Oracle Critical Patch Update Advisory - January 2021

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third-party components included in Oracle products. 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. 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 329 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 2021 Critical Patch Update: Executive Summary and Analysis.

Please note that since the release of the October 2020 Critical Patch Update, Oracle has released a Security Alert for Oracle WebLogic Server: CVE-2020-14750 (November 1, 2020). Customers are strongly advised to apply this Critical Patch Update, which includes patches for this Alert as well as additional patches.

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
Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Enterprise Manager Base Platform, versions 13.2.1.0, 13.3.0.0, 13.4.0.0	Enterprise Manager
Enterprise Manager for Fusion Applications, version 13.3.0.0	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
Hyperion Financial Reporting, version 11.1.2.4	Fusion Middleware
Hyperion Infrastructure Technology, version 11.1.2.4	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1-17.3	Oracle Construction and Engineering Suite
JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.5.1	JD Edwards
JD Edwards EnterpriseOne Tools, versions prior to 9.2.5.0	JD Edwards
MySQL Client, versions 5.6.50 and prior, 5.7.32 and prior, 8.0.22 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.22 and prior	MySQL
MySQL Server, versions 5.6.50 and prior, 5.7.32 and prior, 8.0.22 and prior	MySQL
MySQL Workbench, versions 8.0.22 and prior	MySQL
Oracle Adaptive Access Manager, version 11.1.2.3.0	Fusion Middleware
Oracle Agile Engineering Data Management, version 6.2.1.0	Oracle Supply Chain Products
Oracle Agile PLM, versions 9.3.5, 9.3.6	Oracle Supply Chain Products
Oracle Agile Product Lifecycle Management for Process, version 6.1	Oracle Supply Chain Products
Oracle Application Express Opportunity Tracker, versions prior to 20.2	Database
Oracle Application Express Survey Builder, versions prior to 20.2	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle Argus Safety, version 8.2.2	Health Sciences
Oracle BAM (Business Activity Monitoring), versions 11.1.1.9.0, 12.2.1.3.0	Fusion Middleware
Oracle Banking Corporate Lending Process Management, versions 14.1.0, 14.3.0, 14.4.0	Oracle Financial Services Applications
Oracle Banking Credit Facilities Process Management, versions 14.1.0, 14.3.0, 14.4.0	Oracle Financial Services Applications

Affected Products and Versions	Patch Availability Document
Oracle Banking Extensibility Workbench, versions 14.3.0, 14.4.0	Oracle Financial Services Applications
Oracle Banking Liquidity Management, versions 14.0.0-14.4.0	Oracle Financial Services Applications
Oracle Banking Payments, version 14.4.0	Oracle Financial Services Applications
Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.6.2, 2.7.0, 2.7.1, 2.8.0, 2.9.0	Oracle Banking Platform
Oracle Banking Supply Chain Finance, versions 14.2.0-14.4.0	Oracle Financial Services Applications
Oracle Banking Trade Finance Process Management, versions 14.1.0, 14.3.0, 14.4.0	Oracle Financial Services Applications
Oracle Banking Virtual Account Management, versions 14.1.0, 14.3.0, 14.4.0	Oracle Financial Services Applications
Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle Communications Application Session Controller, version 3.9m0p2	Oracle Communications Application Session Controller
Oracle Communications ASAP, version 7.3	Oracle Communications ASAP
Oracle Communications BRM - Elastic Charging Engine, versions 11.3.0.9, 12.0.0.3	Oracle Communications BRM - Elasti Charging Engine
Oracle Communications Calendar Server, version 8.0.0.4.0	Oracle Communications Calendar Ser
Oracle Communications Contacts Server, version 8.0.0.5.0	Oracle Communications Contacts Ser
Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0-8.2.2	Oracle Communications Diameter Signaling Router
Oracle Communications Element Manager, versions 8.2.1.0-8.2.2.1	Oracle Communications Element Manager
Oracle Communications MetaSolv Solution, versions 6.3.0-6.3.1	Oracle Communications MetaSolv Solution
Oracle Communications Network Charging and Control, versions 6.0.1, 12.0.2	Oracle Communications Network Charging and Control
Oracle Communications Operations Monitor, versions 3.4, 4.1, 4.2, 4.3	Oracle Communications Operations Monitor

Affected Products and Versions	Patch Availability Document
Oracle Communications Performance Intelligence Center (PIC) Software, version 10.4.0.2	Oracle Communications Performance Intelligence Center (PIC) Software
Oracle Communications Session Report Manager, versions 8.2.1.0-8.2.2.1	Oracle Communications Session Rep Manager
Oracle Complex Maintenance, Repair, and Overhaul, versions 11.5.10, 12.1, 12.2	Oracle Supply Chain Products
Oracle Configurator, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Data Integrator, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 18c, 19c	Database
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10	E-Business Suite
Oracle Endeca Information Discovery Integrator, version 3.2.0.0	Fusion Middleware
Oracle Enterprise Communications Broker, versions 3.1, 3.2	Oracle Enterprise Communications Broker
Oracle Enterprise Data Quality, versions 11.1.1.9.0, 12.2.1.3.0	Fusion Middleware
Oracle Enterprise Repository, version 11.1.1.7.0	Fusion Middleware
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.0	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Asset Liability Management, versions 8.0.7, 8.1.0	Oracle Financial Services Asset Liabil Management
Oracle Financial Services Data Integration Hub, versions 8.0.3, 8.0.6	Oracle Financial Services Data Integration Hub
Oracle Financial Services Funds Transfer Pricing, versions 8.0.6, 8.0.7, 8.1.0	Oracle Financial Services Funds Trans Pricing
Oracle Financial Services Market Risk Measurement and Management, version 8.0.6	Oracle Financial Services Market Risk Measurement and Management
Oracle Financial Services Profitability Management, versions 8.0.6, 8.0.7, 8.1.0	Oracle Financial Services Profitability Management
Oracle Financial Services Revenue Management and Billing, versions 2.9.0.0, 2.9.0.1	Oracle Financial Services Revenue Management and Billing
Oracle FLEXCUBE Core Banking, versions 11.5.0-11.9.0	Oracle Financial Services Applications
Oracle FLEXCUBE Universal Banking, version 14.4.0	Oracle Financial Services Applications
Oracle Fusion Middleware MapViewer, version 12.2.1.3.0	Fusion Middleware
Oracle Global Lifecycle Management OPatch	Fusion Middleware
Oracle Global Lifecycle Manager	Global Lifecycle Management
Oracle GoldenGate Application Adapters, version 19.1.0.0.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle GraalVM Enterprise Edition, versions 19.3.4, 20.3.0	Oracle GraalVM Enterprise Edition
Oracle Health Sciences Information Manager, version 3.0.1	Health Sciences
Oracle Healthcare Master Person Index, version 4.0.2.5	Health Sciences
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle Hospitality Simphony, versions 18.2.7.2, 19.1.3	Oracle Hospitality Simphony
Oracle Insurance Allocation Manager for Enterprise Profitability, version 8.1.0	Oracle Insurance Allocation Manager Enterprise Profitability
Oracle Insurance Insbridge Rating and Underwriting, versions 5.0.0.20, 5.1.1.3	Oracle Insurance Applications
Oracle Insurance Policy Administration, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0-11.3.0	Oracle Insurance Applications
Oracle Insurance Rules Palette, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0-11.3.0	Oracle Insurance Applications
Oracle Java SE, versions 7u281, 8u271	Java SE
Oracle Java SE Embedded, version 8u271	Java SE
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Outside In Technology, versions 8.5.4, 8.5.5	Fusion Middleware
Oracle Real-Time Decision Server, version 3.2.1.0	Fusion Middleware
Oracle Retail Assortment Planning, version 16.0.3	Retail Applications
Oracle Retail Bulk Data Integration, versions 15.0.3, 16.0.3	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0, 19.0	Retail Applications
Oracle Retail Extract Transform and Load, versions 13.2.5, 13.2.8	Retail Applications
Oracle Retail Financial Integration, versions 14.1.3, 15.0.3, 16.0.3	Retail Applications
Oracle Retail Integration Bus, versions 14.1.3, 15.0.3, 16.0.3	Retail Applications
Oracle Retail Invoice Matching, versions 13.2, 14.0, 14.1	Retail Applications
Oracle Retail Merchandising System, version 15.0	Retail Applications
Oracle Retail Order Broker, versions 15.0, 16.0	Retail Applications
Oracle Retail Order Broker Cloud Service, version 15.0	Retail Applications
Oracle Retail Sales Audit, version 14.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1.3, 15.0.3, 16.0.3	Retail Applications

