE-2020-2728
- Tomasz Wisniewski: CVE-2020-2688
- Tzachy Horesh (Motorola Solutions) of Motorola Solutions: CVE-2020-2557
- Vivek Parikh: CVE-2020-2678
- ZHAN Julien: CVE-2020-2570, CVE-2020-2573, CVE-2020-2574
- Zhongcheng Li (CK01) of Topsec Alpha Team: CVE-2020-2725

- Zohaib Tasneem of Sabic: CVE-2020-2707

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.:

- An Trinh
- Andres Georgieff of Sandia National Laboratories
- Benjamin Horvat of Cologne-Intelligence
- Josh Bressers of Elastic
- Marek Cybul
- Markus Loewe
- Martin Doyhenard of Onapsis
- Matias Mevied of Onapsis
- Quentin Rhoads-Herrera of Critical Start
- Tolga Han Jonas Özgan of Cologne-Intelligence
- Vahagn Vardanyan
- Vladimir Egorov

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:

- Aditya Shende
- Ahmet Gürel
- Andy Bentley

- Apoorv Raj Saxena of FireCompass
- Arcot Manju
- Hardikkumar Patel
- Jimmy Bruneel
- Joby Y Daniel
- Lutfu Mert Ceylan
- Mohamed Yaser
- Mohammed Rafi
- Pankaj Kumar Thakur (Nepal)
- Roger Meyer
- Sai Kiran Battaluri
- Saiteja Pinoju
- Zeel D. Chavda

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 April 2020
- 14 July 2020
- 20 October 2020
- 19 January 2021

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - January 2020 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
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2020-April-20	Rev 7. Updated affected versions associated with CVE-2020-2555.
2020-March-11	Rev 6. Updated affected versions of Oracle AutoVue associated with CVE-2019-10247 a CVE-2020-2592. Updated affected versions associated with CVE-2020-2569.
2020-March-5	Rev 5. Updated affected versions associated with CVE-2020-2517.
2020-January-23	Rev 4. Updated affected versions associated with CVE-2020-2555 and modified credit entries for CVE-2020-2551, CVE-2020-2559 and CVE-2020-2663.
2020-January-17	Rev 3. Updated MOS note number for Oracle Communications Session Border Controll
2020-January-15	Rev 2. JavaSE and Database Versions Updated.
2020-January-14	Rev 1. Initial Release.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 12 new security patches for the Oracle Database Server. 3 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.

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-2020-2511	Core RDBMS	Create Session	OracleNet	No	7.7	Network	Low	Low
CVE-2020-2510	Core RDBMS	None	OracleNet	Yes	7.5	Network	High	None

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-2020-2518	Java VM	Create Session	Multiple	No	7.5	Network	High	Low
CVE-2019-10072	Workload Manager (Apache Tomcat)	None	HTTP	Yes	7.5	Network	Low	None
CVE-2020-2512	Database Gateway for ODBC	None	OracleNet	Yes	5.9	Network	High	None
CVE-2020-2515	Database Gateway for ODBC	Create Session	OracleNet	No	5.0	Network	High	Low
CVE-2020-2527	Core RDBMS	Create Index, Create Table	OracleNet	No	4.1	Network	Low	High
CVE-2020-2731	Core RDBMS	Local Logon	Local Logon	No	3.9	Local	Low	Low
CVE-2020-2568	Oracle Applications DBA	Local Logon	Local Logon	No	3.9	Local	Low	Low
CVE-2020-2569	Oracle Applications DBA	Local Logon	Local Logon	No	3.9	Local	Low	Low
CVE-2020-2517	Database Gateway for ODBC	Create Procedure, Create Database Link	OracleNet	No	3.3	Network	High	High
CVE-2020-2516	Core RDBMS	Create Materialized View, Create Table	OracleNet	No	2.4	Network	Low	High

Notes:

1. This patch also addresses four additional vulnerabilities: CVE-2018-11784, CVE-2019-0199, CVE-2019-0221 and CVE-2019-0232. For Windows platform - due to CVE-2019-0232 - the CVSS 3.0 score is 8.1.

Additional CVEs addressed are below:

