Oracle Critical Patch Update Advisory - July 2022

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 349 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 July 2022 Critical Patch Update: Executive Summary and Analysis.

Please note that since the release of the April 2022 Critical Patch Update, Oracle has released a Security Alert for Oracle E-Business Suite CVE-2022-21500 (May 19, 2022). Customers are strongly advised to apply the July 2022 Critical Patch Update for Oracle E-Business Suite, which includes patches for this Alert as well as additional patches.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Autonomous Health Framework	Oracle Autonomous Health Framew
Big Data Spatial and Graph, versions prior to 23.1	Database
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0	Enterprise Manager
Enterprise Manager for MySQL Database	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
JD Edwards EnterpriseOne Orchestrator, versions 9.2.6.3 and prior	JD Edwards
JD Edwards EnterpriseOne Tools, versions 9.2.6.3 and prior	JD Edwards
MySQL Cluster, versions 7.4.36 and prior, 7.5.26 and prior, 7.6.22 and prior, 8.0.29 and prior, and8.0.29 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.30 and prior	MySQL
MySQL Server, versions 5.7.38 and prior, 8.0.29 and prior	MySQL
MySQL Shell, versions 8.0.28 and prior	MySQL
MySQL Shell for VS Code, versions 1.1.8 and prior	MySQL
MySQL Workbench, versions 8.0.29 and prior	MySQL
Oracle Agile Engineering Data Management, version 6.2.1.0	Oracle Supply Chain Products
Oracle Agile PLM, version 9.3.6	Oracle Supply Chain Products
Oracle Agile Product Lifecycle Management for Process, versions 6.2.2, 6.2.3	Oracle Supply Chain Products
Oracle Application Express, versions prior to 22.1.1	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2	Oracle Supply Chain Products
Oracle Banking Branch, version 14.5	Contact Support
Oracle Banking Cash Management, version 14.5	Contact Support
Oracle Banking Corporate Lending Process Management, version 14.5	Contact Support
Oracle Banking Credit Facilities Process Management, version 14.5	Contact Support
Oracle Banking Deposits and Lines of Credit Servicing, version 2.7	Contact Support
Oracle Banking Electronic Data Exchange for Corporates, version 14.5	Contact Support
Oracle Banking Liquidity Management, versions 14.2, 14.5	Contact Support

Affected Products and Versions	Patch Availability Document
Oracle Banking Origination, version 14.5	Contact Support
Oracle Banking Party Management, version 2.7	Oracle Banking Platform
Oracle Banking Platform, versions 2.6.2, 2.9, 2.12	Oracle Banking Platform
Oracle Banking Supply Chain Finance, version 14.5	Contact Support
Oracle Banking Trade Finance, version 14.5	Contact Support
Oracle Banking Trade Finance Process Management, version 14.5	Contact Support
Oracle Banking Virtual Account Management, version 14.5	Contact Support
Oracle Berkeley DB	Berkeley DB
Oracle BI Publisher, versions 12.2.1.3.0, 12.2.1.4.0	Oracle Analytics
Oracle Blockchain Platform	Oracle Blockchain Platform
Oracle Business Intelligence Enterprise Edition, version 5.9.0.0.0	Oracle Analytics
Oracle Coherence, versions 3.7.1.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle Commerce Guided Search, version 11.3.2	Oracle Commerce
Oracle Commerce Merchandising, version 11.3.2	Oracle Commerce
Oracle Commerce Platform, versions 11.3.0, 11.3.1, 11.3.2	Oracle Commerce
Oracle Communications ASAP, version 7.3	Oracle Communications ASAP
Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.6.0	Oracle Communications Billing and Revenue Management
Oracle Communications BRM - Elastic Charging Engine, versions prior to 12.0.0.4.6, prior to 12.0.0.5.1	Oracle Communications BRM - Elast Charging Engine
Oracle Communications Cloud Native Core Binding Support Function, versions 22.1.3, 22.2.0	Oracle Communications Cloud Nativ Core Binding Support Function
Oracle Communications Cloud Native Core Console, versions 22.1.2, 22.2.0	Oracle Communications Cloud Nativ Core Console
Oracle Communications Cloud Native Core Network Exposure Function, version 22.1.1	Oracle Communications Cloud Nativ Core Network Exposure Function
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 22.1.0, 22.1.2, 22.2.0	Oracle Communications Cloud Nativ Core Network Function Cloud Native Environment
Oracle Communications Cloud Native Core Network Repository Function, versions 22.1.2, 22.2.0	Oracle Communications Cloud Nativ Core Network Repository Function
Oracle Communications Cloud Native Core Network Slice Selection Function, version 22.1.1	Oracle Communications Cloud Nativ Core Network Slice Selection Functic

