Oracle Critical Patch Update Advisory - April 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 391 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 April 2021 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite, versions 3.5, 3.6	Oracle Supply Chain Products
Agile Product Lifecycle Management Integration Pack for SAP: Design to Release, versions 3.5, 3.6	Oracle Supply Chain Products

Affected Products and Versions	Patch Availability Document
Enterprise Manager Base Platform, version 13.4.0.0	Enterprise Manager
Enterprise Manager for Fusion Middleware, versions 12.2.1.4, 13.4.0.0	Enterprise Manager
Enterprise Manager for Virtualization, version 13.4.0.0	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
FMW Platform, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Hyperion Analytic Provider Services, versions 11.1.2.4, 12.2.1.4	Fusion Middleware
Hyperion Financial Management, version 11.1.2.4	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineering Sui
JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.5.3	JD Edwards
JD Edwards EnterpriseOne Tools, versions prior to 9.2.4.0, prior to 9.2.5.3	JD Edwards
JD Edwards World Security, version A9.4	JD Edwards
MySQL Cluster, versions 8.0.23 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.23 and prior	MySQL
MySQL Server, versions 5.7.33 and prior, 8.0.23 and prior	MySQL
MySQL Workbench, versions 8.0.23 and prior	MySQL
Oracle Advanced Supply Chain Planning, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Agile PLM, versions 9.3.3, 9.3.5, 9.3.6	Oracle Supply Chain Products
Oracle API Gateway, version 11.1.2.4.0	Fusion Middleware
Oracle Application Express, versions prior to 20.2	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle BAM (Business Activity Monitoring), versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Banking Platform, versions 2.4.0, 2.6.2, 2.7.0, 2.7.1, 2.8.0, 2.9.0, 2.10.0	Oracle Banking Platform
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 Cloud Infrastructure Storage Gateway, versions prior to 1.4	Contact Support
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

Affected Products and Versions	Patch Availability Document
Oracle Commerce Guided Search, versions 11.3.0, 11.3.1, 11.3.2	Oracle Commerce
Oracle Commerce Merchandising, versions 0, 11.0.0, 11.1, 11.2.0, 11.3.0, 11.3.1, 11.3.2	Oracle Commerce
Oracle Communications Application Session Controller, version 3.9m0p3	Oracle Communications Application Sess Controller
Oracle Communications Calendar Server, version 8.0	Oracle Communications Calendar Server
Oracle Communications Contacts Server, version 8.0	Oracle Communications Contacts Server
Oracle Communications Converged Application Server - Service Controller, version 6.2	Oracle Communications Converged Application Server - Service Controller
Oracle Communications Design Studio, version 7.4.2	Oracle Communications Design Studio
Oracle Communications Interactive Session Recorder, versions 6.3, 6.4	Oracle Communications Interactive Sessi Recorder
Oracle Communications Messaging Server, versions 8.0.2, 8.1, 8.1.0	Oracle Communications Messaging Serv
Oracle Communications MetaSolv Solution, versions 6.3.0, 6.3.1	Oracle Communications MetaSolv Soluti
Oracle Communications Performance Intelligence Center Software, versions 10.4.0.2, 10.4.0.3	Oracle Communications Performance Intelligence Center (PIC) Software
Oracle Communications Services Gatekeeper, versions 6.0, 6.1, 7.0	Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller, versions Cz8.2, Cz8.3, Cz8.4	Oracle Communications Session Border Controller
Oracle Communications Session Router, versions Cz8.2, Cz8.3, Cz8.4	Oracle Communications Session Router
Oracle Communications Subscriber-Aware Load Balancer, versions Cz8.2, Cz8.3, Cz8.4	Oracle Communications Subscriber-Awa Load Balancer
Oracle Communications Unified Inventory Management, versions 7.3.4, 7.3.5, 7.4.0, 7.4.1	Oracle Communications Unified Inventor Management
Oracle Communications Unified Session Manager, version SCz8.2.5	Oracle Communications Unified Session Manager
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 Studio, version 3.2.0.0	Fusion Middleware
Oracle Enterprise Communications Broker, versions PCZ3.1, PCZ3.2, PCZ3.3	Oracle Enterprise Communications Broke

Affected Products and Versions	Patch Availability Document
Oracle Enterprise Repository, version 11.1.1.7.0	Fusion Middleware
Oracle Enterprise Session Border Controller, versions Cz8.2, Cz8.3, Cz8.4	Oracle Enterprise Session Border Control
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.0	Oracle Financial Services Analytical Applications Infrastructure
Oracle FLEXCUBE Direct Banking, versions 12.0.2, 12.0.3	Contact Support
Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0	Contact Support
Oracle Fusion Middleware, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Fusion Middleware MapViewer, version 12.2.1.4.0	Fusion Middleware
Oracle Global Lifecycle Management OPatch, versions prior to 12.2.0.1.22	Global Lifecycle Management
Oracle GraalVM Enterprise Edition, versions 19.3.5, 20.3.1.2, 21.0.0.2	Oracle GraalVM Enterprise Edition
Oracle Graph Server and Client	Database
Oracle Health Sciences Empirica Signal, versions 9.0, 9.1	Health Sciences
Oracle Health Sciences Information Manager, versions 3.0.0-3.0.2	Health Sciences
Oracle Healthcare Foundation, versions 7.1.5, 7.2.2, 7.3.0, 7.3.1, 8.0.1	Health Sciences
Oracle Hospitality Cruise Shipboard Property Management System, version 20.1.0	Oracle Hospitality Cruise Shipboard Prop Management System
Oracle Hospitality Inventory Management, version 9.1.0	Oracle Hospitality Inventory Managemer
Oracle Hospitality OPERA 5, versions 5.5, 5.6	Oracle Hospitality OPERA 5 Property Services
Oracle Hospitality RES 3700, versions 5.7.0-5.7.6	Oracle Hospitality RES
Oracle HTTP Server, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Identity Manager Connector, version 11.1.1.5.0	Fusion Middleware
Oracle iLearning, versions 6.2, 6.3	iLearning
Oracle Insurance Data Gateway, version 1.0.2.3	Oracle Insurance Applications
Oracle Java SE, versions 7u291, 8u281, 11.0.10, 16	Java SE
Oracle Java SE Embedded, version 8u281	Java SE
Oracle NoSQL Database, versions prior to 20.3	NoSQL Database
Oracle Outside In Technology, version 8.5.5	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Platform Security for Java, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Rapid Planning, version 12.1.3	Oracle Supply Chain Products
Oracle REST Data Services, versions prior to 20.4.3.50.1904	Database
Oracle Retail Advanced Inventory Planning, version 14.1	Retail Applications
Oracle Retail Assortment Planning, version 16.0.3	Retail Applications
Oracle Retail Back Office, version 14.1	Retail Applications
Oracle Retail Category Management Planning & Optimization, version 16.0.3	Retail Applications
Oracle Retail Central Office, version 14.1	Retail Applications
Oracle Retail EFTLink, versions 15.0.2, 16.0.3, 17.0.2, 18.0.1, 19.0.1, 20.0.0	Retail Applications
Oracle Retail Insights Cloud Service Suite, version 19.0	Retail Applications
Oracle Retail Item Planning, version 16.0.3	Retail Applications
Oracle Retail Macro Space Optimization, version 16.0.3	Retail Applications
Oracle Retail Merchandise Financial Planning, version 16.0.3	Retail Applications
Oracle Retail Merchandising System, version 16.0.3	Retail Applications
Oracle Retail Point-of-Service, version 14.1	Retail Applications
Oracle Retail Predictive Application Server, versions 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Regular Price Optimization, version 16.0.3	Retail Applications
Oracle Retail Replenishment Optimization, version 16.0.3	Retail Applications
Oracle Retail Returns Management, version 14.1	Retail Applications
Oracle Retail Sales Audit, version 14.0	Retail Applications
Oracle Retail Size Profile Optimization, version 16.0.3	Retail Applications
Oracle Retail Store Inventory Management, versions 14.1.3.10, 15.0.3.5, 16.0.3.5	Retail Applications
Oracle Retail Xstore Point of Service, versions 15.0.4, 16.0.6, 17.0.4, 18.0.3, 19.0.2	Retail Applications
Oracle SD-WAN Aware, version 8.2	Oracle SD-WAN Aware
Oracle SD-WAN Edge, versions 8.2, 9.0	Oracle SD-WAN Edge
Oracle Secure Backup	Oracle Secure Backup