- The patch for CVE-2019-10072 also addresses CVE-2018-11784, CVE-2019-0199, CVE-2019-0221 and CVE-2019-0232.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 25 new security patches for Oracle Communications Applications. 23 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 VERSI		
					Base Score	Attack Vector	Attacl Compl
CVE-2019-14379	Oracle Communications Instant Messaging Server	Presence-api (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2017-5645	Oracle Communications Instant Messaging Server	Core (Log4j)	XMPP	Yes	9.8	Network	Low
CVE-2018-16395	Oracle Communications Interactive Session Recorder	Security (Ruby)	TLS	Yes	9.8	Network	Low
CVE-2018-11058	Oracle Communications IP Service Activator	Database Client (NZ)	TCPS/HTTPS	Yes	9.8	Network	Low
CVE-2019-8457	Oracle Communications Unified Inventory Management	Tools (SQLite)	HTTP	Yes	9.8	Network	Low
CVE-2019-3862	Oracle Communications	Platform (libssh2)	SSH	Yes	9.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attacl Compl
	Diameter Signaling Router (DSR)						
CVE-2019-0227	Oracle Communications Design Studio	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-16168	Oracle Communications Design Studio	Core (SQLite)	HTTP	Yes	7.5	Network	Low
CVE-2019-10072	Oracle Communications Instant Messaging Server	Core (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2018-6829	Oracle Communications Interactive Session Recorder	General (libgcrypt)	HTTP	Yes	7.5	Network	Low
CVE-2019-11477	Oracle Communications Session Border Controller	Security (Kernel)	TCP	Yes	7.5	Network	Low
CVE-2019-11477	Oracle Communications Session Router	Security (Kernel)	TCP	Yes	7.5	Network	Low
CVE-2019-11477	Oracle Communications Subscriber-Aware Load Balancer	IP Stack (Kernel)	TCP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Communications Unified Inventory Management	Security (Spring Framework)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attacl Compl
CVE-2019-11477	Oracle Enterprise Communications Broker	IP Stack (Kernel)	TCP	Yes	7.5	Network	Low
CVE-2019-11477	Oracle Enterprise Session Border Controller	Security (Kernel)	TCP	Yes	7.5	Network	Low
CVE-2019-11358	Oracle Communications Interactive Session Recorder	General (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-17091	Oracle Communications Unified Inventory Management	Maps (Mojarra)	HTTP	Yes	6.1	Network	Low
CVE-2019-11358	Oracle Communications Unified Inventory Management	Maps (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-1559	Oracle Communications Diameter Signaling Router (DSR)	Platform (OpenSSL)	TLS	Yes	5.9	Network	High
CVE-2019-1559	Oracle Communications Session Border Controller	Security (OpenSSL)	TLS	Yes	5.9	Network	High
CVE-2019-1559	Oracle Communications Session Router	Security (OpenSSL)	TLS	Yes	5.9	Network	High
CVE-2019-1559	Oracle Communications Unified Session Manager	Routing (OpenSSL)	TLS	Yes	5.9	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attacl Compl
CVE-2018-0734	Oracle Enterprise Communications Broker	Security (OpenSSL)	None	No	5.1	Local	High
CVE-2018-0734	Oracle Enterprise Session Border Controller	Security (OpenSSL)	None	No	5.1	Local	High

Additional CVEs addressed are below:

- The patch for CVE-2018-0734 also addresses CVE-2018-0735, CVE-2018-5407, CVE-2019-1547 and CVE-2019-1559.
- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10072 also addresses CVE-2018-11784 and CVE-2019-0232.
- The patch for CVE-2019-11477 also addresses CVE-2019-11478 and CVE-2019-11479.
- The patch for CVE-2019-14379 also addresses CVE-2018-14718, CVE-2018-19362, CVE-2019-12086 and CVE-2019-14439.
- The patch for CVE-2019-1559 also addresses CVE-2018-0734.
- The patch for CVE-2019-16168 also addresses CVE-2019-8457, CVE-2019-9936 and CVE-2019-9937.
- The patch for CVE-2019-8457 also addresses CVE-2019-9936 and CVE-2019-9937.

Oracle Construction and Engineering Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-14540	Primavera Gateway	Admin (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-14540	Primavera Unifier	Core (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10088	Primavera Unifier	Core (Apache Tika)	HTTP	Yes	8.8	Network	Low	N
CVE-2019-0227	Primavera Gateway	Provider (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	N
CVE-2019-0227	Primavera Unifier	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	N
CVE-2020-2556	Primavera P6 Enterprise Project Portfolio Management	Core	None	No	7.3	Local	Low	L
CVE-2012-1695	Instantis EnterpriseTrack	Mobile (Mobile Application Framework)	HTTP	Yes	6.8	Network	High	N
CVE-2019-11358	Primavera Gateway	UI (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-17091	Primavera P6 Enterprise Project Portfolio Management	Web Access (Mojarra)	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-12415	Primavera Gateway	Admin (Apache POI)	None	No	5.5	Local	Low	L
CVE-2019-12415	Primavera Unifier	Core (Apache POI)	None	No	5.5	Local	Low	L
CVE-2020-2707	Primavera P6 Enterprise Project Portfolio Management	WebAccess	HTTP	No	5.4	Network	Low	L

Notes:
1. JRockit is removed.