Affected Products and Versions	Patch Availability Document
Oracle Communications Cloud Native Core Policy, versions 22.1.3, 22.2.0	Oracle Communications Cloud Nativ Core Policy
Oracle Communications Cloud Native Core Security Edge Protection Proxy, version 22.1.1	Oracle Communications Cloud Nativ Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Service Communication Proxy, version 22.2.0	Oracle Communications Cloud Nativ Core Service Communication Proxy
Oracle Communications Cloud Native Core Unified Data Repository, version 22.2.0	Oracle Communications Cloud Nativ Core Unified Data Repository
Oracle Communications Core Session Manager, versions 8.2.5, 8.4.5	Oracle Communications Core Sessio Manager
Oracle Communications Design Studio, version 7.4.2	Oracle Communications Design Stuc
Oracle Communications Instant Messaging Server, version 10.0.1.5.0	Oracle Communications Instant Messaging Server
Oracle Communications IP Service Activator	Oracle Communications IP Service Activator
Oracle Communications Offline Mediation Controller, versions prior to 12.0.0.4.4, prior to 12.0.0.5.1	Oracle Communications Offline Mediation Controller
Oracle Communications Operations Monitor, versions 4.3, 4.4, 5.0	Oracle Communications Operations Monitor
Oracle Communications Session Border Controller, versions 8.4, 9.0, 9.1	Oracle Communications Session Bor Controller
Oracle Communications Unified Inventory Management, versions 7.4.1, 7.4.2, 7.5.0	Oracle Communications Unified Inventory Management
Oracle Communications Unified Session Manager, version 8.2.5	Oracle Communications Unified Ses Manager
Oracle Crystal Ball, versions 11.1.2.0.0-11.1.2.4.900	Oracle Construction and Engineerin Suite
Oracle Data Integrator	Fusion Middleware
Oracle Database Server, versions 12.1.0.2, 19c, 21c	Database
Oracle E-Business Suite, versions 12.2.3-12.2.11	Oracle E-Business Suite
Oracle Enterprise Communications Broker, version 3.3	Oracle Enterprise Communications Broker
Oracle Enterprise Operations Monitor, versions 4.3, 4.4, 5.0	Oracle Enterprise Operations Monitc
Oracle Enterprise Session Border Controller, versions 8.4, 9.0, 9.1	Oracle Enterprise Session Border Controller
Oracle Essbase, version 21.3	Database