Affected Products and Versions	Patch Availability Document
Oracle Retail Store Inventory Management, versions 14.0.4.0, 14.1.3.0, 14.1.3.9, 15.0.3.0, 16.0.3.0	Retail Applications
Oracle SD-WAN Edge, version 9.0	Oracle SD-WAN Edge
Oracle Secure Backup	Oracle Secure Backup
Oracle Transportation Management, version 1.4.3	Oracle Supply Chain Products
Oracle Utilities Framework, versions 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.18	Virtualization
Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0	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, 14.1.1.0.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
PeopleSoft Enterprise FIN Payables, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Human Resources, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft
Primavera Gateway, versions 16.2.0-16.2.11, 17.12.0-17.12.9, 18.8.0-18.8.10, 19.12.0-19.12.10	Oracle Construction and Engineering Suite
Primavera P6 Enterprise Project Portfolio Management, versions 16.1.0-16.2.20, 17.1.0-17.12.19, 18.1.0-18.8.21, 19.12.0-19.12.10	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12, 20.12	Oracle Construction and Engineering Suite
Siebel Applications, versions 20.12 and prior	Siebel
StorageTek Tape Analytics SW Tool, version 2.3.1	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.

- Solaris Third Party Bulletins are used to announce security patches for third party software distributed with Oracle Solaris. Solaris 10 customers should refer to the latest patch-sets which contain critical security fixes and detailed in Systems Patch Availability Document. Please see Reference Index of CVE IDs and Solaris Patches (My Oracle Support Note 1448883.1) for more information.
- Users running Java SE with a browser can download the latest release from https://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 its unique identifier. 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 3.1 (see Oracle CVSS Scoring for an explanation of how Oracle applies CVSS version 3.1).

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.

Oracle lists updates that address vulnerabilities in third-party components which are not exploitable in the context of their inclusion in their respective Oracle product beneath the product's risk matrix.

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:

- 0rich1 of Ant Security FG Lab: CVE-2021-2109

- 0xfoxone: CVE-2021-2068
- Alessandro Bosco of TIM S.p.A: CVE-2021-2005
- Alves Christopher of Telecom Nancy: CVE-2021-2006, CVE-2021-2010, CVE-2021-2011
- Amey Anekar of CyberCube Services: CVE-2021-2052
- Amy Tran: CVE-2021-2026, CVE-2021-2027
- Andrej Simko of Accenture: CVE-2021-2077, CVE-2021-2078, CVE-2021-2079, CVE-2021-2080, CVE-2021-2082, CVE-2021-2083, CVE-2021-2084, CVE-2021-2085, CVE-2021-2090, CVE-2021-2091, CVE-2021-2092, CVE-2021-2093, CVE-2021-2094, CVE-2021-2096, CVE-2021-2097, CVE-2021-2098, CVE-2021-2099, CVE-2021-2100, CVE-2021-2101, CVE-2021-2102, CVE-2021-2103, CVE-2021-2104, CVE-2021-2105, CVE-2021-2106, CVE-2021-2107, CVE-2021-2114, CVE-2021-2115, CVE-2021-2118
- Antonin B. of NCIA / NCSC: CVE-2021-2017
- Bui Duong from Viettel Cyber Security: CVE-2021-2013, CVE-2021-2049, CVE-2021-2050, CVE-2021-2051
- ChauUHM from Sacombank: CVE-2021-2062
- ChenNan Of Chaitin Security Research Lab: CVE-2021-2086, CVE-2021-2111, CVE-2021-2112, CVE-2021-2119, CVE-2021-2120, CVE-2021-2121, CVE-2021-2125, CVE-2021-2126, CVE-2021-2129, CVE-2021-2131
- Chi Tran: CVE-2021-2026, CVE-2021-2027
- Chris Barnabo: CVE-2021-2128
- Cl0und Syclover Security Team: CVE-2020-14756
- Codeplutos of AntGroup FG Security Lab: CVE-2020-14756, CVE-2021-2075
- DoHyun Lee of VirtualBoBs: CVE-2021-2086
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2021-2035, CVE-2021-2054
- Edoardo Predieri of TIM S.p.A: CVE-2021-2005
- Emad Al-Mousa working with Trend Micro Zero Day Initiative: CVE-2021-2054
- Esteban Montes Morales of Accenture: CVE-2021-2089
- Fabio Minarelli of TIM S.p.A: CVE-2021-2005
- Francesco Russo of TIM S.p.A: CVE-2021-2005
- Gaoning Pan of Zhejiang University & Ant Security Light-Year Lab: CVE-2021-2073, CVE-2021-2074, CVE-2021-2086, CVE-2021-2123, CVE-2021-2130
- Girlelecta: CVE-2021-2066, CVE-2021-2067, CVE-2021-2069
- Glassy of Alibaba Cloud Security Group: CVE-2021-2109
- Hangfan Zhang: CVE-2021-2030
- Julien Zhan of Telecom Nancy: CVE-2021-2006, CVE-2021-2010, CVE-2021-2011