Additional CVEs addressed are below:
- The patch for CVE-2012-1695 also addresses CVE-2012-3135.
- The patch for CVE-2019-0227 also addresses CVE-2014-3596 and CVE-2018-8032.
- The patch for CVE-2019-10088 also addresses CVE-2019-10093 and CVE-2019-10094.
- The patch for CVE-2019-11358 also addresses CVE-2015-9251.
- The patch for CVE-2019-14540 also addresses CVE-2019-16335.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 23 new security patches for the Oracle E-Business Suite. 21 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

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 January 2020 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 2020), My Oracle Support Note 2613782.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2586	Oracle Human Resources	Hierarchy Diagrammers	HTTPS	No	9.9	Network	Low	Low
CVE-2020-2587	Oracle Human Resources	Hierarchy Diagrammers	HTTPS	No	9.9	Network	Low	Low
CVE-2020-2651	Oracle CRM Technical Foundation	Preferences	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2652	Oracle CRM Technical Foundation	Preferences	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2653	Oracle CRM Technical Foundation	Preferences	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2669	Oracle Email Center	Message Display	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2670	Oracle Email Center	Message Display	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2671	Oracle Email Center	Message Display	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2672	Oracle Email Center	Message Display	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2582	Oracle iStore	Shopping Cart	HTTPS	Yes	8.2	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-2020-2658	Oracle iSupport	Others	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2661	Oracle iSupport	Others	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2662	Oracle iSupport	Others	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2665	Oracle iSupport	Others	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2591	Oracle Web Applications Desktop Integrator	Application Service	HTTPS	Yes	8.2	Network	Low	None
CVE-2020-2603	Oracle Field Service	Wireless	HTTPS	Yes	6.1	Network	Low	None
CVE-2020-2666	Oracle Applications Framework	Attachments / File Upload	HTTPS	Yes	5.3	Network	Low	None
CVE-2020-2566	Oracle Applications Framework	Attachments / File Upload	HTTPS	Yes	4.7	Network	Low	None
CVE-2020-2596	Oracle CRM Technical Foundation	Message Hooks	HTTPS	Yes	4.7	Network	Low	None
CVE-2020-2657	Oracle CRM Technical Foundation	Preferences	HTTPS	Yes	4.7	Network	Low	None
CVE-2020-2667	Oracle iSupport	Others	HTTPS	Yes	4.7	Network	Low	None
CVE-2020-2668	Oracle iSupport	Others	HTTPS	Yes	4.7	Network	Low	None
CVE-2020-2597	Oracle One-to-One	Call Phone Number	HTTPS	Yes	4.7	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
	Fulfillment	Page						

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 50 new security patches for Oracle Enterprise Manager. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these 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 January 2020 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 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2602410.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2018-11058	Enterprise Manager Ops Center	Networking (Oracle Security Service)	HTTPS	Yes	9.8	Network	Low	None
CVE-2019-5482	Enterprise Manager Ops Center	Networking (cURL)	Multiple	Yes	9.8	Network	Low	None
CVE-2019-2904	Oracle Application Testing Suite	Load Testing for Web Apps (Application Development Framework)	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-2016-4000	Oracle Application Testing Suite	Oracle Flow Builder (Jython)	HTTP	Yes	9.8	Network	Low	None
CVE-2017-12626	Oracle Application Testing Suite	Load Testing for Web Apps (Apache POI)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-2673	Oracle Application Testing Suite	Oracle Flow Builder	HTTP	Yes	7.5	Network	Low	None
CVE-2017-12626	Oracle Application Testing Suite	Oracle Flow Builder (Apache POI)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-11358	Oracle Application Testing Suite	Oracle Flow Builder (jQuery)	HTTP	Yes	7.2	Network	Low	None
CVE-2020-2609	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.3	Network	Low	Low
CVE-2017-14735	Oracle Application Testing Suite	Load Testing for Web Apps (AntiSamy)	HTTP	Yes	6.1	Network	Low	None
CVE-2017-14735	Oracle Application Testing Suite	Oracle Flow Builder (Antisamy)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-2631	Enterprise Manager Base Platform	Application Service Level Mgmt	HTTP	No	6.0	Network	Low	High
CVE-2020-2636	Enterprise Manager Base Platform	Application Service Level Mgmt	HTTP	No	6.0	Network	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2626	Enterprise Manager Base Platform	Cloud Control Manager - OMS	HTTP	No	6.0	Network	Low	High
CVE-2020-2634	Enterprise Manager Base Platform	Configuration Standard Framewk	HTTP	No	6.0	Network	Low	High
CVE-2020-2624	Enterprise Manager Base Platform	Connector Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2633	Enterprise Manager Base Platform	Connector Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2642	Enterprise Manager Base Platform	Connector Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2645	Enterprise Manager Base Platform	Connector Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2617	Enterprise Manager Base Platform	Discovery Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2610	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2611	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2612	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2618	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2619	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2620	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2621	Enterprise Manager Base Platform	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2616	Enterprise Manager Base Platform	Enterprise Manager Repository	HTTP	No	6.0	Network	Low	High
CVE-2020-2622	Enterprise Manager Base Platform	Event Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2629	Enterprise Manager Base Platform	Extensibility Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2630	Enterprise Manager Base Platform	Extensibility Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2613	Enterprise Manager Base Platform	Global EM Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2628	Enterprise Manager Base Platform	Host Management	HTTP	No	6.0	Network	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2639	Enterprise Manager Base Platform	Host Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2625	Enterprise Manager Base Platform	Job System	HTTP	No	6.0	Network	Low	High
CVE-2020-2643	Enterprise Manager Base Platform	Job System	HTTP	No	6.0	Network	Low	High
CVE-2020-2623	Enterprise Manager Base Platform	Metrics Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2615	Enterprise Manager Base Platform	Oracle Management Service	HTTP	No	6.0	Network	Low	High
CVE-2020-2644	Enterprise Manager Base Platform	Oracle Management Service	HTTP	No	6.0	Network	Low	High
CVE-2020-2608	Enterprise Manager Base Platform	Repository	HTTP	No	6.0	Network	Low	High
CVE-2020-2632	Enterprise Manager Base Platform	System Monitoring	HTTP	No	6.0	Network	Low	High
CVE-2020-2635	Enterprise Manager Base Platform	System Monitoring	HTTP	No	6.0	Network	Low	High
CVE-2020-2614	Enterprise Manager for Fusion Middleware	APM Mesh	HTTP	No	6.0	Network	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2637	Enterprise Manager for Oracle Database	Change Manager - web based	HTTP	No	6.0	Network	Low	High
CVE-2020-2641	Enterprise Manager for Oracle Database	Discovery Framework	HTTP	No	6.0	Network	Low	High
CVE-2020-2638	Enterprise Manager for Oracle Database	Enterprise Config Management	HTTP	No	6.0	Network	Low	High
CVE-2020-2640	Enterprise Manager for Oracle Database	Target Management	HTTP	No	6.0	Network	Low	High
CVE-2019-12415	Oracle Application Testing Suite	Load Testing for Web Apps (Apache POI)	none	No	5.5	Local	Low	Low
CVE-2020-2646	Enterprise Manager Base Platform	Command Line Interface	HTTP	No	5.4	Network	Low	Low
CVE-2019-1547	Enterprise Manager Ops Center	Networking (RSA Bsafe)	None	No	4.7	Local	High	Low