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.0-8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Behavior Detection Platform, versions 8.0.7.0, 8.0.8.0, 8.1.1.0-8.1.2.1	Oracle Financial Services Behavior Detection Platform
Oracle Financial Services Crime and Compliance Management Studio, versions 8.0.8.2.0, 8.0.8.3.0	Oracle Financial Services Crime and Compliance Management Studio
Oracle Financial Services Enterprise Case Management, versions 8.0.7.1, 8.0.7.2, 8.0.8.0, 8.0.8.1, 8.1.1.0-8.1.2.1	Oracle Financial Services Enterprise Case Management
Oracle Financial Services Revenue Management and Billing, versions 2.9.0.0.0, 2.9.0.1.0, 3.0.0.0.0-3.2.0.0.0, 4.0.0.0.0	Oracle Financial Services Revenue Management and Billing
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, versions 8.0.7.0, 8.0.8.0	Oracle Financial Services Trade-Base Anti Money Laundering Enterprise Edition
Oracle FLEXCUBE Core Banking, versions 5.2, 11.6-11.8, 11.10	Contact Support
Oracle FLEXCUBE Private Banking, version 12.1	Contact Support
Oracle FLEXCUBE Universal Banking, versions 12.1-12.4, 14.0-14.3, 14.5	Contact Support
Oracle Global Lifecycle Management NextGen OUI Framework, versions prior to 13.9.4.2.10	Fusion Middleware
Oracle Global Lifecycle Management OPatch, versions prior to 12.2.0.1.30	Global Lifecycle Management
Oracle GoldenGate, versions [19c] prior to 19.1.0.0.220719, [21c] prior to 21.7.0.0.0	Database
Oracle GraalVM Enterprise Edition, versions 20.3.6, 21.3.2, 22.1.0	Java SE
Oracle Graph Server and Client, versions prior to 22.2.0	Database
Oracle Health Sciences Data Management Workbench, versions 2.4.8.7, 2.5.2.1, 3.0.0.0, 3.1.0.3	Health Sciences
Oracle Health Sciences Empirica Signal, versions 9.1.0.52, 9.2.0.52	Health Sciences
Oracle Health Sciences Information Manager, versions 3.0.0.1, 3.0.1.0-3.0.5.0	HealthCare Applications
Oracle Healthcare Foundation, versions 8.1.0, 8.2.0, 8.2.1	HealthCare Applications
Oracle Hospitality Cruise Shipboard Property Management System, version 20.2.1	Oracle Hospitality Cruise Shipboard Property Management System
Oracle Hospitality Inventory Management, version 9.1	Oracle Hospitality Inventory Management
Oracle Hospitality Materials Control, version 18.1	Oracle Hospitality Materials Control

Affected Products and Versions	Patch Availability Document
Oracle Hospitality OPERA 5, version 5.6	Oracle Hospitality OPERA 5 Property Services
Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Identity Management Suite	Fusion Middleware
Oracle Identity Manager Connector	Fusion Middleware
Oracle Java SE, versions 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1	Java SE
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle NoSQL Database	NoSQL Database
Oracle Policy Automation, versions 12.2.0-12.2.25	Oracle Policy Automation
Oracle Policy Automation for Mobile Devices, versions 12.2.0-12.2.24	Oracle Policy Automation
Oracle Product Lifecycle Analytics, version 3.6.1	Oracle Supply Chain Products
Oracle REST Data Services, versions prior to 22.1.1	Database
Oracle Retail Allocation, versions 15.0.3.1, 16.0.3	Retail Applications
Oracle Retail Bulk Data Integration, version 16.0.3	Retail Applications
Oracle Retail Customer Insights, versions 15.0.2, 16.0.2	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 17.0, 18.0, 19.0	Retail Applications
Oracle Retail Extract Transform and Load, version 13.2.5	Retail Applications
Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Merchandising System, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Order Broker, versions 18.0, 19.1	Retail Applications
Oracle Retail Pricing, version 19.0.1	Retail Applications
Oracle Retail Sales Audit, versions 15.0.3.1, 16.0.3	Retail Applications
Oracle Retail Xstore Point of Service, versions 17.0.4, 18.0.3, 19.0.2, 20.0.1, 21.0.1	Retail Applications
Oracle SD-WAN Edge, versions 9.0, 9.1	Oracle SD-WAN Edge
Oracle Security Service, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle SOA Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Solaris, versions 10, 11	Systems
Oracle Spatial Studio, versions prior to 22.1.0	Database
Oracle SQL Developer	Database
Oracle Stream Analytics, versions [19c] prior to 19.1.0.0.6.4	Database
Oracle TimesTen In-Memory Database, versions prior to 22.1.1.1.0	Database
Oracle Transportation Management, version 1.4.4	Oracle Supply Chain Products
Oracle Utilities Framework, versions 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.5.0.0.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.36	Virtualization
Oracle WebCenter Content, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Portal, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Sites Support Tools, versions 4.4.2 and prior	Fusion Middleware
Oracle WebLogic Server, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle Weblogic Server Proxy Plug-in, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59	PeopleSoft
Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.14, 19.12.0-19.12.13, 20.12.0-20.12.8, 21.12.0-21.12.1	Oracle Construction and Engineering Suite
Primavera P6 Enterprise Project Portfolio Management, versions 17.12.0.0-17.12.20.4, 18.8.0.0-18.8.25.4, 19.12.0.0-19.12.19.0, 20.12.0.0-20.12.14.0, 21.12.0.0-21.12.4.0	Oracle Construction and Engineering Suite
Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12, 21.12	Oracle Construction and Engineering Suite
Siebel Applications, versions 22.6 and prior	Siebel