- JungHyun Kim (jidoc01) of VirtualBoBs: CVE-2021-2124
- JunYoung Park and DongJun Shin of VirtualBoBs: CVE-2021-2127
- Khuyen Nguyen of secgit.com: CVE-2021-2023
- Kun Yang of Chaitin Security Research Lab: CVE-2021-2086, CVE-2021-2111, CVE-2021-2112, CVE-2021-2119, CVE-2021-2120, CVE-2021-2121, CVE-2021-2125, CVE-2021-2126, CVE-2021-2129, CVE-2021-2131
- Longofo of Knownsec 404 Team: CVE-2021-2109
- Luca Di Giuseppe of TIM S.p.A: CVE-2021-2005
- Lukasz Plonka: CVE-2021-2063
- Lukasz Rupala of ING Tech Poland: CVE-2021-2003
- Maciej Grabiec of ING Tech Poland: CVE-2021-2063
- Massimiliano Brolli of TIM S.p.A: CVE-2021-2005
- Nam HaBach of NightSt0rm: CVE-2021-2034
- Omur Ugur of Turk Telekom: CVE-2021-2003
- Pawel Gocyla of ING Tech Poland: CVE-2021-2063
- Philippe Antoine of Telecom Nancy: CVE-2021-2006, CVE-2021-2010, CVE-2021-2011
- r00t4dm at Cloud-Penetrating Arrow Lab: CVE-2021-2109
- Roberto Suggi Liverani of NCIA / NCSC: CVE-2021-2017
- Rui Zhong: CVE-2021-2030
- Rémi Badonnel of Telecom Nancy: CVE-2021-2010, CVE-2021-2011
- Shimizu Kawasaki of DiDiGlobal Security Product Technology Department (Basic Security): CVE-2021-2109
- Thiscodecc: CVE-2021-2047
- Trung Le: CVE-2021-2026, CVE-2021-2027
- Tuan Anh Nguyen of Viettel Cyber Security: CVE-2021-2025, CVE-2021-2029
- Ved Prabhu: CVE-2021-2116, CVE-2021-2117
- Xiayu Zhang of Tencent Keen Security Lab: CVE-2021-2064
- Xingwei Lin of Ant Security Light-Year Lab: CVE-2021-2073, CVE-2021-2074, CVE-2021-2086, CVE-2021-2123, CVE-2021-2130
- Xu Yuanzhen of Alibaba Cloud Security Team: CVE-2021-2109
- Yakov Shafranovich of T. Rowe Price Associates, Inc.: CVE-2021-2018
- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2021-2055
- Yongheng Chen: CVE-2021-2030

- Yu Wang of BMH Security Team: CVE-2021-2108
- Zhangyanyu of Chaitin Security Research Lab: CVE-2021-2131
- Zouhair Janatil-Idrissi of Telecom Nancy: CVE-2021-2006, CVE-2021-2010, CVE-2021-2011

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, Oracle recognizes the following for contributions to Oracle's Security-In-Depth program.:

- Markus Loewe [2 reports]
- Salini Reus of Fiji Roads Authority

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:

- Aakash Adhikari (dark_haxor)
- Adam Willard [2 reports]
- Ahlan S
- Ahmed Alwardani
- Ahmed Ouahabi
- Anas Rahmani
- Ayushmaan Banerjee
- Boo
- Bradley Baker
- Bui Dinh Bao aka 0xd0ff9 of Zalo Security Team (VNG Corp)
- Bui Duc Anh Khoa aka khoabda of Zalo Security Team (VNG Corp)

- Christopher Hanlon
- Fabien B
- Flaviu Popescu
- Hamoud Al-Helmani [2 reports]
- Harpreet Singh
- Harshal S. Sharma
- Mahmoud ElSayed
- Marwan Albahar [6 reports]
- Matt Bushey
- Mohammad Hosein Askari
- Phan Quan of VNPT Information Security Center (VNPT ISC)
- Prabharoop C.C. [2 reports]
- Prashant Saini
- Pratik Khalane
- Purbasha Ghosh
- Quan Doan of R&D Center - VinCSS LLC (a member of Vingroup) [5 reports]
- Ram Kumar
- Ratnadip Gajbhiye
- Robert Kulig
- Robert Lee Dick
- Sarwar Abbas
- Saurabh Dilip Mhatre
- Shailesh Kumavat
- Shivam Pandey
- Tuan Anh Nguyen of Viettel Cyber Security
- Virendra Singh Rathore

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:

- 20 April 2021
- 20 July 2021

- 19 October 2021
- 18 January 2022

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - January 2021 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/Alert
- Software Error Correction Support Policy
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2021-February-22	Rev 3. Updated the affected versions for CVE-2021-2047
2021-January-25	Rev 2. Update to Credit Statements.
2021-January-19	Rev 1. Initial Release.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 8 new security patches plus additional third party patches noted below for Oracle Database Products. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these 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 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2021-2035	RDBMS Scheduler	Export Full Database	Oracle Net	No	8.8	Network	Low	Low	
CVE-2021-2018	Advanced Networking Option	None	Oracle Net	Yes	8.3	Network	High	None	R
CVE-2021-2054	RDBMS Sharding	Create Any Procedure, Create Any View, Create Any Trigger	Oracle Net	No	7.2	Network	Low	High	
CVE-2021-2116	Oracle Application Express Opportunity Tracker	Valid User Account	HTTP	No	5.4	Network	Low	Low	R
CVE-2021-2117	Oracle Application Express Survey Builder	Valid User Account	HTTP	No	5.4	Network	Low	Low	R
CVE-2021-1993	Java VM	Create Session	Oracle Net	No	4.8	Network	High	Low	R
CVE-2021-2045	Oracle Text	Create Session	Oracle Net	No	3.1	Network	High	Low	
CVE-2021-2000	Unified Audit	SYS Account	Oracle Net	No	2.4	Network	Low	High	R

Notes:

1. CVE-2021-2018 affects Windows platform only.

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Perl: CVE-2020-10878, CVE-2020-10543 and CVE-2020-12723.

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Global Lifecycle Management. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle Global Lifecycle Management. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matr					
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope
There are no exploitable vulnerabilities for these product Third party patches for non-exploitable CVEs are noted bel										

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Oracle Global Lifecycle Manager
  - Patch Installer (Apache Commons Compress): CVE-2019-12402.