Affected Products and Versions	Patch Availability Document
Oracle Secure Global Desktop, version 5.6	Virtualization
Oracle Security Service, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Service Bus, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Solaris, versions 10, 11	Systems
Oracle Spatial Studio, versions prior to 19.1.0, prior to 20.1.1	Database
Oracle SQL Developer, versions prior to 20.4.1.407.6	Database
Oracle Storage Cloud Software Appliance, versions prior to 16.3.1.4.2	Contact Support
Oracle TimesTen In-Memory Database	Database
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, 4.4.0.3.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.20	Virtualization
Oracle WebCenter Portal, 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 WebLogic Server Proxy Plug-In, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
OSS Support Tools, versions prior to 2.12.41	Support Tools
PeopleSoft Enterprise CS Campus Community, version 9.2	PeopleSoft
PeopleSoft Enterprise FIN Common Application Objects, version 9.2	PeopleSoft
PeopleSoft Enterprise FIN Expenses, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft
PeopleSoft Enterprise PT PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft
PeopleSoft Enterprise SCM eProcurement, version 9.2	PeopleSoft
PeopleSoft Enterprise SCM Purchasing, version 9.2	PeopleSoft
Primavera Gateway, versions 17.12.0-17.12.10	Oracle Construction and Engineering Sui
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12, 20.12	Oracle Construction and Engineering Sui
Siebel Applications, versions 21.2 and prior	Siebel

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 that 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:

- 0xfoxone: CVE-2021-2240
- Alessandra Zullo: CVE-2021-2152
- Andrej Simko of Accenture: CVE-2021-2150, CVE-2021-2155, CVE-2021-2182, CVE-2021-2183, CVE-2021-2184, CVE-2021-2185, CVE-2021-2186, CVE-2021-2187, CVE-2021-2188, CVE-2021-2189, CVE-2021-2190, CVE-2021-2195, CVE-2021-2198, CVE-2021-2199, CVE-2021-2200
- Aobo Wang of Chaitin Security Research Lab: CVE-2021-2312
- Artur Obuchowski and Jakub Sajniak of STM Cyber: CVE-2021-2053
- Bartłomiej Stasiek: CVE-2021-2218, CVE-2021-2219, CVE-2021-2220
- Billy Jheng Bing-Jhong (st424204) working with Trend Micro Zero Day Initiative: CVE-2021-2250, CVE-2021-2321
- Calvin Fong (Lord_Idiot) of STAR Labs working with Trend Micro Zero Day Initiative: CVE-2021-2250, CVE-2021-2321
- Charley Celice of Quorum Cyber: CVE-2021-2214
- ChenNan of Chaitin Security Research Lab: CVE-2021-2280, CVE-2021-2281, CVE-2021-2282, CVE-2021-2283, CVE-2021-2284, CVE-2021-2285, CVE-2021-2286, CVE-2021-2287, CVE-2021-2306
- Cl0und of Syclover Security Team: CVE-2021-2135, CVE-2021-2136
- Codeplutos of AntGroup FG Security Lab: CVE-2021-2135
- Damian Bury: CVE-2021-2140
- DongJun Shin working with Trend Micro Zero Day Initiative: CVE-2021-2309
- Emad Al-Mousa of Saudi Aramco: CVE-2021-2173, CVE-2021-2175, CVE-2021-2207
- Esteban Montes Morales of Accenture: CVE-2021-2181
- Ghost Said: CVE-2021-2204
- Girlelecta: CVE-2021-2242

- JungHyun Kim (jidoc01) of VirtualBoBs working with Trend Micro Zero Day Initiative: CVE-2021-2279, CVE-2021-2291
- JunYoung Park (candymate) of VirtualBoBs working with Trend Micro Zero Day Initiative: CVE-2021-2266
- Kajetan Rostojek: CVE-2021-2191
- Kun Yang of Chaitin Security Research Lab: CVE-2021-2280, CVE-2021-2281, CVE-2021-2282, CVE-2021-2283, CVE-2021-2284, CVE-2021-2285, CVE-2021-2286, CVE-2021-2287, CVE-2021-2306, CVE-2021-2312
- Longofo of Knownsec 404 Team: CVE-2021-2211, CVE-2021-2277, CVE-2021-2294
- Lucas Leong (wmliang) of Trend Micro Zero Day Initiative: CVE-2021-2296, CVE-2021-2297
- Markus Loewe: CVE-2021-2161
- Martin Neumann of Accenture: CVE-2021-2205, CVE-2021-2206, CVE-2021-2209, CVE-2021-2210
- Martí Guasch Jimenez: CVE-2021-2167
- Matthias Gerstner of SUSE: CVE-2021-2264
- Matthias Kaiser of Apple Information Security: CVE-2021-2135
- Max Van Amerongen (maxpl0it) working with Trend Micro Zero Day Initiative: CVE-2021-2145, CVE-2021-2310
- Maxime Escourbiac of Michelin CERT: CVE-2021-2153
- Michał Skowron: CVE-2021-2219
- Muhammad Alifa Ramdhan (n0psledbyte) working with Trend Micro Zero Day Initiative: CVE-2021-2250, CVE-2021-2321
- Okan Cokun of Biznet: CVE-2021-2008
- Patrick Star of BMH Security Team: CVE-2021-2204
- peterjson of RedTeam@VNG Corporation working with Trend Micro Zero Day Initiative: CVE-2021-2244
- Quynh Le of VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2021-2211, CVE-2021-2302, CVE-2021-2303
- r00t4dm at Cloud-Penetrating Arrow Lab: CVE-2021-2211, CVE-2021-2277, CVE-2021-2294
- Spyridon Chatzimichail of OTE Hellenic Telecommunications Organization S.A.: CVE-2021-2158
- thiscodecc of MoyunSec V-Lab: CVE-2021-2211, CVE-2021-2277, CVE-2021-2294
- threedr3am: CVE-2021-2136
- Tomasz Wiśniewski: CVE-2021-2219
- Torben Capiau of Accenture: CVE-2021-2197

- UnicodeSec potats0: CVE-2021-2211
- Venustech ADLab: CVE-2021-2135
- Veronica Venturi: CVE-2021-2152
- Waleed Ezz Eldin of Cysiv (Previously SecureMisr): CVE-2021-2141
- Wei Bo of UGUARDSEC Security Team: CVE-2021-2157
- Will Dormann of CERT/CC: CVE-2021-2307
- Xianglai Liu of Dbappsecurity Team: CVE-2021-2277
- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2021-2169, CVE-2021-2230
- Yi Ren of Alibaba: CVE-2021-2203
- Yuyue Wang of Alibaba: CVE-2021-2203

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:

- Artem
- Markus Loewe
- Mohit Rawat
- Ofir Moskovitch

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:

- Abdulaziz Almisfer
- Abhishek Misal

- Aditra Andri Laksana
- Adrián Pedrazzoli
- Ali Hassan Ghori
- Ankur Vaidya
- Aswin Krishna (733n_wolf)
- Aurélien Salomon
- Bader Almutairi
- Danish Tariq
- Derek Chapman
- George Crook
- Hamit Cibo
- Jehad Alqurashi
- Luca Ottoni
- Mohamed Ahmed Naji
- Mohamed ELobeid
- Qasim Shaikh
- Rahul PS
- Reworr
- Srikar V - exp1o1t9r
- Waleed Ezz Eldin of Cysiv (Previously SecureMisr) [2 reports]
- Yevgeny Zharovsky

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 July 2021
- 19 October 2021
- 18 January 2022
- 19 April 2022

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins

- Critical Patch Update - April 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
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2021-September-4	Rev 7. Removed CVE-2021-21345 from the additional CVE list of BAM.
2021-July-28	Rev 6. Removed Oracle Weblogic Server version 12.1.3.0.0 for CVE-2021-2135.
2021-June-29	Rev 5. Affected version changes to CVE-2020-10683 in the Fusion Middleware Matr
2021-May-5	Rev 4. Added CVE-2019-17638 to the Fusion Middleware Matrix for Weblogic Server and it is CVSS 0.
2021-April-26	Rev 3. Added CVE-2021-2321 to the Virtualization risk matrix and updated the Credi Statement section.
2021-April-22	Rev 2. Affected version changed for CVE-2021-2008, Note added for CVE-2021-226 Database matrix client-only updated.
2021-April-20	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 18 new security patches for Oracle Database Products divided as follows:

- 10 new security patches for Oracle Database Products
- 1 new security patch for Oracle Global Lifecycle Management
- No new security patches for Oracle Graph Server and Client, but third party patches are provided
- 4 new security patches for Oracle NoSQL Database
- 1 new security patch for Oracle REST Data Services

- No new security patches for Oracle Secure Backup, but third party patches are provided
- 2 new security patches for Oracle Spatial Studio
- No new security patches for Oracle TimesTen In-Memory Database, but third party patches are provided

Oracle Database Server Risk Matrix

This Critical Patch Update contains 10 new security patches plus additional third party patches noted below for Oracle Database Products. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 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 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-5360	Oracle Database - Enterprise Edition Security (Dell BSAFE Micro Edition Suite)	None	Multiple	Yes	7.5	Network	Low	None
CVE-2020-17527	Workload Manager (Apache Tomcat)	None	HTTP	Yes	7.5	Network	Low	None
CVE-2019-3740	Oracle Database - Enterprise Edition (Dell BSAFE Crypto-J)	None	Oracle Net	Yes	6.5	Network	Low	None
CVE-2020-11023	Oracle Application Express (jQuery)	None	HTTP	Yes	6.1	Network	Low	None
CVE-2021-2234	Java VM	Create Session	Oracle Net	No	5.3	Network	High	Low

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2020-7760	Oracle Application Express (CodeMirror)	Valid User Account	HTTP	No	4.3	Network	Low	Low	
CVE-2021-2173	Recovery	DBA Level Account	Oracle Net	No	4.1	Network	Low	High	
CVE-2021-2175	Database Vault	Create Any View, Select Any View	Oracle Net	No	2.7	Network	Low	High	
CVE-2021-2245	Oracle Database - Enterprise Edition Unified Audit	Create Audit Policy	Oracle Net	No	2.7	Network	Low	High	
CVE-2021-2207	Oracle Database - Enterprise Edition	RMAN executable	Local Logon	No	2.3	Local	Low	High	

Additional CVEs addressed are:

- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739.
- The patch for CVE-2020-11023 also addresses CVE-2019-11358 and CVE-2020-11022.
- The patch for CVE-2020-17527 also addresses CVE-2020-13943 and CVE-2020-9484.
- The patch for CVE-2020-5360 also addresses CVE-2020-5359.

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

- Oracle Database Configuration Assistant (Apache Commons Compress): CVE-2019-12402.

Oracle Database Server Client-Only Installations:

- The following Oracle Database Server Vulnerability included in the Critical Patch Update affects client-only installations: CVE-2020-5360.

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle Global Lifecycle Management. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-3740	Oracle Global Lifecycle Management OPatch	Patch Installer (Dell BSAFE Crypto-J)	Oracle Net	Yes	6.5	Network	Low	None

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.
  - Patch Installer (jackson-databind): CVE-2020-36189, CVE-2020-14195 and CVE-2020-25649.

Oracle Graph Server and Client Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Graph Server and Client. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for the Oracle Graph Server and Client. 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 Mat					
					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 Graph Server and Client
    - Packaging/Install (lodash): CVE-2020-8203.

Oracle NoSQL Database Risk Matrix

This Critical Patch Update contains 4 new security patches plus additional third party patches noted below for Oracle NoSQL Database. 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-2020-13956	Oracle NoSQL Database	Administration (Apache HttpClient)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-11612	Oracle NoSQL Database	Administration (Netty)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-22883	Oracle NoSQL Database	Administration (Node.js)	Multiple	Yes	7.5	Network	Low	None
CVE-2020-8908	Oracle NoSQL Database	Administration (Google Guava)	Local Logon	No	3.3	Local	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2020-11612 also addresses CVE-2021-21290.
- The patch for CVE-2021-22883 also addresses CVE-2021-22884 and CVE-2021-23840.

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

- Oracle NoSQL Database
    - Administration (Go): CVE-2020-24553.

- Administration (jackson-databind): CVE-2019-14379, CVE-2019-12086, CVE-2019-16942, CVE-2020-14195, CVE-2020-24616, CVE-2020-24750, CVE-2020-25649 and CVE-2020-36189.

Oracle REST Data Services Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle REST Data Services. 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	U Int
CVE-2020-27223	Oracle REST Data Services	General (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	None	N

Additional CVEs addressed are:

- The patch for CVE-2020-27223 also addresses CVE-2020-27218.

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

- Oracle REST Data Services
  - General (jackson-databind): CVE-2019-14379, CVE-2019-12086, CVE-2019-16942, CVE-2020-14060, CVE-2020-14061, CVE-2020-14062, CVE-2020-14195, CVE-2020-24750, CVE-2020-25649 and CVE-2020-36189.

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 Mat					
					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
  - Install (Flexera InstallShield): CVE-2016-2542.
  - Oracle Secure Backup (PHP): CVE-2020-7060, CVE-2020-7059 and CVE-2020-7069.

Oracle Spatial Studio Risk Matrix

This Critical Patch Update contains 2 new security patches plus additional third party patches noted below for Oracle Spatial Studio. 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-2020-13956	Oracle Spatial Studio	Install (Apache HttpClient)	HTTP	Yes	5.3	Network	Low	None	N
CVE-2020-7760	Oracle Spatial Studio	Install (CodeMirror)	HTTP	No	4.3	Network	Low	Low	N

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

- Oracle Spatial Studio
  - Install (Apache POI): CVE-2019-12415.
  - Install (jackson-databind): CVE-2020-36189, CVE-2019-12086, CVE-2020-14195, CVE-2020-24750, CVE-2020-25649, CVE-2020-35490, CVE-2020-35491, CVE-2020-35728,

CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187 and CVE-2020-36188.

Oracle SQL Developer Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle SQL Developer. 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	
CVE-2020-13956	Oracle SQL Developer (Apache HttpClient)	Install (Apache HttpClient)	HTTP	Yes	7.5	Network	Low	None	

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

- Oracle SQL Developer
  - General Infrastructure (Bootstrap): CVE-2019-8331, CVE-2018-14040, CVE-2018-14041 and CVE-2018-14042.
  - General Infrastructure (jQuery): CVE-2020-11023, CVE-2019-11358 and CVE-2020-11022.
  - Install (Apache Kafka): CVE-2019-12399.
  - Install (Apache Log4j): CVE-2020-9488.
  - Install (dom4j): CVE-2018-1000632.
  - NoSQL Extension (jackson-databind): CVE-2020-25649.
- Oracle SQL Developer Install
  - Install (Apache POI): CVE-2019-12415.

Oracle TimesTen In-Memory Database Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle TimesTen In-Memory Database. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle TimesTen In-Memory Database. 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 TimesTen In-Memory Database
  - Install (Go): CVE-2020-24553, CVE-2020-14039, CVE-2020-15586, CVE-2020-16845 and CVE-2020-7919.
  - Install (Perl): CVE-2020-10878 and CVE-2020-12723.
  - Kubernetes Operator (Go): CVE-2020-24553, CVE-2020-14039, CVE-2020-15586, CVE-2020-16845 and CVE-2020-7919.

Oracle Commerce Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Commerce. 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 Req
CVE-2019-12423	Oracle Commerce Guided Search	Content Acquisition System (Apache CXF)	HTTP	Yes	7.5	Network	Low	Non
CVE-2020-11022	Oracle Commerce Guided Search	Workbench, Experience Manager (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2020-11022	Oracle Commerce Merchandising	Business Control Center (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2020-27193	Oracle Commerce Merchandising	Experience Manager, Business Control Center (CKEditor)	HTTP	Yes	6.1	Network	Low	Non

Additional CVEs addressed are:

- The patch for CVE-2019-12423 also addresses CVE-2019-12406, CVE-2019-1241, CVE-2019-12419 and CVE-2019-17573.
- The patch for CVE-2020-11022 also addresses CVE-2019-11358 and CVE-2020-11023.
- The patch for CVE-2020-27193 also addresses CVE-2020-9281.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 13 new security patches for Oracle Communications Applications. 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			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-11612	Oracle Communications Design Studio	Inventory Services (Netty)	HTTP	Yes	9.8	Network	Low	
CVE-2019-0228	Oracle Communications Messaging Server	Message Store (Apache PDFBox)	HTTP	Yes	9.8	Network	Low	
CVE-2020-11612	Oracle Communications Messaging Server	Message Store (Netty)	HTTP	Yes	9.8	Network	Low	
CVE-2020-28052	Oracle Communications Messaging Server	Message Store (Bouncy Castle Java Library)	HTTPS	Yes	9.8	Network	Low	
CVE-2020-5421	Oracle Communications Unified Inventory Management	Reservations (Spring Framework)	HTTP	No	8.8	Network	Low	
CVE-2020-24750	Oracle Communications Calendar Server	Event Reminders (jackson-databind)	HTTP	Yes	8.1	Network	High	
CVE-2020-24750	Oracle Communications Contacts Server	Contact Sharing (jackson-databind)	HTTP	Yes	8.1	Network	High	
CVE-2020-24750	Oracle Communications Messaging Server	Security (jackson-databind)	HTTP	Yes	8.1	Network	High	
CVE-2020-13871	Oracle Communications Messaging Server	Message Store (SQLite)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Communications Unified	Security Component	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Inventory Management	(Apache Ant)						
CVE-2019-10086	Oracle Communications Unified Inventory Management	Inventory Group (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2020-13954	Oracle Communications Messaging Server	Message Store (Apache CXF)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11987	Oracle Communications MetaSolv Solution	Planning and Modeling (Apache Batik)	HTTP	Yes	5.3	Network	Low	

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-2020-13954 also addresses CVE-2020-25649, CVE-2020-28052 and CVE-2020-36189.
- The patch for CVE-2020-24750 also addresses CVE-2020-24616.
- The patch for CVE-2020-28052 also addresses CVE-2020-13954, CVE-2020-25649 and CVE-2020-36189.

Oracle Communications Risk Matrix

This Critical Patch Update contains 22 new security patches for Oracle Communications. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-28052	Oracle Communications Application Session Controller	Security (Bouncy Castle Java Library)	HTTPS	Yes	9.8	Network	Low	
CVE-2021-22112	Oracle Communications Interactive Session Recorder	Provision API (Spring Security)	HTTP	No	8.8	Network	Low	
CVE-2020-10188	Oracle Communications Performance Intelligence Center Software	Mediation server (Telnet)	Telnet	No	8.3	Network	Low	
CVE-2020-25649	Oracle Communications Interactive Session Recorder	Provision API (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2020-1971	Oracle Communications Session Border Controller	Routing (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2020-25649	Oracle SD-WAN Edge	Config (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2020-17527	Oracle SD-WAN Edge	MGMT (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	
CVE-2019-10086	Oracle Communications Performance Intelligence Center Software	PMAC (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2020-8203	Oracle Communications Session Border Controller	Routing (Lodash)	HTTP	No	6.4	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-8203	Oracle Communications Session Router	Routing (Lodash)	HTTP	No	6.4	Network	High	
CVE-2020-8203	Oracle Communications Subscriber-Aware Load Balancer	Routing (Lodash)	HTTP	No	6.4	Network	High	
CVE-2020-8203	Oracle Enterprise Communications Broker	Routing (Lodash)	HTTP	No	6.4	Network	High	
CVE-2019-3900	Oracle SD-WAN Edge	OS (Linux Kernel)	Multiple	No	6.3	Network	High	
CVE-2020-1927	Oracle SD-WAN Aware	OS (Linux Kernel)	Multiple	Yes	6.1	Network	Low	I
CVE-2020-17521	Oracle Communications Services Gatekeeper	PRM (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-11987	Oracle Communications Application Session Controller	Security (Apache Batik)	HTTP	Yes	5.3	Network	Low	I
CVE-2020-27218	Oracle Communications Converged Application Server - Service Controller	SC Admin server (Eclipse Jetty)	HTTP	Yes	4.8	Network	High	I
CVE-2020-1971	Oracle Communications Session Router	Routing (OpenSSL)	TLS	No	4.2	Network	High	
CVE-2020-1971	Oracle Communications Subscriber-Aware Load Balancer	Routing (OpenSSL)	TLS	No	4.2	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-1971	Oracle Communications Unified Session Manager	Routing (OpenSSL)	TLS	No	4.2	Network	High	
CVE-2020-1971	Oracle Enterprise Communications Broker	Routing (OpenSSL)	TLS	No	4.2	Network	High	
CVE-2020-1971	Oracle Enterprise Session Border Controller	Routing (OpenSSL)	TLS	No	4.2	Network	High	

Additional CVEs addressed are:

- The patch for CVE-2019-3900 also addresses CVE-2018-14613, CVE-2018-16884, CVE-2019-10638, CVE-2019-10639, CVE-2019-11487, CVE-2019-11599, CVE-2019-14898, CVE-2019-15218, CVE-2019-16746, CVE-2019-17075, CVE-2019-17133, CVE-2019-18885, CVE-2019-19052, CVE-2019-19063, CVE-2019-19066, CVE-2019-19073, CVE-2019-19074, CVE-2019-19078, CVE-2019-19535, CVE-2019-19922, CVE-2019-20812, CVE-2019-3874, CVE-2019-5108, CVE-2020-10751, CVE-2020-10769, CVE-2020-12114, CVE-2020-12771, CVE-2020-16166 and CVE-2020-24394.
- The patch for CVE-2020-1927 also addresses CVE-2019-10098.
- The patch for CVE-2020-25649 also addresses CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188 and CVE-2020-36189.
- The patch for CVE-2020-27218 also addresses CVE-2020-27216.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Construction and Engineering. 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-2019-0219	Instantis EnterpriseTrack	Browser (Apache Cordova InAppBrowser)	HTTP	Yes	9.8	Network	Low
CVE-2020-17527	Instantis EnterpriseTrack	WebServer (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2020-11022	Primavera Unifier	Core UI (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2016-5725	Primavera Gateway	Admin (JCraft JSch)	HTTP	Yes	5.9	Network	High
CVE-2020-17521	Primavera Gateway	Admin (Apache Groovy)	None	No	5.5	Local	Low
CVE-2020-17521	Primavera Unifier	Platform (Apache Groovy)	None	No	5.5	Local	Low
CVE-2020-11987	Instantis EnterpriseTrack	Dashboards and Reports (Apache Batik)	HTTP	Yes	5.3	Network	Low
CVE-2020-13956	Primavera Unifier	Core (HTTP Client)	HTTP	Yes	5.3	Network	Low

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 70 new security patches plus additional third party patches noted below for Oracle E-Business Suite. 22 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 April 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 (April 2021), My Oracle Support Note 2759182.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2200	Oracle Applications Framework	Home page	HTTP	Yes	9.1	Network	Low	N
CVE-2021-2205	Oracle Marketing	Marketing Administration	HTTP	Yes	9.1	Network	Low	N
CVE-2021-2209	Oracle Email Center	Message Display	HTTP	No	8.5	Network	Low	L
CVE-2021-2182	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2183	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2184	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2185	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2186	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2187	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2188	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2197	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2150	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2199	Oracle iStore	Shopping Cart	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2198	Oracle Knowledge Management	Setup, Admin	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2195	Oracle Partner Management	Attribute Admin Setup	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2206	Oracle Trade Management	Quotes	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2210	Oracle Trade Management	Quotes	HTTP	Yes	8.2	Network	Low	N
CVE-2021-2247	Oracle Advanced Collections	Admin	HTTP	No	8.1	Network	Low	L
CVE-2021-2269	Oracle Advanced Pricing	Price Book	HTTP	No	8.1	Network	Low	L
CVE-2021-2314	Oracle Application Object Library	Profiles	HTTP	No	8.1	Network	Low	L
CVE-2021-2222	Oracle Bill Presentment Architecture	Template Search	HTTP	No	8.1	Network	Low	L
CVE-2021-2288	Oracle Bills of Material	Bill Issues	HTTP	No	8.1	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2227	Oracle Cash Management	Bank Account Transfer	HTTP	No	8.1	Network	Low	l
CVE-2021-2224	Oracle Compensation Workbench	Compensation Workbench	HTTP	No	8.1	Network	Low	l
CVE-2021-2295	Oracle Concurrent Processing	BI Publisher Integration	HTTP	No	8.1	Network	Low	l
CVE-2021-2251	Oracle CRM Technical Foundation	Data Source	HTTP	No	8.1	Network	Low	l
CVE-2021-2156	Oracle Customers Online	Customer Tab	HTTP	No	8.1	Network	Low	l
CVE-2021-2229	Oracle Depot Repair	LOVs	HTTP	No	8.1	Network	Low	l
CVE-2021-2292	Oracle Document Management and Collaboration	Document Management	HTTP	No	8.1	Network	Low	l
CVE-2021-2225	Oracle E-Business Intelligence	DBI Setups	HTTP	No	8.1	Network	Low	l
CVE-2021-2274	Oracle E-Business Tax	User Interface	HTTP	No	8.1	Network	Low	l
CVE-2021-2290	Oracle Engineering	Change Management	HTTP	No	8.1	Network	Low	l
CVE-2021-2233	Oracle Enterprise Asset Management	Setup	HTTP	No	8.1	Network	Low	l
CVE-2021-2236	Oracle Financials Common Modules	Advanced Global Intercompany	HTTP	No	8.1	Network	Low	l