Note:

- 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 patches 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:

- 4ra1n: CVE-2022-21557, CVE-2022-21560, CVE-2022-21562, CVE-2022-21564
- Ahmed Alwardani: CVE-2022-21568

- Ahmed Shah of Red Canari: CVE-2022-21543
- Alexander Kornbrust of Red Database Security: CVE-2022-21510
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2022-21550
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2022-21511
- Emad Al-Mousa of Saudi Aramco: CVE-2022-21432
- Felix Wilhelm of Google: CVE-2022-34169
- Hugo Santiago dos Santos: CVE-2022-21575
- korean_buljumuk: CVE-2022-21571
- Kun Yang of Chaitin Security Research Lab: CVE-2022-21554
- Liboheng of Tophant Starlight laboratory: CVE-2022-21548
- Lidor Ben Shitrit from Orca Security: CVE-2022-21551
- Lu Yu of Chaitin Security Research Lab: CVE-2022-21554
- M Talha Shafique: CVE-2022-21545
- Matthias Kaiser of Apple Information Security: CVE-2022-21516, CVE-2022-21536
- Nadeem Douba of Red Canari: CVE-2022-21543
- Orwa Atyat: CVE-2022-21567
- r00t4dm: CVE-2022-21523
- Ronnie Salomonsen of Mandiant Services: CVE-2022-21558
- Sanehdeep Singh: CVE-2022-21544
- thiscodecc of MoyunSec V-Lab: CVE-2022-21570
- Turki Al-harthi: CVE-2022-21567
- y4tacker: CVE-2022-21557
- Zacharias Pigadas of Foregenix: CVE-2022-21552
- Zu-Ming Jiang: CVE-2022-21556
- 潘宏弢: CVE-2022-21549

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:

- Cheng Xu
- Dennis Katz
- Emad Al-Mousa of Saudi Aramco
- John Jackson
- Kelly Kaoudis
- Markus Loewe
- Nick Sahler
- Rizal Muhammed
- Sick Codes
- Stuart Monteith of Arm
- Victor Viale

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:

- Ahmed Hassan
- Ekin Şiar Bayer
- Elad Gabay of Wiz.io
- Gabriel
- Hamoud Al-Helmani
- Hannu Forsten [3 reports]
- Heitor Gouvêa
- ilyas ORAK
- k0xx
- Lawrence See Yon Hoe
- Nikesh Gogia

- Paul Wise
- Semih Comak
- Shuvam Adhikari [2 reports]
- Siddhesh Parab
- tayyab sial
- wardi abdi
- Yassine Triki
- Zach Edwards of victorymedium.com

Critical Patch Update Schedule

Critical Patch Updates are released on the third Tuesday of January, April, July, and October. The next four dates are:

- 18 October 2022
- 17 January 2023
- 18 April 2023
- 18 July 2023

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - July 2022 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
- CSAF JSON version of the risk matrices
- Map of CVE to Advisory/Alert
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2022-October-31	Rev 4. Updated Credit section
2022-July-28	Rev 3. Updated the affected versions WebLogic CVE-2021-40690
2022-July-25	Rev 2. Updated the version details for WebCenter Sites Support Tools and Credit add for CVE-2022-21551
2022-July-19	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 23 new security patches for Oracle Database Products divided as follows:

- 9 new security patches for Oracle Database Products
- No new security patches for Oracle Autonomous Health Framework, but third party patches are provided
- No new security patches for Oracle Berkeley DB, but third party patches are provided
- 3 new security patches for Oracle Big Data Graph
- No new security patches for Oracle Blockchain Platform, but third party patches are provided
- 1 new security patch for Oracle Essbase
- 1 new security patch for Oracle Global Lifecycle Management
- 4 new security patches for Oracle GoldenGate
- 1 new security patch for Oracle Graph Server and Client
- No new security patches for Oracle NoSQL Database, but third party patches are provided
- 2 new security patches for Oracle REST Data Services
- 1 new security patch for Oracle Spatial Studio
- No new security patches for Oracle SQL Developer, but third party patches are provided
- 1 new security patch for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 9 new security patches plus additional third party patches noted below for Oracle Database Products. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 of these patches is 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.?	CV	
					Base Score	Attack Vector
CVE-2020-35169	Oracle Database - Enterprise Edition	None	TCPS	Yes	9.1	Network
CVE-2022-21510	Oracle Database - Enterprise Edition Sharding	Local Logon	None	No	8.8	Local
CVE-2022-21511	Oracle Database - Enterprise Edition Recovery	EXECUTE ON DBMS_IR.EXECUTESQLSCRIPT	Oracle Net	No	7.2	Network
CVE-2022-21565	Java VM	Create Procedure	Oracle Net	No	6.5	Network
CVE-2022-24729	Oracle Application Express (CKEditor)	User Account	HTTP	No	5.7	Network
CVE-2021-41184	Oracle Application Express (jQueryUI)	User Account	HTTP	No	5.4	Network
CVE-2022-0839	Oracle SQLcl (Liquibase)	Local Logon	None	No	5.0	Local
CVE-2021-45943	Oracle Spatial and Graph (GDAL)	Create Session	Oracle Net	No	4.3	Network
CVE-2022-21432	Oracle Database - Enterprise Edition RDBMS Security	DBA role	Oracle Net	No	2.7	Network

Notes:

1. None of the supported versions are affected.

Additional CVEs addressed are:

- The patch for CVE-2020-35169 also addresses CVE-2020-26185, CVE-2020-29505, CVE-2020-29506, CVE-2020-29507, CVE-2020-29508, CVE-2020-35163, CVE-2020-35164, CVE-2020-35166, CVE-2020-35167, and CVE-2020-35168.
- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.
- The patch for CVE-2022-24729 also addresses CVE-2022-24728.

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

- Oracle Database Enterprise Edition (Apache Tomcat): CVE-2022-29885.
- Oracle Universal Installer (jackson-databind): CVE-2020-36518.

Oracle Database Server Client-Only Installations

- The following Oracle Database Server vulnerability included in this Critical Patch Update affects client-only installations: CVE-2020-35169.

Oracle Autonomous Health Framework Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Autonomous Health Framework. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle Autonomous Health Framework. 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:

- Autonomous Health Framework
  - Autonomous Health Framework (NumPy): CVE-2021-41496 and CVE-2021-41495.

- Autonomous Health Framework (Python): CVE-2021-29921 and CVE-2020-29396.
- Trace File Analyzer (jackson-databind): CVE-2020-36518.

Oracle Berkeley DB Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Berkeley DB. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle Berkeley DB. 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:

- Berkeley DB Data Store
  - Data Store (Apache Log4j): CVE-2022-23305, CVE-2021-4104, CVE-2022-23302 and CVE-2022-23307.

Oracle Big Data Graph Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Big Data Graph. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-42340	Big Data	Big Data Graph	HTTP	Yes	7.5	Network	Low	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
	Spatial and Graph	(Apache Tomcat)							
CVE-2020-36518	Big Data Spatial and Graph	Big Data Graph (jackson-databind)	HTTP	Yes	7.5	Network	Low	None	
CVE-2021-41184	Big Data Spatial and Graph	Big Data Graph (jQueryUI)	HTTP	Yes	6.1	Network	Low	None	Re

Additional CVEs addressed are:

- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.

Oracle Blockchain Platform Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Blockchain Platform. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle Blockchain Platform. 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 Blockchain Platform
  - Blockchain Cloud Service Console (OpenSSH): CVE-2021-41617.