Oracle Secure Backup Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Secure Backup. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle Secure Backup. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matr					
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope
There are no exploitable vulnerabilities for these product Third party patches for non-exploitable CVEs are noted bel										

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Oracle Secure Backup
  - User Interface (PHP): CVE-2020-7064.
  - Web Server (Apache HTTP Server): CVE-2020-11984, CVE-2020-11993 and CVE-2020-9490.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Communications 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 VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2020-14195	Oracle Communications Calendar Server	REST API (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-14195	Oracle Communications Contacts Server	REST API (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2019-17566	Oracle Communications MetaSolv Solution	Print Preview (Apache Batik)	HTTP	Yes	7.5	Network	Low
CVE-2020-13871	Oracle Communications Network Charging and Control	Common (SQLite)	SQL	Yes	7.5	Network	Low
CVE-2019-10086	Oracle Communications BRM - Elastic Charging Engine	Coherence Query (Apache Commons BeanUtils)	TCP/IP	Yes	7.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2019-10086	Oracle Communications MetaSolv Solution	Online Help (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2020-5421	Oracle Communications BRM - Elastic Charging Engine	Orchestration, Processor and Messages (Spring Framework)	TCP/IP	No	6.5	Network	High
CVE-2020-1945	Oracle Communications ASAP	Core (Apache Ant)	None	No	6.2	Local	Low

Additional CVEs addressed are:

- The patch for CVE-2020-13871 also addresses CVE-2020-15358.
- The patch for CVE-2020-14195 also addresses CVE-2020-14060, CVE-2020-14061 and CVE-2020-14062.
- The patch for CVE-2020-1945 also addresses CVE-2017-5645.

Oracle Communications Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Communications. 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 VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2019-7164	Oracle Communications Operations Monitor	ORMB DB Query in VSP (SQLAlchemy)	HTTP	Yes	9.8	Network	Low
CVE-2020-24750	Oracle Communications Diameter	IDIH (jackson-databind)	HTTP	Yes	8.1	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Signaling Router (DSR)						
CVE-2020-27216	Oracle Communications Application Session Controller	Core (Eclipse Jetty)	None	No	7.8	Local	Low
CVE-2020-27216	Oracle Communications Element Manager	REST API (Eclipse Jetty)	None	No	7.8	Local	Low
CVE-2020-14147	Oracle Communications Operations Monitor	In-Memeory DB for FDP/VSP (Redis)	HTTP	No	7.7	Network	Low
CVE-2019-17566	Oracle Communications Application Session Controller	Core (Apache Batik)	HTTP	Yes	7.5	Network	Low
CVE-2020-11080	Oracle Enterprise Communications Broker	System (nghttp2)	HTTP	Yes	7.5	Network	Low
CVE-2019-10086	Oracle Communications Diameter Signaling Router (DSR)	IDIH (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2019-10086	Oracle SD-WAN Edge	Management (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2020-10723	Oracle Enterprise Communications Broker	System (DPDK)	None	No	6.7	Local	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2020-5421	Oracle Communications Session Report Manager	Core (Spring Framework)	HTTP	No	6.5	Network	High
CVE-2019-1559	Oracle Communications Performance Intelligence Center (PIC) Software	Security (OpenSSL)	HTTPS	Yes	5.9	Network	High

Additional CVEs addressed are:

- The patch for CVE-2019-1559 also addresses CVE-2018-0732.
- The patch for CVE-2019-7164 also addresses CVE-2019-7548.
- The patch for CVE-2020-10723 also addresses CVE-2020-10722, CVE-2020-10724, CVE-2020-10725 and CVE-2020-10726.
- The patch for CVE-2020-11080 also addresses CVE-2019-9511 and CVE-2019-9513.
- The patch for CVE-2020-24750 also addresses CVE-2020-24616 and CVE-2020-9546.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Construction and Engineering. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-25020	Primavera Unifier	Platform (MPXJ)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-17566	Instantis EnterpriseTrack	Dashboard module	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
		(Apache Batik)						
CVE-2020-11979	Primavera Gateway	Admin (Apache Ant)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-11979	Primavera Unifier	Core, Config (Apache Ant)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-10086	Primavera Unifier	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2020-5421	Primavera Gateway	Admin (Spring Framework)	HTTP	No	6.5	Network	High	L
CVE-2020-5421	Primavera P6 Enterprise Project Portfolio Management	Web access (Spring Framework)	HTTP	No	6.5	Network	High	L

Additional CVEs addressed are:

- The patch for CVE-2020-25020 also addresses CVE-2020-35460.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 31 new security patches for Oracle E-Business Suite. 29 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited

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

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 2021 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 2021), My Oracle Support Note 2737201.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-2029	Oracle Scripting	Miscellaneous	HTTP	Yes	9.8	Network	Low	Nc
CVE-2021-2100	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	9.1	Network	Low	Nc
CVE-2021-2101	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	9.1	Network	Low	Nc
CVE-2021-2093	Oracle Common Applications	CRM User Management Framework	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2114	Oracle Common Applications Calendar	Applications Calendar	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2034	Oracle Common Applications Calendar	Tasks	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2084	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-2085	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2092	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2099	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2105	Oracle Customer Interaction History	Outcome-Result	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2106	Oracle Customer Interaction History	Outcome-Result	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2107	Oracle Customer Interaction History	Outcome-Result	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2090	Oracle Email Center	Message Display	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2098	Oracle Email Center	Message Display	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2089	Oracle iStore	Runtime Catalog	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2077	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2082	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2096	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-2097	Oracle iSupport	Profile	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2083	Oracle iSupport	User Responsibilities	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2026	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2027	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2118	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2094	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2091	Oracle Scripting	Miscellaneous	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2015	Oracle Workflow	Worklist	HTTP	Yes	8.2	Network	Low	Nc
CVE-2021-2115	Oracle Common Applications Calendar	Tasks	HTTP	No	7.6	Network	Low	Lc
CVE-2021-2059	Oracle iStore	Web interface	HTTP	Yes	5.3	Network	Low	Nc
CVE-2021-2023	Oracle Installed Base	APIs	HTTP	Yes	4.7	Network	Low	Nc
CVE-2021-2017	Oracle User Management	Proxy User Delegation	HTTP	No	4.3	Network	Low	Lc

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Enterprise Manager. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these 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 2021 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 2021 Patch Availability Document for Oracle Products, My Oracle Support Note 2725756.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-13990	Enterprise Manager Base Platform	Connector Framework (Quartz)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-11973	Enterprise Manager Base Platform	Reporting Framework (Apache Camel)	HTTP	Yes	9.8	Network	Low	Non
CVE-2016-1000031	Enterprise Manager Base Platform	Reporting Framework (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-11984	Enterprise Manager Ops Center	Control Proxy (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-10683	Oracle Application Testing Suite	Load Testing for Web Apps (dom4j)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2018-15756	Enterprise Manager for Fusion Applications	Topology Viewer (Spring Framework)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2020-11022	Oracle Application Testing Suite	Load Testing for Web Apps (jQuery)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2015-4000	Enterprise Manager Ops Center	User Interface (OpenSSL)	HTTPS	Yes	3.7	Network	High	Nor

Additional CVEs addressed are:

- The patch for CVE-2016-1000031 also addresses CVE-2018-11775 and CVE-2019-0188.
- The patch for CVE-2018-15756 also addresses CVE-2018-1258.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-11973 also addresses CVE-2019-0188, CVE-2020-11971 and CVE-2020-11972.
- The patch for CVE-2020-11984 also addresses CVE-2020-11993 and CVE-2020-9490.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 50 new security patches for Oracle Financial Services Applications. 41 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-2020-11612	Oracle Banking Corporate Lending Process Management	Core (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle Banking Credit Facilities Process Management	Core (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10744	Oracle Banking Extensibility Workbench	Core (Lodash)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-8174	Oracle Banking Extensibility Workbench	Core (Node.js)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle Banking Liquidity Management	Common (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle Banking Payments	Payments Core (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle Banking Supply Chain Finance	Core (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle Banking Trade Finance Process Management	Dashboard (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle Banking Virtual	Common Core (Netty)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Account Management							
CVE-2019-3773	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Spring Web Services)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-0230	Oracle Financial Services Data Integration Hub	User Interface (Apache Struts)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-0230	Oracle Financial Services Market Risk Measurement and Management	User Interface (Apache Struts)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-11612	Oracle FLEXCUBE Universal Banking	Infrastructure (Netty)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-1945	Oracle Banking Liquidity Management	Common (Apache Ant)	HTTP	Yes	9.1	Network	Low	N
CVE-2020-27216	Oracle FLEXCUBE Core Banking	Securities (Eclipse Jetty)	None	No	7.8	Local	Low	L
CVE-2019-12399	Oracle Banking Corporate Lending Process Management	Core (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle Banking Credit Facilities	Core (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Process Management							
CVE-2019-12399	Oracle Banking Liquidity Management	Common (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle Banking Payments	Payments Core (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-11979	Oracle Banking Platform	Installer (Apache Ant)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12402	Oracle Banking Platform	Party, Financials (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle Banking Platform	Product Manufacturing (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle Banking Supply Chain Finance	Core (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle Banking Trade Finance Process Management	Dashboard (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle Banking Virtual Account Management	Common Core (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-11979	Oracle Financial Services Analytical	Infrastructure (Apache Ant)	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Applications Infrastructure							
CVE-2019-12399	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-12399	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache Kafka)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-10086	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-10086	Oracle Financial Services Asset Liability Management	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-10086	Oracle Financial Services Funds Transfer Pricing	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-10086	Oracle Financial Services Market Risk Measurement and Management	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-10086	Oracle Financial Services Profitability Management	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-10086	Oracle Insurance Allocation Manager for Enterprise Profitability	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2020-5408	Oracle Banking Corporate Lending Process Management	Core (Spring Security)	HTTP	No	6.5	Network	Low	L
CVE-2020-5408	Oracle Banking Credit Facilities Process Management	Core (Spring Security)	HTTP	No	6.5	Network	Low	L
CVE-2020-5408	Oracle Banking Liquidity Management	Common (Spring Security)	HTTP	No	6.5	Network	Low	L
CVE-2020-5408	Oracle Banking Supply Chain Finance	Core (Spring Security)	HTTP	No	6.5	Network	Low	L
CVE-2020-5408	Oracle Banking Trade Finance Process Management	Dashboard (Spring Security)	HTTP	No	6.5	Network	Low	L
CVE-2020-5408	Oracle Banking Virtual Account Management	Common Core (Spring Security)	HTTP	No	6.5	Network	Low	L
CVE-2020-5421	Oracle Financial Services Analytical	Infrastructure (Spring Framework)	HTTP	No	6.5	Network	High	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Applications Infrastructure							
CVE-2019-11269	Oracle Banking Corporate Lending Process Management	Core (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle Banking Credit Facilities Process Management	Core (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle Banking Liquidity Management	Common (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle Banking Payments	Payments Core (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle Banking Supply Chain Finance	Core (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle Banking Trade Finance Process Management	Dashboard (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle Banking Virtual Account Management	Common Core (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N
CVE-2019-11269	Oracle FLEXCUBE Universal Banking	Infrastructure (Spring Security Oauth)	HTTP	Yes	5.4	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2113	Oracle Financial Services Revenue Management and Billing	On Demand Billing	HTTP	No	4.3	Network	Low	L

Additional CVEs addressed are:

- The patch for CVE-2019-0230 also addresses CVE-2019-0233 and CVE-2020-17530.
- The patch for CVE-2019-11269 also addresses CVE-2019-3778.
- The patch for CVE-2020-1945 also addresses CVE-2020-11979.
- The patch for CVE-2020-5408 also addresses CVE-2020-5407.
- The patch for CVE-2020-8174 also addresses CVE-2020-10531, CVE-2020-11080 and CVE-2020-8172.

Oracle Food and Beverage Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2018-1285	Oracle Hospitality Simphony	Simphony Server (Apache log4net)	HTTP	Yes	9.8	Network	Low	None	
CVE-2021-1997	Oracle Hospitality Reporting and Analytics	Report	HTTP	No	8.1	Network	Low	Low	