Additional CVEs addressed are below:

- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.
- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.
- The patch for CVE-2019-5482 also addresses CVE-2019-5481.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 24 new security patches for Oracle Financial Services Applications. 6 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-0227	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Non
CVE-2019-0227	Oracle Financial Services Funds Transfer Pricing	Web Service (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Non
CVE-2020-2718	Oracle Banking Corporate Lending	Core	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2713	Oracle Banking Payments	Core	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2688	Oracle Financial Services Analytical Applications Infrastructure	Object Migration	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2723	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2699	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	7.1	Network	Low	Lo
CVE-2020-2716	Oracle Banking	Core	HTTP	No	6.5	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Corporate Lending							
CVE-2020-2711	Oracle Banking Payments	Core	HTTP	No	6.5	Network	Low	Lo
CVE-2020-2721	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	6.5	Network	Low	Lo
CVE-2020-2684	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.5	Network	Low	Lo
CVE-2020-2715	Oracle Banking Corporate Lending	Core	HTTP	No	5.4	Network	Low	Lo
CVE-2020-2717	Oracle Banking Corporate Lending	Core	HTTP	Yes	5.4	Network	Low	Nor
CVE-2020-2710	Oracle Banking Payments	Core	HTTP	No	5.4	Network	Low	Lo
CVE-2020-2712	Oracle Banking Payments	Core	HTTP	Yes	5.4	Network	Low	Nor
CVE-2020-2730	Oracle Financial Services Revenue Management and Billing	File Upload	HTTP	No	5.4	Network	Low	Lo
CVE-2020-2720	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	5.4	Network	Low	Lo
CVE-2020-2722	Oracle FLEXCUBE	Infrastructure	HTTP	Yes	5.4	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Investor Servicing							
CVE-2020-2685	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	Yes	5.4	Network	Low	Non
CVE-2020-2683	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTPS	No	5.4	Network	Low	Lo
CVE-2020-2719	Oracle Banking Corporate Lending	Core	HTTP	No	4.3	Network	Low	Lo
CVE-2020-2714	Oracle Banking Payments	Core	HTTP	No	4.3	Network	Low	Lo
CVE-2020-2724	Oracle FLEXCUBE Investor Servicing	Infrastructure	HTTP	No	4.3	Network	Low	Lo
CVE-2020-2700	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	4.3	Network	Low	Lo

Oracle Food and Beverage Applications Risk Matrix

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

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2020-2697	Oracle Hospitality	Request Tracker	None	No	4.9	Physical	Low	Low	

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	In
	Suites Management								

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 38 new security patches for Oracle Fusion Middleware. 30 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 January 2020 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 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2602410.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVS	
					Base Score	Attack Vector
CVE-2020-2555	Oracle Coherence	Caching,CacheStore,Invocation	T3	Yes	9.8	Network
CVE-2020-2551	Oracle WebLogic Server	WLS Core Components	IIOP	Yes	9.8	Network
CVE-2020-2546	Oracle WebLogic Server	Application Container - JavaEE	T3	Yes	9.8	Network
CVE-2020-2728	Identity Manager	OIM - LDAP user and role Synch	HTTP	Yes	7.5	Network
CVE-2019-0227	Oracle Big Data	Studio (Apache Axis)	HTTP	Yes	7.5	Adjacent Network