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2237	Oracle General Ledger	Account Hierarchy Manager	HTTP	No	8.1	Network	Low	l
CVE-2021-2316	Oracle HRMS (France)	French HR	HTTP	No	8.1	Network	Low	l
CVE-2021-2260	Oracle Human Resources	iRecruitment	HTTP	No	8.1	Network	Low	l
CVE-2021-2228	Oracle Incentive Compensation	User Interface	HTTP	No	8.1	Network	Low	l
CVE-2021-2231	Oracle Installed Base	APIs	HTTP	No	8.1	Network	Low	l
CVE-2021-2276	Oracle iSetup	General Ledger Update Transform, Reports	HTTP	No	8.1	Network	Low	l
CVE-2021-2241	Oracle iStore	Shopping Cart	HTTP	No	8.1	Network	Low	l
CVE-2021-2267	Oracle Labor Distribution	User Interface	HTTP	No	8.1	Network	Low	l
CVE-2021-2249	Oracle Landed Cost Management	Shipment Workbench	HTTP	No	8.1	Network	Low	l
CVE-2021-2261	Oracle Lease and Finance Management	Quotes	HTTP	No	8.1	Network	Low	l
CVE-2021-2273	Oracle Legal Entity Configurator	Create Contracts	HTTP	No	8.1	Network	Low	l
CVE-2021-2252	Oracle Loans	Loan Details, Loan Accounting Events	HTTP	No	8.1	Network	Low	l
CVE-2021-2238	Oracle MES for Process Manufacturing	Process Operations	HTTP	No	8.1	Network	Low	l
CVE-2021-2259	Oracle Payables	India Localization,	HTTP	No	8.1	Network	Low	l

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
		Results						
CVE-2021-2289	Oracle Product Hub	Template, GTIN search	HTTP	No	8.1	Network	Low	l
CVE-2021-2254	Oracle Project Contracts	Hold Management	HTTP	No	8.1	Network	Low	l
CVE-2021-2258	Oracle Projects	User Interface	HTTP	No	8.1	Network	Low	l
CVE-2021-2262	Oracle Purchasing	Endeca	HTTPS	No	8.1	Network	Low	l
CVE-2021-2268	Oracle Quoting	Courseware	HTTP	No	8.1	Network	Low	l
CVE-2021-2223	Oracle Receivables	Receipts	HTTP	No	8.1	Network	Low	l
CVE-2021-2255	Oracle Service Contracts	Authoring	HTTP	No	8.1	Network	Low	l
CVE-2021-2270	Oracle Site Hub	Sites	HTTP	No	8.1	Network	Low	l
CVE-2021-2263	Oracle Sourcing	Intelligence, RFx	HTTP	No	8.1	Network	Low	l
CVE-2021-2272	Oracle Subledger Accounting	Inquiries	HTTP	No	8.1	Network	Low	l
CVE-2021-2239	Oracle Time and Labor	Timecard	HTTP	No	8.1	Network	Low	l
CVE-2021-2235	Oracle Transportation Execution	Install and Upgrade	HTTP	No	8.1	Network	Low	l
CVE-2021-2246	Oracle Universal Work Queue	Work Provider Site Level Administration	HTTP	No	8.1	Network	Low	l
CVE-2021-2271	Oracle Work in Process	Resource Exceptions	HTTP	No	8.1	Network	Low	l
CVE-2021-2181	Oracle Document	Attachments	HTTP	No	7.6	Network	Low	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Management and Collaboration							
CVE-2020-1967	Application Server	Technology Stack (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2021-2189	Oracle Sales Offline	Template	HTTP	Yes	7.5	Network	Low	N
CVE-2021-2190	Oracle Sales Offline	Template	HTTP	Yes	7.5	Network	Low	N
CVE-2021-2275	Oracle Applications Manager	View Reports	HTTP	No	6.5	Network	Low	H
CVE-2017-14735	Oracle E-Business Suite Technology Stack	Attachments, iRecruitment, Contracts (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2021-2153	Oracle Internet Expenses	Mobile Expenses	HTTP	Yes	4.3	Network	Low	N
CVE-2021-2155	Oracle One-to-One Fulfillment	Documents	HTTP	Yes	4.3	Network	Low	N

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

- Oracle E-Business Suite Information Discovery
  - Installer (Apache Log4j): CVE-2020-9488.

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Enterprise Manager. 8 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 April 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 April 2021 Patch Availability Document for Oracle Products, My Oracle Support Note 2749094.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-17195	Enterprise Manager Base Platform	Enterprise Manager Install (Nimbus JOSE+JWT)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-5064	Oracle Application Testing Suite	Load Testing for Web Apps (OpenCV)	HTTP	Yes	8.8	Network	Low	N
CVE-2020-10878	Enterprise Manager Base Platform	EM on Market Place (Perl)	HTTP	Yes	8.6	Network	Low	N
CVE-2020-11994	Enterprise Manager Base Platform	Reporting Framework (Apache Camel)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-1971	Enterprise Manager Ops Center	Satellite Framework (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2021-2008	Enterprise Manager for Fusion Middleware	FMW Control Plugin	HTTP	Yes	7.3	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-10086	Enterprise Manager for Virtualization	Administration operations (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2021-2134	Enterprise Manager for Fusion Middleware	FMW Control Plugin	HTTP	No	6.5	Network	Low	L
CVE-2021-2053	Enterprise Manager Base Platform	UI Framework	HTTP	Yes	6.1	Network	Low	N

Additional CVEs addressed are:

- The patch for CVE-2019-5064 also addresses CVE-2019-5063.
- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723.
- The patch for CVE-2020-1971 also addresses CVE-2021-23839, CVE-2021-23840 and CVE-2021-23841.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle Financial Services Applications. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-11998	Oracle FLEXCUBE Private Banking	Financial Planning (Apache ActiveMQ)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-5413	Oracle FLEXCUBE	Order Management	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Private Banking	(Spring Integration)						
CVE-2019-3773	Oracle FLEXCUBE Private Banking	Order Management (Spring Web Services)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-17638	Oracle FLEXCUBE Private Banking	Demographics (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low	N
CVE-2020-26217	Oracle Banking Platform	Collections (XStream)	HTTP	No	8.8	Network	Low	L
CVE-2020-5421	Oracle FLEXCUBE Private Banking	Financial Planning (Spring Framework)	HTTP	No	8.8	Network	Low	L
CVE-2020-25649	Oracle Banking Platform	Framework (jackson-databind)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-17566	Oracle Financial Services Analytical Applications Infrastructure	Rate Management (Apache Batik)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-10086	Oracle Banking Platform	Collections (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-10086	Oracle FLEXCUBE Private Banking	Loans and Pledges (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2020-5408	Oracle FLEXCUBE Private Banking	Order Management (Spring Security)	HTTP	No	6.5	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-27193	Oracle Banking Platform	Alerts (CKEditor)	HTTP	Yes	6.1	Network	Low	N
CVE-2021-2140	Oracle Financial Services Analytical Applications Infrastructure	Rules Framework	HTTP	Yes	6.1	Network	Low	N
CVE-2020-9489	Oracle FLEXCUBE Private Banking	Financial Planning (Apache Tika)	None	No	5.5	Local	Low	N
CVE-2021-2141	Oracle FLEXCUBE Direct Banking	Pre Login	Oracle Net	No	2.0	Network	High	H

Additional CVEs addressed are:

- The patch for CVE-2019-10086 also addresses CVE-2020-5413 and CVE-2020-9489.
- The patch for CVE-2019-17638 also addresses CVE-2019-17632 and CVE-2020-27218.
- The patch for CVE-2019-3773 also addresses CVE-2019-10086, CVE-2020-5413 and CVE-2020-9489.
- The patch for CVE-2020-11998 also addresses CVE-2020-11973 and CVE-2020-1941.
- The patch for CVE-2020-25649 also addresses CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188 and CVE-2020-36189.
- The patch for CVE-2020-27193 also addresses CVE-2020-9281.
- The patch for CVE-2020-5408 also addresses CVE-2020-5407.
- The patch for CVE-2020-5413 also addresses CVE-2019-10086 and CVE-2020-9489.
- The patch for CVE-2020-5421 also addresses CVE-2020-5408.
- The patch for CVE-2020-9489 also addresses CVE-2019-10086, CVE-2020-5408 and CVE-2020-5413.