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 60 new security patches plus additional third party patches noted below for Oracle Fusion Middleware. 47 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Please note that the Security Alert patches for Oracle WebLogic Server: CVE-2020-14750 are included in this Critical Patch Update. Customers are strongly advised to apply this Critical Patch Update.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-10173	Oracle BAM (Business Activity Monitoring)	General (Xstream)	HTTP	Yes	9.8	Network	Low
CVE-2020-10683	Oracle Business Process Management Suite	Installer (dom4j)	HTTP	Yes	9.8	Network	Low
CVE-2020-14756	Oracle Coherence	Core Components	IIOP, T3	Yes	9.8	Network	Low
CVE-2015-8965	Oracle Data Integrator	Install, config, upgrade (Rogue Wave JViews)	HTTP	Yes	9.8	Network	Low
CVE-2020-10683	Oracle Data Integrator	Runtime Java agent for ODI (dom4j)	HTTP	Yes	9.8	Network	Low
CVE-2016-1000031	Oracle Enterprise Data Quality	General (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low
CVE-2020-10683	Oracle Enterprise	General (dom4j)	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
	Data Quality						
CVE-2020-11998	Oracle Enterprise Repository	Security Subsystem (Apache ActiveMQ)	HTTP	Yes	9.8	Network	Low
CVE-2020-10683	Oracle WebCenter Portal	Portlet Services (dom4j)	HTTP	Yes	9.8	Network	Low
CVE-2019-17195	Oracle WebLogic Server	Core Components (Connect2id Nimbus JOSE+JWT)	HTTP	Yes	9.8	Network	Low
CVE-2021-1994	Oracle WebLogic Server	Web Services	HTTP	Yes	9.8	Network	Low
CVE-2021-2047	Oracle WebLogic Server	Core Components	IIOP, T3	Yes	9.8	Network	Low
CVE-2021-2064	Oracle WebLogic Server	Core Components	IIOP, T3	Yes	9.8	Network	Low
CVE-2021-2108	Oracle WebLogic Server	Core Components	IIOP, T3	Yes	9.8	Network	Low
CVE-2021-2075	Oracle WebLogic Server	Samples	IIOP, T3	Yes	9.8	Network	Low
CVE-2020-1945	Oracle Real-Time Decision Server	Decision Studio (Apache Ant)	HTTP	Yes	9.1	Network	Low
CVE-2020-5421	Oracle Endeca Information Discovery Integrator	Integrator ETL (Spring Framework)	HTTP	No	8.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2021-2066	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	8.6	Network	Low
CVE-2021-2067	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	8.6	Network	Low
CVE-2021-2068	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	8.6	Network	Low
CVE-2021-2069	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	8.6	Network	Low
CVE-2021-2025	Oracle Business Intelligence Enterprise Edition	Analytics Web General	HTTP	Yes	8.2	Network	Low
CVE-2021-2041	Oracle Business Intelligence Enterprise Edition	Installation	HTTP	Yes	8.1	Network	High
CVE-2021-2049	Oracle BI Publisher	Administration	HTTP	No	7.6	Network	Low
CVE-2021-2013	Oracle BI Publisher	BI Publisher Security	HTTP	No	7.6	Network	Low
CVE-2021-2050	Oracle BI Publisher	E-Business Suite - XDO	HTTP	No	7.6	Network	Low
CVE-2021-2051	Oracle BI Publisher	E-Business Suite - XDO	HTTP	No	7.6	Network	Low
CVE-2021-2062	Oracle BI Publisher	Web Server	HTTP	No	7.6	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-17359	Oracle Data Integrator	Runtime Java agent for ODI (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2017-12626	Oracle Enterprise Data Quality	General (Apache POI)	HTTP	Yes	7.5	Network	Low
CVE-2020-11979	Oracle Enterprise Repository	Security Subsystem (Apache Ant)	HTTP	Yes	7.5	Network	Low
CVE-2019-17566	Oracle Enterprise Repository	Security Subsystem (Apache Batik)	HTTP	Yes	7.5	Network	Low
CVE-2020-11994	Oracle Enterprise Repository	Security Subsystem (Apache Camel)	HTTP	Yes	7.5	Network	Low
CVE-2020-13935	Oracle Managed File Transfer	MFT Runtime Server (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2019-0227	Oracle Real-Time Decision Server	Platform Installation (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-10086	Oracle Data Integrator	Install, config, upgrade (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2019-10086	Oracle Endeca Information Discovery Integrator	Integrator ETL (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2019-10086	Oracle Fusion	Install (Apache Commons	HTTP	Yes	7.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
	Middleware MapViewer	BeanUtils)					
CVE-2019-10086	Oracle Real-Time Decision Server	Platform Installation (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2019-10086	Oracle WebCenter Portal	Security Framework (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2019-10086	Oracle WebLogic Server	Console (Apache Commons Beanutils)	HTTP	Yes	7.3	Network	Low
CVE-2021-2109	Oracle WebLogic Server	Console	HTTP	No	7.2	Network	Low
CVE-2018-2587	Oracle Adaptive Access Manager	Install and Config	HTTP	Yes	6.5	Network	High
CVE-2018-9019	Oracle Data Integrator	Rest Service (Dolibarr)	HTTP	Yes	6.5	Network	Low
CVE-2020-5421	Oracle GoldenGate Application Adapters	Application Adapters (Spring Framework)	HTTP	No	6.5	Network	High
CVE-2020-5421	Oracle WebLogic Server	Sample apps (Spring Framework)	HTTP	No	6.5	Network	High
CVE-2021-1995	Oracle WebLogic Server	Web Services	HTTP	No	6.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-14862	Oracle Business Intelligence Enterprise Edition	Analytics Server (Knockout)	HTTP	Yes	6.1	Network	Low
CVE-2019-17091	Oracle Enterprise Data Quality	General (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle WebCenter Sites	WebCenter Sites (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle WebLogic Server	Sample apps (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2016-5725	Oracle Data Integrator	Install, config, upgrade (JCraft JSch)	SFTP	Yes	5.9	Network	High
CVE-2018-10237	Oracle WebLogic Server	Centralized Thirdparty Jars (Google Guava)	HTTP	Yes	5.9	Network	High
CVE-2021-2003	Business Intelligence Enterprise Edition	Analytics Web Dashboards	HTTP	No	5.4	Network	Low
CVE-2019-10247	Oracle Data Integrator	Centralized Thirdparty Jars (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2021-2005	Oracle Business Intelligence Enterprise Edition	BI Platform Security	HTTP	Yes	4.7	Network	Low
CVE-2021-2033	Oracle WebLogic Server	Core Components	HTTP	No	4.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-9488	Oracle Data Integrator	Install, config, upgrade (Apache Log4j)	HTTP	Yes	3.7	Network	High
CVE-2020-9488	Oracle GoldenGate Application Adapters	Application Adapters (Apache Log4j)	HTTP	Yes	3.7	Network	High
CVE-2021-1996	Oracle WebLogic Server	Web Services	HTTP	No	2.4	Network	Low

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:

- The patch for CVE-2018-9019 also addresses CVE-2017-5611 and CVE-2018-7318.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10247 also addresses CVE-2019-10246.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-13935 also addresses CVE-2020-13934.
- The patch for CVE-2021-2041 also addresses CVE-2019-2697.

Additional patches are included in this Critical Patch Update for the following non-exploitable CVEs in this Oracle product family:

- Oracle Global Lifecycle Management OPatch
    - Patch Installer (Apache Commons Compress): CVE-2019-12402 and CVE-2012-2098.

Oracle GraalVM Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle GraalVM. 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 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-8277	Oracle GraalVM Enterprise Edition	Node (Node.js)	HTTP	Yes	7.5	Network	Low	None	
CVE-2020-14803	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	5.3	Network	High	None	

Additional CVEs addressed are:

- The patch for CVE-2020-8277 also addresses CVE-2020-1971, CVE-2020-8265 and CVE-2020-8287.