Oracle Essbase Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Essbase. 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-2022-21508	Oracle Essbase	Security and Provisioning	None	No	5.8	Local	Low	High	Req

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 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2022-23437	Oracle Global Lifecycle Management OPatch	Patch Installer (Apache Xerces-J)	Local Logon	No	4.2	Local	Low	High

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 (jackson-databind): CVE-2020-36518.

Oracle GoldenGate Risk Matrix

This Critical Patch Update contains 4 new security patches plus additional third party patches noted below for Oracle GoldenGate. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-3749	Oracle GoldenGate	Oracle GoldenGate (axios)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-21551	Oracle GoldenGate	Oracle GoldenGate	HTTP	No	6.8	Network	Low	High
CVE-2021-34429	Oracle Stream Analytics	Oracle Stream Analytics (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	None
CVE-2021-37714	Oracle Stream Analytics	Oracle Stream Analytics (jsoup)	HTTP	No	4.9	Network	Low	High

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

- Oracle GoldenGate
  - General (Apache Log4j): CVE-2022-23307, CVE-2019-17571, CVE-2021-4104, CVE-2022-23302 and CVE-2022-23305.
  - Oracle GoldenGate (zlib): CVE-2018-25032.
- Oracle Stream Analytics
  - Install (Apache Log4j): CVE-2022-23305, CVE-2019-17571, CVE-2021-4104, CVE-2022-23302 and CVE-2022-23307.

Oracle Graph Server and Client Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle Graph Server and Client. 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 Int
CVE-2020-36518	Oracle Graph Server and Client	Oracle Graph Server (jackson-databind)	HTTP	No	6.5	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 Graph Server and Client
  - Install (Apache Tomcat): CVE-2022-23181 and CVE-2020-9484.

Oracle NoSQL Database Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle NoSQL Database. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle NoSQL 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 NoSQL Database
  - Administration (Netty): CVE-2021-43797.

Oracle REST Data Services Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-41184	Oracle REST Data Services	Oracle REST Data Services (jQueryUI)	HTTP	Yes	6.1	Network	Low	None	Re
CVE-2021-34429	Oracle REST Data Services	Oracle REST Data Services (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	None	

Additional CVEs addressed are:

- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.

Oracle Spatial Studio Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Spatial Studio. 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 Int
CVE-2020-36518	Oracle Spatial Studio	Oracle Spatial Studio (jackson-databind)	HTTP	No	6.5	Network	Low	Low	N

Oracle SQL Developer Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle SQL Developer. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for Oracle SQL Developer. 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 SQL Developer
  - Oracle SQL Developer (Apache PDFBox): CVE-2021-31812 and CVE-2021-31811.

Oracle TimesTen In-Memory Database Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle TimesTen In-Memory Database. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2021-2351	Oracle TimesTen In-Memory Database	Oracle TimesTen In-Memory Database Cache	Oracle Net	Yes	8.3	Network	High	None	Rec

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
  - Kubernetes Operator (Go): CVE-2022-23806, CVE-2021-41771, CVE-2021-41772, CVE-2022-23772 and CVE-2022-23773.
  - TimesTen Grid (Apache Log4j): CVE-2022-23305, CVE-2021-4104, CVE-2022-23302 and CVE-2022-23307.

Oracle Commerce Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Commerce. 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			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2020-10683	Oracle Commerce Guided Search	Content Acquisition System (dom4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2019-17495	Oracle Commerce Guided Search	Framework, Experience Manager (Swagger UI)	HTTP	Yes	9.8	Network	Low	No
CVE-2022-22965	Oracle Commerce	Endeca Integration	HTTP	Yes	9.8	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
	Platform	(Spring Framework)						
CVE-2020-28052	Oracle Commerce Guided Search	Framework, Experience Manager (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	No
CVE-2021-40690	Oracle Commerce Guided Search	Content Acquisition System (Apache CXF)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-22946	Oracle Commerce Guided Search	Framework, Experience Manager (cURL)	HTTP	Yes	7.5	Network	Low	No
CVE-2022-24729	Oracle Commerce Merchandising	Core (CKEditor)	HTTP	Yes	7.5	Network	Low	No
CVE-2020-36518	Oracle Commerce Platform	Dynamo Application Framework (jackson-databind)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-40690	Oracle Commerce Platform	Endeca Integration (Apache CXF)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-3450	Oracle Commerce Guided Search	Framework, Experience Manager (OpenSSL)	TLS	Yes	7.4	Network	High	No
CVE-2020-7712	Oracle Commerce Guided Search	Framework, Experience Manager (Apache ZooKeeper)	HTTP	No	7.2	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2022-21559	Oracle Commerce Platform	Dynamo Application Framework	None	No	5.5	Local	Low	Lo