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 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2018-20843	Oracle Hospitality RES 3700	Common (LibExpat)	HTTP	Yes	7.5	Network	Low	Non
CVE-2021-2311	Oracle Hospitality Inventory Management	Export to Reporting and Analytics	HTTP	No	6.5	Network	Low	Low

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 45 new security patches for Oracle Fusion Middleware. 36 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 April 2021 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 April 2021 Patch Availability Document for Oracle Products, My Oracle Support Note 2749094.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-9480	Oracle Business Intelligence Enterprise Edition	Analytics Server (Apache Spark)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-10683	Oracle Fusion Middleware	Centralized Thirdparty Jars (dom4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2021-2302	Oracle Platform Security for Java	OPSS	HTTP	Yes	9.8	Network	Low	No
CVE-2020-11612	Oracle WebCenter Portal	Security Framework (Netty)	HTTP	Yes	9.8	Network	Low	No
CVE-2021-2136	Oracle WebLogic Server	Core	IIOP	Yes	9.8	Network	Low	No
CVE-2021-2135	Oracle WebLogic Server	Coherence Container	T3, IIOP	Yes	9.8	Network	Low	No
CVE-2019-17638	FMW Platform	Common Components (Eclipse Jetty)	HTTP	Yes	9.4	Network	Low	No
CVE-2020-26217	Oracle BAM (Business Activity Monitoring)	General (XStream)	HTTP	No	8.8	Network	Low	Lo
CVE-2020-26217	Oracle Endeca Information Discovery Studio	Studio (XStream)	HTTP	No	8.8	Network	Low	Lo
CVE-2020-5421	Oracle Fusion Middleware	Centralized Thirdparty Jars (Spring Framework)	HTTP	No	8.8	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2021-2242	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	8.2	Network	Low	No
CVE-2020-24750	Oracle Identity Manager Connector	General and Misc (jackson-databind)	HTTP	Yes	8.1	Network	High	No
CVE-2020-11979	Oracle API Gateway	Oracle API Gateway (Apache Ant)	HTTP	Yes	7.5	Network	Low	No
CVE-2019-17566	Oracle API Gateway	Oracle API Gateway (Apache Batik)	HTTP	Yes	7.5	Network	Low	No
CVE-2020-1971	Oracle API Gateway	Oracle API Gateway (OpenSSL)	HTTPS	Yes	7.5	Network	Low	No
CVE-2020-1971	Oracle Business Intelligence Enterprise Edition	BI Platform Security (OpenSSL)	HTTPS	Yes	7.5	Network	Low	No
CVE-2021-2277	Oracle Coherence	Core	HTTP	Yes	7.5	Network	Low	No
CVE-2020-25649	Oracle Coherence	Core (jackson-databind)	HTTP	Yes	7.5	Network	Low	No
CVE-2020-11979	Oracle Endeca Information Discovery Studio	Studio (Apache Ant)	HTTP	Yes	7.5	Network	Low	No
CVE-2018-1000180	Oracle Enterprise Repository	Security Subsystem (Bouncy	HTTPS	Yes	7.5	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
		Castle Java Library)						
CVE-2019-17566	Oracle Fusion Middleware MapViewer	Install (Apache Batik)	HTTP	Yes	7.5	Network	Low	No
CVE-2020-5360	Oracle HTTP Server	SSL Module (Dell BSAFE Micro Edition Suite)	HTTPS	Yes	7.5	Network	Low	No
CVE-2020-5360	Oracle Security Service	C Oracle SSL API (Dell BSAFE Micro Edition Suite)	Multiple	Yes	7.5	Network	Low	No
CVE-2019-12402	Oracle WebCenter Portal	Security Framework (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-2157	Oracle WebLogic Server	TopLink Integration	HTTP	Yes	7.5	Network	Low	No
CVE-2020-5360	Oracle WebLogic Server Proxy Plug-In	SSL Module (Dell BSAFE Micro Edition Suite)	HTTPS	Yes	7.5	Network	Low	No
CVE-2019-10086	Oracle Fusion Middleware	Centralized Thirdparty Jars (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	No
CVE-2021-2240	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2019-10086	Oracle Service Bus	Web Container (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	No
CVE-2019-10086	Oracle WebLogic Server	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	No
CVE-2019-3740	Oracle WebLogic Server	Core (Dell BSAFE Crypto-J)	HTTPS	Yes	6.5	Network	Low	No
CVE-2021-2294	Oracle WebLogic Server	Core	T3, IIOP	Yes	6.5	Network	Low	No
CVE-2019-0221	Oracle Business Intelligence Enterprise Edition	BI Platform Security (Apache Tomcat)	HTTP	Yes	6.1	Network	Low	No
CVE-2020-11022	Oracle Business Intelligence Enterprise Edition	BI Platform Security (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2020-11022	Oracle Fusion Middleware MapViewer	Install (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2021-2142	Oracle WebLogic Server	Console	HTTP	Yes	6.1	Network	Low	No
CVE-2021-2211	Oracle WebLogic Server	Web Services	T3, IIOP	Yes	5.9	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2020-27842	Oracle Outside In Technology	Installation (OpenJPEG)	None	No	5.5	Local	Low	No
CVE-2021-20227	Oracle Outside In Technology	Installation (SQLite)	None	No	5.5	Local	Low	Lo
CVE-2020-9489	Oracle WebCenter Portal	Security Framework (Apache Tika)	None	No	5.5	Local	Low	No
CVE-2021-2191	Oracle Business Intelligence Enterprise Edition	Analytics Actions	HTTP	No	5.4	Network	Low	Lo
CVE-2021-2315	Oracle HTTP Server	Web Listener	HTTP	Yes	5.4	Network	Low	No
CVE-2021-2204	Oracle WebLogic Server	Core	HTTP	Yes	5.3	Network	Low	No
CVE-2021-2214	Oracle WebLogic Server	Console	HTTP	No	4.4	Network	High	Hig
CVE-2021-2152	Oracle Business Intelligence Enterprise Edition	Analytics Web General	HTTP	No	4.0	Network	High	Hig

Notes:

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

Additional CVEs addressed are:

- The patch for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The patch for CVE-2019-17566 also addresses CVE-2020-11987.
- The patch for CVE-2019-17638 also addresses CVE-2019-0232, CVE-2019-10072, CVE-2019-10246, CVE-2019-10247, CVE-2019-17632, CVE-2020-13934, CVE-2020-13935 and CVE-2020-9484.
- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-11979 also addresses CVE-2017-5645 and CVE-2020-1945.
- The patch for CVE-2020-24750 also addresses CVE-2020-24616.
- The patch for CVE-2020-26217 also addresses CVE-2019-10173.
- The patch for CVE-2020-27842 also addresses CVE-2020-27841, CVE-2020-27843, CVE-2020-27844 and CVE-2020-27845.
- The patch for CVE-2020-5360 also addresses CVE-2020-5359.
- The patch for CVE-2021-20227 also addresses CVE-2020-13434 and CVE-2020-13435.

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

- Oracle WebLogic Server
    - Core: CVE-2019-17638, CVE-2019-0232, CVE-2019-10072, CVE-2019-10246, CVE-2019-10247, CVE-2019-17632, CVE-2020-13934, CVE-2020-13935 and CVE-2020-9484.

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 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-1945	Oracle Health Sciences Information Manager	Health Record Locator (Apache Ant)	HTTP	Yes	9.1	Network	Low	None
CVE-2020-25649	Oracle Health Sciences Empirica Signal	Topics, REST Services (jackson-databind)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-10086	Oracle Healthcare Foundation	Self Service Analytics (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	None

Additional CVEs addressed are:

- The patch for CVE-2020-1945 also addresses CVE-2017-5645.