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVS	
					Base Score	Attack Vector
	Discovery					
CVE-2019-0227	Oracle Endeca Information Discovery Studio	Studio (Apache Axis)	HTTP	Yes	7.5	Adjacent Network
CVE-2017-12626	Oracle Endeca Information Discovery Studio	Studio (Apache POI)	HTTP	Yes	7.5	Network
CVE-2019-0227	Oracle Tuxedo	TX SALT (Apache Axis)	HTTP	Yes	7.5	Adjacent Network
CVE-2020-6950	Oracle WebLogic Server	Web Container (JavaServer Faces)	HTTP	Yes	7.5	Network
CVE-2019-17359	Oracle WebLogic Server	Third Party Tools (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network
CVE-2020-2543	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network
CVE-2020-2549	Oracle WebLogic Server	WLS Core Components	HTTP	No	7.2	Network
CVE-2020-2537	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	Yes	7.1	Network
CVE-2020-2538	Oracle WebCenter Sites	Advanced UI	HTTP	Yes	7.1	Network
CVE-2020-2540	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network
CVE-2020-2541	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVS	
					Base Score	Attack Vector
CVE-2020-2576	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network
CVE-2020-2542	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	6.5	Network
CVE-2020-2530	Oracle HTTP Server	Web Listener	HTTP	Yes	6.1	Network
CVE-2020-2533	Oracle Reports Developer	Security and Authentication	HTTP	Yes	6.1	Network
CVE-2020-2534	Oracle Reports Developer	Security and Authentication	HTTP	Yes	6.1	Network
CVE-2020-2539	Oracle WebCenter Sites	Advanced UI	HTTP	Yes	6.1	Network
CVE-2019-1559	Oracle Business Intelligence Enterprise Edition	Analytics Server and Analytics Web General (OpenSSL)	HTTPS	Yes	5.9	Network
CVE-2019-12415	Oracle Endeca Information Discovery Studio	Studio (Apache POI)	None	No	5.5	Local
CVE-2019-12415	Oracle Enterprise Repository	Security Subsystem (Apache POI)	None	No	5.5	Local
CVE-2020-2729	Identity Manager	Advanced Console	HTTP	No	5.4	Network
CVE-2020-2536	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.4	Network
CVE-2019-10247	Oracle Endeca Information	Integrator Acquistion System (Eclipse Jetty)	HTTP	Yes	5.3	Network

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVS	
					Base Score	Attack Vector
	Discovery Integrator					
CVE-2020-2545	Oracle HTTP Server	OSSL Module	HTTPS	Yes	5.3	Network
CVE-2020-2545	Oracle Security Service	SSL API	HTTPS	Yes	5.3	Network
CVE-2020-2550	Oracle WebLogic Server	WLS Core Components	None	No	5.1	Local
CVE-2020-2547	Oracle WebLogic Server	Console	HTTP	No	4.8	Network
CVE-2020-2548	Oracle WebLogic Server	WLS Core Components	HTTP	No	4.8	Network
CVE-2020-2552	Oracle WebLogic Server	WLS Core Components	HTTP	No	4.8	Network
CVE-2020-2535	Oracle Business Intelligence Enterprise Edition	Analytics Server	HTTP	Yes	4.7	Network
CVE-2020-2544	Oracle WebLogic Server	Console	HTTP	Yes	4.3	Network
CVE-2020-2519	Oracle WebLogic Server	Console	HTTP	Yes	4.3	Network
CVE-2020-2531	Oracle Business Intelligence Enterprise Edition	BI Platform Security	HTTP	Yes	3.1	Network

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

Oracle GraalVM Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle GraalVM. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2019-15845	Oracle GraalVM Enterprise Edition	Interpreter and runtime (Ruby)	Multiple	Yes	9.8	Network	Low	None	
CVE-2020-2604	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	8.1	Network	High	None	
CVE-2019-16776	Oracle GraalVM Enterprise Edition	JavaScript (Node.js)	Multiple	No	8.1	Network	Low	Low	
CVE-2020-2595	Oracle GraalVM Enterprise Edition	GraalVM Compiler	Multiple	Yes	5.8	Network	Low	None	
CVE-2020-2581	Oracle GraalVM Enterprise Edition	LLVM Interpreter	None	No	4.0	Local	Low	None	

Notes:

1. This vulnerability is in the standard Ruby libraries, not in the TruffleRuby interpreter.

2. GraalVM Enterprise 19.3 and above includes both Java SE 8 and Java SE 11.

Additional CVEs addressed are below:

- The patch for CVE-2019-15845 also addresses CVE-2019-16201, CVE-2019-16254 and CVE-2019-16255.
- The patch for CVE-2019-16776 also addresses CVE-2019-16775 and CVE-2019-16777.