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle Health Sciences Applications. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-10683	Oracle Health Sciences Information Manager	Recordlocator, DSUB (dom4j)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-5421	Oracle Healthcare Master	MDM Module (Spring Framework)	HTTP	No	6.5	Network	High	Lov

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Person Index							
CVE-2021-2040	Oracle Argus Safety	Case Form, Local Affiliate Form	HTTP	Yes	6.1	Network	Low	Non
CVE-2021-2110	Oracle Argus Safety	Letters	HTTP	No	5.0	Network	Low	Lov
CVE-2020-9488	Oracle Health Sciences Information Manager	Recordlocator, DSUB (Apache Log4j)	HTTP	Yes	3.7	Network	High	Non

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Hyperion. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2019-13990	Hyperion Infrastructure Technology	Common Security (Quartz)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-11984	Hyperion Infrastructure Technology	Installation and Configuration (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-17563	Hyperion Infrastructure Technology	Common Security (Apache Tomcat)	HTTP	Yes	7.5	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2019-12402	Hyperion Infrastructure Technology	Installation and Configuration (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2020-5421	Hyperion Infrastructure Technology	Installation and Configuration (Spring Framework)	HTTP	No	6.5	Network	High	Lo
CVE-2020-11022	Hyperion Financial Reporting	Installation (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2019-12415	Hyperion Infrastructure Technology	Common Security (Apache POI)	None	No	5.5	Local	Low	Lo

Notes:

1. This CVE is not exploitable in Hyperion Infrastructure Technology. The CVSS v3.1 Base Score for this CVE in the National Vulnerability Database (NVD) is 9.5. Tomcat is removed in Hyperion Infrastructure Technology with the January 2021 Critical Patch Update.

2. This CVE is not exploitable in Hyperion Financial Reporting. The CVSS v3.1 Base Score for this CVE in the National Vulnerability Database (NVD) is 6.1. jQuery is removed from Hyperion Financial Reporting with the January 2021 Critical Patch Update.

Additional CVEs addressed are:

- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-11984 also addresses CVE-2020-11993 and CVE-2020-9490.

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Insurance Applications. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-5421	Oracle Insurance Policy Administration	Architecture (Spring Framework)	HTTP	No	6.5	Network	High	Lo
CVE-2020-5421	Oracle Insurance Rules Palette	Architecture (Spring Framework)	HTTP	No	6.5	Network	High	Lo
CVE-2019-11358	Oracle Insurance Insbridge Rating and Underwriting	Framework Administrator IBFA (jQuery)	HTTP	Yes	6.1	Network	Low	No

Oracle Java SE Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Java SE. 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 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14803	Java SE, Java SE Embedded	Libraries	Multiple	Yes	5.3	Network	Low	None

Notes:

1. This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 5 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 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-1967	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure SEC (OpenSSL)	JDENET	Yes	7.5	Network	Low	No
CVE-2020-11022	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2020-11022	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech - Cloud (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2020-11022	JD Edwards EnterpriseOne Tools	Web Runtime (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2021-2052	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security	HTTP	Yes	5.8	Network	Low	No

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-1967 also addresses CVE-2019-1551.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 43 new security patches for Oracle MySQL. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-13871	MySQL Workbench	Workbench (SQLite)	MySQL Workbench	Yes	7.5	Network	Low	Nor
CVE-2019-10086	MySQL Enterprise Monitor	Service Manager (Apache Commons BeanUtils)	HTTPS	Yes	7.3	Network	Low	Nor
CVE-2021-2046	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	6.8	Network	Low	Hig
CVE-2020-5421	MySQL Enterprise Monitor	Service Manager (Spring Framework)	HTTPS	No	6.5	Network	High	Lo
CVE-2020-5408	MySQL Enterprise Monitor	Service Manager (Spring Security)	HTTPS	No	6.5	Network	Low	Lo
CVE-2021-2020	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2021-2024	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2021-2011	MySQL Client	C API	MySQL Protocol	Yes	5.9	Network	High	Nor
CVE-2020-1971	MySQL Workbench	MySQL Workbench (OpenSSL)	MySQL Workbench	Yes	5.9	Network	High	Nor
CVE-2021-2006	MySQL Client	C API	MySQL Protocol	No	5.3	Network	High	Lo
CVE-2021-2048	MySQL Server	InnoDB	MySQL Protocol	No	5.0	Network	High	Hig
CVE-2021-2028	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-2122	MySQL Server	Server: DDL	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2058	MySQL Server	Server: Locking	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2001	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2016	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2021	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2030	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2031	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2036	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2055	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2060	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2070	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2076	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2065	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2014	MySQL Server	Server: PAM Auth Plugin	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2002	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-2012	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2009	MySQL Server	Server: Security: Roles	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2072	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2081	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2022	MySQL Server	InnoDB	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2021-2038	MySQL Server	Server: Components Services	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2021-2061	MySQL Server	Server: DDL	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2021-2056	MySQL Server	Server: DML	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2021-2087	MySQL Server	Server: DML	MySQL Protocol	No	4.4	Local	Low	Hig
CVE-2021-2088	MySQL Server	Server: DML	MySQL Protocol	No	4.4	Local	Low	Hig
CVE-2021-2032	MySQL Server	Information Schema	MySQL Protocol	No	4.3	Network	Low	Lo
CVE-2021-2010	MySQL Client	C API	MySQL Protocol	No	4.2	Network	High	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-1998	MySQL Server	Server: Optimizer	MySQL Protocol	No	3.8	Network	Low	Hig
CVE-2021-2007	MySQL Client	C API	MySQL Protocol	Yes	3.7	Network	High	Nor
CVE-2021-2019	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	2.7	Network	Low	Hig
CVE-2021-2042	MySQL Server	InnoDB	MySQL Protocol	No	2.3	Local	Low	Hig

Additional CVEs addressed are:

- The patch for CVE-2020-13871 also addresses CVE-2020-11655, CVE-2020-11656, CVE-2020-15358 and CVE-2020-9327.
- The patch for CVE-2020-5408 also addresses CVE-2020-5407.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle PeopleSoft. 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 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2063	PeopleSoft Enterprise PeopleTools	Portal	None	No	8.4	Local	Low	None
CVE-2021-2071	PeopleSoft Enterprise PeopleTools	Elastic Search	HTTP	Yes	8.1	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-0227	PeopleSoft Enterprise HCM Human Resources	Global Payroll for Switzerland (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	None
CVE-2021-2044	PeopleSoft Enterprise FIN Payables	Financial Sanctions	HTTP	No	6.5	Network	Low	Low
CVE-2020-11022	PeopleSoft Enterprise HCM Human Resources	Company Dir / Org Chart Viewer, Employee Snapshot (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-2043	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	None
CVE-2020-9281	PeopleSoft Enterprise PeopleTools	Rich Text Editor (CKEditor)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-1968	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	3.7	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 32 new security patches for Oracle Retail Applications. 20 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-2020-10683	Oracle Retail Customer Management and Segmentation Foundation	Segment (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Retail Merchandising System	Foundation (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-9546	Oracle Retail Sales Audit	Rule Wizards (jackson-databind)	HTTP	Yes	9.8	Network	Low	
CVE-2020-1945	Oracle Retail Extract Transform and Load	Mathematical Operators (Apache Ant)	HTTP	Yes	9.1	Network	Low	
CVE-2020-5421	Oracle Retail Order Broker	System Administration (Spring Framework)	HTTP	No	8.8	Network	Low	
CVE-2017-8028	Oracle Retail Invoice Matching	Posting (Spring-LDAP)	HTTP	Yes	8.1	Network	High	
CVE-2020-5398	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2020-11979	Oracle Retail Financial Integration	PeopleSoft Integration (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Integration Bus	RIB Kernal (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2019-17566	Oracle Retail Integration Bus	RIB Kernal (Apache Batik)	HTTP	Yes	7.5	Network	Low	
CVE-2019-17566	Oracle Retail Order Broker	System Administration (Apache Batik)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-11979	Oracle Retail Service Backbone	RSB kernel (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Store Inventory Management	SIM Integration (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2019-10086	Oracle Retail Financial Integration	PeopleSoft Integration (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Integration Bus	RIB Kernal (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Order Broker	System Administration (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Service Backbone	RSB kernel (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2020-9484	Oracle Retail Order Broker	System Administration (Apache Tomcat)	None	No	7.0	Local	High	
CVE-2020-5421	Oracle Retail Assortment Planning	Application Core (Spring Framework)	HTTP	No	6.5	Network	High	
CVE-2020-5421	Oracle Retail Financial Integration	PeopleSoft Integration (Spring Framework)	HTTP	No	6.5	Network	High	
CVE-2020-5421	Oracle Retail Integration Bus	RIB Kernal (Spring Framework)	HTTP	No	6.5	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-5421	Oracle Retail Invoice Matching	Security (Spring Framework)	HTTP	No	6.5	Network	High	
CVE-2020-5421	Oracle Retail Service Backbone	RSB kernel (Spring Framework)	HTTP	No	6.5	Network	High	
CVE-2021-2057	Oracle Retail Customer Management and Segmentation Foundation	Internal Operations	HTTP	No	6.3	Network	Low	
CVE-2019-17091	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2020-13954	Oracle Retail Order Broker Cloud Service	Supplier Direct Fulfillment (Apache CXF)	HTTP	Yes	6.1	Network	Low	
CVE-2019-17091	Oracle Retail Store Inventory Management	SIM Integration (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	
CVE-2020-17521	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-17521	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-17521	Oracle Retail Integration Bus	RIB Kernal (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-17521	Oracle Retail Service Backbone	RSB kernel (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-9488	Oracle Retail Customer Management	Promotions (Apache Log4j)	HTTP	Yes	3.7	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	and Segmentation Foundation							

Additional CVEs addressed are:

- The patch for CVE-2020-1945 also addresses CVE-2017-5645.
- The patch for CVE-2020-5398 also addresses CVE-2020-5421.
- The patch for CVE-2020-9546 also addresses CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-11619, CVE-2020-11620, CVE-2020-9547 and CVE-2020-9548.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Siebel CRM. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2039	Siebel Core - Server Framework	Search	HTTP	No	7.6	Network	Low	Low
CVE-2020-9484	Siebel UI Framework	EAI (Apache Tomcat)	None	No	7.0	Local	High	Low
CVE-2020-11022	Siebel Mobile App	Open UI (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-2004	Siebel Core - Server BizLogic Script	Integration - Scripting	HTTP	No	4.3	Network	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-9484 also addresses CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-1935 and CVE-2020-9488.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 11 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 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2021-2102	Oracle Complex Maintenance, Repair, and Overhaul	Dialog Box	HTTP	Yes	8.2	Network	Low	Nor
CVE-2021-2103	Oracle Complex Maintenance, Repair, and Overhaul	Dialog Box	HTTP	Yes	8.2	Network	Low	Nor
CVE-2021-2104	Oracle Complex Maintenance, Repair, and Overhaul	Dialog Box	HTTP	Yes	8.2	Network	Low	Nor
CVE-2021-2078	Oracle Configurator	UI Servlet	HTTP	Yes	8.2	Network	Low	Nor
CVE-2021-2079	Oracle Configurator	UI Servlet	HTTP	Yes	8.2	Network	Low	Nor
CVE-2021-2080	Oracle Configurator	UI Servlet	HTTP	Yes	8.2	Network	Low	Nor
CVE-2020-14195	Oracle Agile PLM	Security (jackson-databind)	HTTP	Yes	8.1	Network	High	Nor
CVE-2019-17563	Oracle Agile Engineering	Install (Apache	HTTP	Yes	7.5	Network	High	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
	Data Management	Tomcat)						
CVE-2020-9281	Oracle Agile PLM	Security (CKEditor)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-11358	Oracle Agile Product Lifecycle Management for Process	Installation (jQuery)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2019-11358	Oracle Transportation Management	Install (jQuery)	HTTP	Yes	6.1	Network	Low	Nor

Additional CVEs addressed are:

- The patch for CVE-2019-11358 also addresses CVE-2020-11022 and CVE-2020-11023.
- The patch for CVE-2019-17563 also addresses CVE-2019-17569, CVE-2020-1935, CVE-2020-1938 and CVE-2020-9484.
- The patch for CVE-2020-14195 also addresses CVE-2020-10650, CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-14060, CVE-2020-14061, CVE-2020-14062, CVE-2020-24616, CVE-2020-24750, CVE-2020-9546, CVE-2020-9547 and CVE-2020-9548.

Oracle Systems Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Systems. 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 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-11984	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	9.8	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-11022	StorageTek Tape Analytics SW Tool	Software (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-1999	Oracle ZFS Storage Appliance Kit	RAS subsystems	None	No	5.0	Local	High	High
CVE-2020-9488	StorageTek Tape Analytics SW Tool	Software (Apache Log4j)	HTTP	Yes	3.7	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-11984 also addresses CVE-2018-20781, CVE-2019-11135, CVE-2019-20892, CVE-2019-20907, CVE-2020-11985, CVE-2020-11993, CVE-2020-13254, CVE-2020-13596, CVE-2020-13871, CVE-2020-14422, CVE-2020-15025, CVE-2020-15358, CVE-2020-17498, CVE-2020-24583, CVE-2020-24584, CVE-2020-25862, CVE-2020-25863, CVE-2020-25866, CVE-2020-26575, CVE-2020-9490 and CVE-2021-1999.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Utilities Applications. 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 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2555	Oracle Utilities Framework	General (Oracle Coherence)	HTTP	Yes	9.8	Network	Low	None	

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 17 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 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2021-2074	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	N
CVE-2021-2129	Oracle VM VirtualBox	Core	None	No	7.9	Local	Low	High	N
CVE-2021-2128	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	N
CVE-2021-2086	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2111	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2112	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2121	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2124	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2119	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2021-2120	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2126	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2131	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	N
CVE-2021-2125	Oracle VM VirtualBox	Core	None	No	4.6	Local	Low	High	N
CVE-2021-2073	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	N
CVE-2021-2127	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	N
CVE-2021-2130	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	N
CVE-2021-2123	Oracle VM VirtualBox	Core	None	No	3.2	Local	Low	High	N