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Hospitality Applications. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2018-1285	Oracle Hospitality OPERA 5	Logging (Apache log4net)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-17530	Oracle Hospitality OPERA 5	Login (Apache Struts)	HTTP	Yes	9.8	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2021-22112	Oracle Hospitality Cruise Shipboard Property Management System	Next-Gen SPMS (Spring Security)	HTTP	No	8.8	Network	Low	Low
CVE-2019-17566	Oracle Hospitality OPERA 5	Integration (Apache Batik)	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-10086	Oracle Hospitality OPERA 5	Integrations (Apache Commons Beanutils)	HTTP	Yes	7.3	Network	Low	Non
CVE-2020-17521	Oracle Hospitality OPERA 5	Reporting (Apache Groovy)	None	No	5.5	Local	Low	Low

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 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2244	Hyperion Analytic Provider Services	JAPI	HTTP	Yes	9.6	Network	Low	None
CVE-2021-2158	Hyperion Financial Management	Task Automation	HTTP	No	3.9	Network	High	High

Oracle iLearning Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Inte
CVE-2020-17521	Oracle iLearning	Installation (Apache Groovy)	None	No	5.5	Local	Low	Low	N

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Insurance 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-2019-10086	Oracle Insurance Data Gateway	Security (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	None	

Oracle Java SE Risk Matrix

This Critical Patch Update contains 4 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 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-23841	Oracle GraalVM Enterprise Edition	Node (OpenSSL)	HTTPS	Yes	7.5	Network	Low	None
CVE-2021-3450	Oracle GraalVM Enterprise Edition	Node (Node.js)	HTTPS	Yes	7.4	Network	High	None
CVE-2021-2161	Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.9	Network	High	None
CVE-2021-2163	Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.3	Network	High	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. It can also be exploited by supplying untrusted data to APIs in the specified Component.

2. 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.

Additional CVEs addressed are:

- The patch for CVE-2021-23841 also addresses CVE-2021-23839 and CVE-2021-23840.
- The patch for CVE-2021-3450 also addresses CVE-2020-7774, CVE-2021-22883, CVE-2021-22884 and CVE-2021-3449.

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 10 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			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-28052	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech - Cloud (Bouncy Castle Java Library)	HTTPS	Yes	9.8	Network	Low	N
CVE-2019-17566	JD Edwards EnterpriseOne Tools	Web Runtime (Apache Batik)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-1971	JD Edwards EnterpriseOne Tools	OneWorld Tools Security (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2020-1971	JD Edwards World Security	World Software	HTTPS	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
		Security (OpenSSL)						
CVE-2019-10086	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator Security (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2019-10086	JD Edwards EnterpriseOne Tools	Portal SEC (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2020-9281	JD Edwards EnterpriseOne Tools	Web Runtime (CKEditor)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-11022	JD Edwards EnterpriseOne Tools	Web Runtime (jQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2016-5725	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure SEC (JCraft JSch)	SFTP	Yes	5.9	Network	High	N
CVE-2020-9488	JD Edwards World Security	World Software Security (Apache Log4j)	HTTP	Yes	3.7	Network	High	N

Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2019-11358 and CVE-2019-5428.
- The patch for CVE-2020-1971 also addresses CVE-2019-1551, CVE-2020-1967, CVE-2020-1968 and CVE-2020-9488.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 49 new security patches for Oracle MySQL. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-17530	MySQL Enterprise Monitor	Monitoring: General (Apache Struts)	HTTPS	Yes	9.8	Network	Low	Non
CVE-2020-8277	MySQL Cluster	Cluster: JS module (Node.js)	Multiple	Yes	7.5	Network	Low	Non
CVE-2020-17527	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	7.5	Network	Low	Non
CVE-2021-23841	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	HTTPS	Yes	7.5	Network	Low	Non
CVE-2020-1971	MySQL Server	Server: Compiling (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low	Non
CVE-2021-3449	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low	Non
CVE-2020-28196	MySQL Server	Server: Security: Encryption (MIT Kerberos)	MySQL Protocol	Yes	7.5	Network	Low	Non
CVE-2021-23841	MySQL Server	Server: Security: Encryption (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low	Non
CVE-2021-3450	MySQL Workbench	MySQL Workbench (OpenSSL)	MySQL Workbench	Yes	7.4	Network	High	Non
CVE-2021-2144	MySQL Server	Server: Parser	MySQL Protocol	No	7.2	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-2172	MySQL Server	Server: DML	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2021-2298	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2021-2178	MySQL Server	Server: Replication	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2021-2202	MySQL Server	Server: Replication	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2021-2307	MySQL Server	Server: Packaging	None	No	6.1	Local	Low	Non
CVE-2021-2304	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	5.5	Network	Low	Hig
CVE-2019-7317	MySQL Workbench	Workbench (libpng)	MySQL Workbench	Yes	5.3	Network	High	Non
CVE-2021-2180	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2194	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2154	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2166	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2196	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-2300	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2305	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2179	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2226	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2160	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2164	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2169	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2170	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2193	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2203	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2212	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2213	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2278	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2299	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2230	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-2146	MySQL Server	Server: Options	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2201	MySQL Server	Server: Partition	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2208	MySQL Server	Server: Partition	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2215	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2217	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2293	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2021-2174	MySQL Server	InnoDB	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2021-2171	MySQL Server	Server: Replication	MySQL Protocol	No	4.4	Network	High	Hig
CVE-2021-2162	MySQL Server	Server: Audit Plug-in	MySQL Protocol	No	4.3	Network	Low	Lov
CVE-2021-2301	MySQL Server	Server: Information Schema	MySQL Protocol	No	2.7	Network	Low	Hig
CVE-2021-2308	MySQL Server	Server: Information Schema	MySQL Protocol	No	2.7	Network	Low	Hig
CVE-2021-2232	MySQL Server	Server: Group Replication Plugin	None	No	1.9	Local	High	Hig

Additional CVEs addressed are:

- The patch for CVE-2019-7317 also addresses CVE-2018-14550.
- The patch for CVE-2020-17530 also addresses CVE-2019-0230 and CVE-2019-0233.
- The patch for CVE-2021-23841 also addresses CVE-2021-23840.
- The patch for CVE-2021-3449 also addresses CVE-2021-3450.
- The patch for CVE-2021-3450 also addresses CVE-2021-3449.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 18 new security patches plus additional third party patches noted below for Oracle PeopleSoft. 13 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-2021-2218	PeopleSoft Enterprise PT PeopleTools	Health Center	HTTP	Yes	8.3	Network	Low	
CVE-2020-28052	PeopleSoft Enterprise PeopleTools	XML Messaging (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	
CVE-2020-8286	PeopleSoft Enterprise PeopleTools	File Processing (cURL)	HTTP	Yes	7.5	Network	Low	
CVE-2017-18640	PeopleSoft Enterprise PT PeopleTools	Application Server (SnakeYAML)	HTTP	Yes	7.5	Network	Low	
CVE-2021-2219	PeopleSoft Enterprise PeopleTools	SQR	HTTP	No	7.4	Network	Low	
CVE-2019-10086	PeopleSoft Enterprise PT PeopleTools	Weblogic (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2017-1000061	PeopleSoft Enterprise PeopleTools	XML Messaging (xmlSec)	None	No	7.1	Local	Low	
CVE-2021-2151	PeopleSoft Enterprise PeopleTools	Security	HTTP	No	6.7	Network	Low	
CVE-2020-11022	PeopleSoft Enterprise FIN Common Application Objects	Common Objects (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	PeopleSoft Enterprise FIN Expenses	Expenses (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2021-2216	PeopleSoft Enterprise PeopleTools	Multichannel Framework	HTTP	Yes	6.1	Network	Low	
CVE-2020-27193	PeopleSoft Enterprise PeopleTools	Rich Text Editor (CKEditor)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	PeopleSoft Enterprise PT PeopleTools	Weblogic (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	PeopleSoft Enterprise SCM eProcurement	Manage Requisition Status (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-11022	PeopleSoft Enterprise SCM Purchasing	Purchasing (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2020-1971	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	5.9	Network	High	
CVE-2021-2220	PeopleSoft Enterprise SCM eProcurement	Manage Requisition Status	HTTP	No	5.4	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-2159	PeopleSoft Enterprise CS Campus Community	Frameworks	HTTP	No	3.5	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2017-18640 also addresses CVE-2019-12402.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-8286 also addresses CVE-2020-8284 and CVE-2020-8285.