Oracle Health Sciences Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2019-2904	Oracle Clinical	User Interface (Application Development Framework)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-2904	Oracle Health Sciences Data Management Workbench	User Interface (Application Development Framework)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2018-15756	Oracle Healthcare Master Person Index	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	Nor

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 5 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-17359	Oracle Hospitality Guest Access	Base (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	None
CVE-2020-2675	Oracle Hospitality OPERA 5	Login	HTTP	No	7.1	Network	Low	Low
CVE-2020-2676	Oracle Hospitality OPERA 5	Printing	HTTP	Yes	6.1	Network	Low	None
CVE-2020-2677	Oracle Hospitality OPERA 5	Login	HTTP	No	5.7	Network	Low	Low
CVE-2020-2599	Oracle Hospitality Cruise Materials Management	MMS All	None	No	4.2	Physical	High	None

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Hyperion. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-2904	Hyperion Planning	Application Development Framework	HTTP	Yes	9.8	Network	Low	None
CVE-2020-2563	Hyperion Financial Close Management	Close Manager	HTTP	No	4.2	Network	High	High

Oracle iLearning Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2020-2709	Oracle iLearning	Learner Pages	HTTP	Yes	4.7	Network	Low	None	Re

Oracle Java SE Risk Matrix

This Critical Patch Update contains 12 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 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2604	Java SE, Java SE Embedded	Serialization	Multiple	Yes	8.1	Network	High	None	
CVE-2019-16168	Java SE	JavaFX (SQLite)	Multiple	Yes	7.5	Network	Low	None	
CVE-2019-13117	Java SE	JavaFX (libxslt)	Multiple	Yes	7.5	Network	Low	None	
CVE-2019-13118	Java SE	JavaFX (libxslt)	Multiple	Yes	7.5	Network	Low	None	
CVE-2020-2601	Java SE, Java SE Embedded	Security	Kerberos	Yes	6.8	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	I
CVE-2020-2585	Java SE	JavaFX	Multiple	Yes	5.9	Network	High	None	
CVE-2020-2655	Java SE	JSSE	HTTPS	Yes	4.8	Network	High	None	
CVE-2020-2593	Java SE, Java SE Embedded	Networking	Multiple	Yes	4.8	Network	High	None	
CVE-2020-2654	Java SE	Libraries	Multiple	Yes	3.7	Network	High	None	
CVE-2020-2590	Java SE, Java SE Embedded	Security	Kerberos	Yes	3.7	Network	High	None	
CVE-2020-2659	Java SE, Java SE Embedded	Networking	Multiple	Yes	3.7	Network	High	None	
CVE-2020-2583	Java SE, Java SE Embedded	Serialization	Multiple	Yes	3.7	Network	High	None	

Notes:

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

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

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

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle JD Edwards. 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-2019-14379	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security (jackson-databind)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-16943	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security (jackson-databind)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-14379	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics SEC (jackson-databind)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-16943	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics	HTTP	Yes	9.8	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
		SEC (jackson-databind)						
CVE-2019-12086	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-12086	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics SEC (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-12086	JD Edwards EnterpriseOne Tools	Web Runtime SEC (jackson databind)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-11358	JD Edwards EnterpriseOne Tools	Web Runtime SEC (jQuery)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-11358	JD Edwards EnterpriseOne Tools	Web Runtime SEC (jQuery)	HTTP	Yes	6.1	Network	Low	Nor

Additional CVEs addressed are below:

- The patch for CVE-2019-14379 also addresses CVE-2019-14439.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 19 new security patches for Oracle MySQL. 6 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-16168	MySQL Workbench	MySQL Workbench (SQLite)	MySQL Workbench	Yes	7.5	Network	Low
CVE-2019-1547	MySQL Connectors	Connector/ODBC (OpenSSL)	TLS	Yes	7.4	Network	High
CVE-2020-2579	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low
CVE-2020-2686	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low
CVE-2020-2627	MySQL Server	Server: Parser	MySQL Protocol	No	6.5	Network	Low
CVE-2020-2570	MySQL Client	C API	MySQL Protocol	Yes	5.9	Network	High
CVE-2020-2573	MySQL Client	C API	MySQL Protocol	Yes	5.9	Network	High
CVE-2020-2574	MySQL Client	C API	MySQL Protocol	Yes	5.9	Network	High
CVE-2020-2577	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2020-2589	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-2580	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low
CVE-2020-2588	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2020-2660	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2020-2679	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2019-1547	MySQL Enterprise Backup	Security (OpenSSL)	TLS	No	4.7	Local	High
CVE-2020-2584	MySQL Server	Server: Options	MySQL Protocol	No	4.4	Network	High
CVE-2020-2694	MySQL Server	Server: Information Schema	MySQL Protocol	No	3.1	Network	High
CVE-2020-2572	MySQL Server	Server: Audit Plugin	MySQL Protocol	No	2.7	Network	Low
CVE-2019-8457	MySQL Cluster	Cluster: General (SQLite)	Multiple	Yes	0.0	Network	Low

Notes:

1. This CVE is not exploitable in MySQL Cluster. The CVSS v3.0 Base Score for this CVE in the National Vulnerability Database (NVD) is 9.8. SQLite is removed from MySQL Cluster releases with the January 2020 Critical Patch Update.

Additional CVEs addressed are below:

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

- The patch for CVE-2019-8457 also addresses CVE-2019-9936 and CVE-2019-9937.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle PeopleSoft. 12 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2017-15708	PeopleSoft Enterprise PeopleTools	Portal (Apache Commons)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2019-2729	PeopleSoft Enterprise PeopleTools	Security (Oracle WebLogic Server)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2017-12626	PeopleSoft Enterprise PeopleTools	Change Impact Analyzer (Apache POI)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-0227	PeopleSoft Enterprise PeopleTools	Portal (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Nor
CVE-2017-1000376	PeopleSoft PeopleTools	PeopleCode (libffi)	None	No	7.0	Local	High	Lo
CVE-2020-2598	PeopleSoft Enterprise PeopleTools	Activity Guide	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2600	PeopleSoft Enterprise PeopleTools	Elastic Search	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2606	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2607	PeopleSoft Enterprise PeopleTools	PIA Core Technology	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	Pri Rec
CVE-2020-2663	PeopleSoft Enterprise PeopleTools	PIA Core Technology	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2602	PeopleSoft Enterprise PeopleTools	Tree Manager	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2695	PeopleSoft Enterprise CC Common Application Objects	Approval Framework	HTTP	Yes	5.3	Network	Low	Nor
CVE-2019-1547	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	None	No	4.7	Local	High	Lo
CVE-2020-2561	PeopleSoft Enterprise HCM Human Resources	Company Dir / Org Chart Viewer	HTTP	No	4.3	Network	Low	Lo
CVE-2020-2687	PeopleSoft Enterprise PeopleTools	Elastic Search	HTTP	Yes	4.3	Network	Low	Nor

Additional CVEs addressed are below:

- The patch for CVE-2017-15708 also addresses CVE-2019-10086.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.
- The patch for CVE-2019-2729 also addresses CVE-2019-2725.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 22 new security patches for Oracle Retail Applications. 14 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2904	Oracle Retail Assortment Planning	Application Core (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Retail Clearance Optimization Engine	Dataset Componen (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2016-5019	Oracle Retail Clearance Optimization Engine	Dataset Component (Apache Trinidad)	HTTP	Yes	9.8	Network	Low	N
CVE-2016-5019	Oracle Retail Clearance Optimization Engine	General Application (Apache Trinidad)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-12814	Oracle Retail Customer Management and Segmentation Foundation	Segment (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Retail Markdown Optimization	Common Component Integration (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-12419	Oracle Retail Order Broker	Order Broker Foundation (CXF)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Retail Sales Audit	Operational Insights (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2018-1258	Oracle Retail Clearance	Dataset Component	HTTP	No	8.8	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Optimization Engine	(Spring Framework)						
CVE-2018-1258	Oracle Retail Markdown Optimization	Common Component Integration (Spring Framework)	HTTPS	No	8.8	Network	Low	L
CVE-2016-1181	Oracle Retail Clearance Optimization Engine	Dataset Component (Struts1)	HTTP	Yes	8.1	Network	High	N
CVE-2016-1181	Oracle Retail Markdown Optimization	Common Component Integration (Struts1)	HTTP	Yes	8.1	Network	High	N
CVE-2018-8039	Oracle Retail Order Broker	System Administration (Apache CXF)	HTTP	Yes	8.1	Network	High	N
CVE-2019-0227	Oracle Retail Order Broker	System Administration (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	N
CVE-2020-2650	Oracle Retail Customer Management and Segmentation Foundation	Promotions	HTTP	Yes	6.5	Network	Low	N
CVE-2020-2648	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations	None	No	6.2	Physical	Low	H
CVE-2019-17091	Oracle Retail Assortment Planning	Application Core (Mojarra)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-12415	Oracle Retail Clearance Optimization Engine	General Application (Apache POI)	None	No	5.5	Local	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-12415	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache POI)	None	No	5.5	Local	Low	L
CVE-2019-12415	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache POI)	None	No	5.5	Local	Low	L
CVE-2020-2567	Oracle Retail Customer Management and Segmentation Foundation	Security	HTTP	No	4.8	Network	Low	H
CVE-2020-2649	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations	None	No	3.3	Local	Low	L

Additional CVEs addressed are below:

- The patch for CVE-2016-1181 also addresses CVE-2016-1182.
- The patch for CVE-2016-5019 also addresses CVE-2019-2904.
- The patch for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257 and CVE-2018-15756.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-12419 also addresses CVE-2019-12406.
- The patch for CVE-2019-12814 also addresses CVE-2018-11307, CVE-2019-12384, CVE-2019-14379, CVE-2019-14439, CVE-2019-14540, CVE-2019-16335, CVE-2019-16942, CVE-2019-16943, CVE-2019-17267 and CVE-2019-17531.
- The patch for CVE-2019-2904 also addresses CVE-2019-2094.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 5 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 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-14379	Siebel Engineering - Installer & Deployment	Siebel Approval Manager (jackson databind)	HTTP	Yes	9.8	Network	Low	None
CVE-2019-14379	Siebel UI Framework	EAI (jackson-databind)	HTTP	Yes	9.8	Network	Low	None
CVE-2020-2564	Siebel UI Framework	EAI	HTTP	Yes	5.3	Network	Low	None
CVE-2020-2559	Siebel UI Framework	UIF Open UI	HTTP	Yes	5.3	Network	Low	None
CVE-2020-2560	Siebel UI Framework	SWSE Server	HTTP	Yes	4.7	Network	Low	None