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

- PeopleSoft Enterprise PeopleTools
  - Security (Apache Log4j): CVE-2019-17571.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 35 new security patches for Oracle Retail Applications. 31 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-10683	Oracle Retail Xstore Point of Service	Xenvironment (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2019-0228	Oracle Retail Xstore Point of Service	Xstore Office (Apache PDFbox)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-5421	Oracle Retail Predictive Application Server	RPAS Fusion Client (Spring Framework)	HTTP	No	8.8	Network	Low	
CVE-2020-5421	Oracle Retail Xstore Point of Service	Xenvironment (Spring Framework)	HTTP	No	8.8	Network	Low	
CVE-2020-11979	Oracle Retail Advanced Inventory Planning	Operations & Maintenance (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Assortment Planning	Custom Workbooks (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11987	Oracle Retail Back Office	Pricing (Apache Batik)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Category Management Planning & Optimization	ODI Integration (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11987	Oracle Retail Central Office	Pricing (Apache Batik)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail EFTLink	Unified Payments (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Item Planning	AAI Framework (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Macro Space Optimization	ODI Integration (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Merchandise Financial Planning	Merchandising Insights (Apache Ant)	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 Merchandising System	Financials (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11987	Oracle Retail Point-of-Service	Mobile POS (Apache Batik)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Regular Price Optimization	Operations & Maintenance (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Replenishment Optimization	AAI Framework (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11987	Oracle Retail Returns Management	Main Dashboard (Apache Batik)	HTTP	Yes	7.5	Network	Low	
CVE-2017-12626	Oracle Retail Sales Audit	Sales Audit Maintenance (Apache POI)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Size Profile Optimization	Solver (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2020-11979	Oracle Retail Xstore Point of Service	Xenvironment (Apache Ant)	HTTP	Yes	7.5	Network	Low	
CVE-2019-10086	Oracle Retail Advanced Inventory Planning	Operations & Maintenance (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Back Office	Pricing (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2019-10086	Oracle Retail Central Office	Commerce Anywhere (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Point-of-Service	Pricing (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Retail Returns Management	Main Dashboard (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-3740	Oracle Retail Predictive Application Server	RPAS Server (DELL BSAFE Crypto-J)	HTTPS	Yes	6.5	Network	Low	
CVE-2020-17521	Oracle Retail Merchandising System	Foundation (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-17521	Oracle Retail Store Inventory Management	SIM Integration (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2020-27218	Oracle Retail EFTLink	Unified Payments (Eclipse Jetty)	HTTP	Yes	4.8	Network	High	
CVE-2020-9488	Oracle Retail EFTLink	Unified Payments (Apache Log4j)	HTTP	Yes	3.7	Network	High	
CVE-2020-9488	Oracle Retail Insights Cloud Service Suite	OBIEE - Metadata (Apache Log4j)	HTTP	Yes	3.7	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-9488	Oracle Retail Xstore Point of Service	Xenvironment (Apache Log4j)	HTTP	Yes	3.7	Network	High	

Additional CVEs addressed are:

- The patch for CVE-2020-11979 also addresses CVE-2017-5645 and CVE-2020-1945.
- The patch for CVE-2020-11987 also addresses CVE-2019-17566.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Siebel CRM. 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-2020-14195	Siebel UI Framework	EAI (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-5398	Siebel Engineering - Installer & Deployment	Siebel Approval Manager (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2019-0227	Siebel UI Framework	SWSE Server (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-10080	Siebel UI Framework	EAI (Jersey)	HTTP	No	6.5	Network	Low
CVE-2020-9281	Siebel Apps - Customer Order Management	Customizable Prod/Configurator (CKEditor)	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2016-7103	Siebel UI Framework	UIF Open UI (jQuery UI)	HTTP	Yes	6.1	Network	Low
CVE-2019-11358	Siebel UI Framework	UIF Open UI (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-9488	Siebel UI Framework	EAI (Apache Log4j)	HTTP	Yes	3.7	Network	High

Additional CVEs addressed are:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2020-14195 also addresses CVE-2020-14060, CVE-2020-14061, CVE-2020-14062, CVE-2020-24616 and CVE-2020-24750.

Oracle Storage Gateway Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Storage Gateway. 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 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2317	Oracle Cloud Infrastructure Storage Gateway	Management Console	HTTP	Yes	10.0	Network	Low	None
CVE-2021-2256	Oracle Storage Cloud Software Appliance	Management Console	HTTP	Yes	10.0	Network	Low	None
CVE-2021-2318	Oracle Cloud Infrastructure Storage Gateway	Management Console	HTTP	No	9.1	Network	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2319	Oracle Cloud Infrastructure Storage Gateway	Management Console	HTTP	No	9.1	Network	Low	High
CVE-2021-2320	Oracle Cloud Infrastructure Storage Gateway	Management Console	HTTP	No	9.1	Network	Low	High
CVE-2021-2257	Oracle Storage Cloud Software Appliance	Management Console	HTTP	No	4.1	Network	Low	High

Notes:

1. Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from here. Refer to Document 2768897.1 for more details.

2. Updating the Oracle Storage Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download the latest version of Oracle Storage Cloud Software Appliance from here. Refer to Document 2768897.1 for more details.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 5 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	Priv Req
CVE-2019-2904	Oracle Rapid Planning	User interface (Application	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	Priv Req
		Development Framework)						
CVE-2021-2253	Oracle Advanced Supply Chain Planning	Core	HTTP	Yes	9.1	Network	Low	Nor
CVE-2019-10086	Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite	Installer (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	Nor
CVE-2019-10086	Agile Product Lifecycle Management Integration Pack for SAP: Design to Release	Core (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	Nor
CVE-2019-10086	Oracle Agile PLM	Security (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	Nor

Oracle Support Tools Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2021-2303	OSS Support Tools	Diagnostic Assistant	HTTP	No	4.9	Network	Low	High	Nc

Oracle Systems Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle Systems. 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	Ir
CVE-2020-1472	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	10.0	Network	Low	None	
CVE-2021-2167	Oracle Solaris	Common Desktop Environment	None	No	7.8	Local	Low	Low	
CVE-2021-2192	Oracle Solaris	Kernel	None	No	6.1	Local	Low	Low	
CVE-2021-2149	Oracle ZFS Storage Appliance Kit	Core	None	No	2.5	Local	High	Low	
CVE-2021-2147	Oracle ZFS Storage Appliance Kit	Installation	None	No	1.8	Local	High	High	Re

Notes:

1. This vulnerability applies to Oracle Solaris on SPARC systems only.

Additional CVEs addressed are:

- The patch for CVE-2020-1472 also addresses CVE-2020-26418, CVE-2020-26419, CVE-2020-26420, CVE-2020-26421, CVE-2020-26422, CVE-2021-22173, CVE-2021-22174, CVE-2021-22191 and CVE-2021-23336.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 5 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 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-17495	Oracle Utilities Framework	General (Swagger UI)	HTTP	Yes	9.8	Network	Low	None
CVE-2020-28052	Oracle Utilities Framework	Securty (Bouncy Castle Java Library)	HTTPS	Yes	9.8	Network	Low	None
CVE-2020-11979	Oracle Utilities Framework	General (Apache Ant)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-25649	Oracle Utilities Framework	General (jackson-databind)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-10086	Oracle Utilities Framework	General (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	None

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 25 new security patches for Oracle Virtualization. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-2177	Oracle Secure Global Desktop	Gateway	Multiple	Yes	10.0	Network	Low	None	
CVE-2021-2248	Oracle Secure Global Desktop	Server	Multiple	Yes	10.0	Network	Low	None	
CVE-2021-2221	Oracle Secure Global Desktop	Client	Multiple	Yes	9.6	Network	Low	None	R
CVE-2021-2264	Oracle VM VirtualBox	Core	None	No	8.4	Local	Low	Low	
CVE-2021-2279	Oracle VM VirtualBox	Core	RDP	Yes	8.1	Network	High	None	
CVE-2021-2309	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2021-2250	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2021-2145	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2021-2310	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2021-3450	Oracle Secure Global Desktop	Core (OpenSSL)	HTTPS	Yes	7.4	Network	High	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2021-2280	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2281	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2282	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2283	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2284	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2285	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2286	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2287	Oracle VM VirtualBox	Core	None	No	7.1	Local	Low	None	
CVE-2021-2306	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2021-2266	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2021-2321	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2021-2296	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2021-2297	Oracle VM VirtualBox	Core	None	No	5.3	Local	High	High	
CVE-2021-2291	Oracle VM VirtualBox	Core	None	No	4.7	Local	High	Low	
CVE-2021-2312	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	

Notes:

1. This vulnerability applies to Linux systems only.

2. This vulnerability applies to Windows systems only.

Additional CVEs addressed are:

- The patch for CVE-2021-3450 also addresses CVE-2021-3449.