Additional CVEs addressed are below:

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

Oracle Systems Risk Matrix

This Critical Patch Update contains 17 new security patches for Oracle Systems. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2019-9636	Sun ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	9.8	Network	Low	Non
CVE-2019-2729	Tape Library ACSLS	Application Server (Oracle	HTTP	Yes	9.8	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
		WebLogic Server)						
CVE-2016-1000031	Tape Library ACSLS	Software (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-2696	Oracle Solaris	Common Desktop Environment	None	No	8.8	Local	Low	Low
CVE-2020-2565	Oracle Solaris	Consolidation Infrastructure	None	No	7.5	Local	High	Low
CVE-2019-2725	Tape Library ACSLS	Application Server (Oracle WebLogic Server)	HTTP	Yes	7.5	Network	Low	Non
CVE-2018-15756	Tape Library ACSLS	Software (Spring Framework)	HTTP	Yes	7.5	Network	Low	Non
CVE-2020-2605	Oracle Solaris	Filesystem	None	No	7.1	Local	Low	Low
CVE-2019-11358	Tape Library ACSLS	Software (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2020-2680	Oracle Solaris	Filesystem	None	No	6.0	Local	Low	Hig
CVE-2020-2558	Oracle Solaris	Kernel	SMB	Yes	5.8	Network	Low	Non
CVE-2020-2578	Oracle Solaris	Kernel	SMB	Yes	5.8	Network	Low	Non
CVE-2020-2647	Oracle Solaris	Kernel	None	No	5.0	Local	Low	Low
CVE-2020-2664	Oracle Solaris	Filesystem	None	No	4.6	Local	Low	Low
CVE-2020-2656	Oracle Solaris	X Window System	None	No	4.4	Local	Low	Low
CVE-2019-9579	Oracle Solaris	SMB Server	None	No	3.3	Local	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-2571	Oracle VM Server for SPARC	Templates	None	No	3.3	Local	Low	Non

Additional CVEs addressed are below:

- The patch for CVE-2019-11358 also addresses CVE-2015-9251.
- The patch for CVE-2019-9636 also addresses CVE-2017-15906, CVE-2018-1000030, CVE-2018-1060, CVE-2018-11759, CVE-2018-15473, CVE-2018-17189, CVE-2018-20684, CVE-2019-0215, CVE-2019-1559, CVE-2019-5718 and CVE-2019-9208.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 8 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 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2016-6814	Oracle Agile PLM MCAD Connector	CAX Client (Apache Groovy)	HTTP	Yes	9.6	Network	Low	Non
CVE-2019-0232	Oracle Agile Engineering Data Management	Install (Apache Tomcat)	HTTP	Yes	8.1	Network	High	Non
CVE-2017-12626	Oracle Agile PLM	Security (Apache POI)	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-10072	Oracle Agile PLM	Security (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-0227	Oracle Agile PLM Framework	Web Services (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-2592	Oracle AutoVue	Security	HTTP	Yes	5.3	Network	Low	Non
CVE-2019-10247	Oracle AutoVue	Security (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	Non
CVE-2020-2557	Oracle Demantra Demand Management	Security	HTTP	Yes	4.7	Network	Low	Non

Additional CVEs addressed are below:

- 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-2019-10247 also addresses CVE-2019-10246.

Oracle Utilities Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2016-1000031	Oracle Utilities Work and Asset Management (v1)	Core (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-11358	Oracle Real-Time Scheduler	Next Gen Mobile Application (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2019-11358	Oracle Utilities Mobile	Next Gen Mobile Application (jQuery)	HTTP	Yes	6.1	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Workforce Management							
CVE-2014-3004	Oracle Utilities Framework	Common (Castor)	HTTP	Yes	5.3	Network	Low	No

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 22 new security patches for Oracle Virtualization. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2674	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High
CVE-2020-2682	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High
CVE-2019-0227	Oracle Secure Global Desktop	Web Services (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	None
CVE-2020-2698	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-2701	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-2702	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-2726	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-2681	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2689	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2690	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2691	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-2692	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2703	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2704	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2705	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2725	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2678	Oracle VM VirtualBox	Core	None	No	6.4	Local	High	Low	
CVE-2019-17091	Oracle Secure Global Desktop	Core (Mojarra)	Multiple	Yes	6.1	Network	Low	None	
CVE-2020-2727	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-2693	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2019-10092	Oracle Secure Global Desktop	Web Server (Apache HTTPD Server)	HTTP	Yes	4.7	Network	High	None	
CVE-2019-1547	Oracle Secure Global Desktop	Core (OpenSSL)	None	No	4.7	Local	High	Low	

Additional CVEs addressed are below:

- The patch for CVE-2019-10092 also addresses CVE-2019-10098.
- The patch for CVE-2019-1547 also addresses CVE-2019-1552 and CVE-2019-1563.