Additional CVEs addressed are:

- The patch for CVE-2021-22946 also addresses CVE-2021-22947.
- The patch for CVE-2021-3450 also addresses CVE-2021-3449.
- The patch for CVE-2022-24729 also addresses CVE-2022-24728.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 17 new security patches plus additional third party patches noted below 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-2022-23305	Oracle Communications Instant Messaging Server	XMPP Server (Apache Log4j)	XMPP	Yes	9.8	Network	Low	
CVE-2022-23305	Oracle Communications Offline Mediation Controller	Charging Server (Apache Log4j)	LDAP	Yes	9.8	Network	Low	
CVE-2022-23632	Oracle Communications Unified Inventory Management	Cloud Native (Traefik)	HTTP	Yes	9.8	Network	Low	
CVE-2022-22965	Oracle Communications	TMF APIs (Spring	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Unified Inventory Management	Framework)						
CVE-2022-21429	Oracle Communications Billing and Revenue Management	Billing Care	HTTP	Yes	8.1	Network	High	
CVE-2020-36518	Oracle Communications Billing and Revenue Management	Billing Care, BOC, DM Kafka, REST API (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2021-37137	Oracle Communications BRM - Elastic Charging Engine	5G gateway (Google Snappy)	HTTP	Yes	7.5	Network	Low	
CVE-2021-43859	Oracle Communications BRM - Elastic Charging Engine	EM Gateway (XStream)	TCP	Yes	7.5	Network	Low	
CVE-2021-44832	Oracle Communications BRM - Elastic Charging Engine	Charging Server (Apache Log4j)	TCP	No	6.6	Network	High	
CVE-2021-44832	Oracle Communications Offline Mediation Controller	Admin Server and Node Manager (Apache Log4j)	LDAP	No	6.6	Network	High	
CVE-2022-23437	Oracle Communications ASAP	SRT (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	
CVE-2022-21573	Oracle Communications Billing and Revenue Management	Billing Care	HTTP	No	6.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-43797	Oracle Communications Design Studio	PSR Designer (Netty)	HTTP	Yes	6.5	Network	Low	
CVE-2022-22969	Oracle Communications Design Studio	Patch Request (Spring Security OAuth)	HTTP	No	6.5	Network	Low	
CVE-2021-38153	Oracle Communications BRM - Elastic Charging Engine	Notifications (Apache Kafka)	TCP	Yes	5.9	Network	High	
CVE-2022-21572	Oracle Communications Billing and Revenue Management	Billing Care	HTTP	No	5.4	Network	Low	
CVE-2022-21574	Oracle Communications Billing and Revenue Management	Connection Manager	HTTP	Yes	5.3	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2021-37137 also addresses CVE-2021-37136.
- The patch for CVE-2021-38153 also addresses CVE-2021-26291.
- The patch for CVE-2022-23305 also addresses CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.

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

- Oracle Communications BRM - Elastic Charging Engine
  - Charging Server (Spring Framework): CVE-2022-22965.
- Oracle Communications IP Service Activator
  - Network Processor (Apache Xerces-J): CVE-2022-23437.

Oracle Communications Risk Matrix

This Critical Patch Update contains 56 new security patches plus additional third party patches noted below for Oracle Communications. 45 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-2022-22947	Oracle Communications Cloud Native Core Binding Support Function	BSF (Spring Cloud Gateway)	HTTP	Yes	10.0	Network	Low	
CVE-2022-22947	Oracle Communications Cloud Native Core Console	CNC Console (Spring Cloud Gateway)	HTTP	Yes	10.0	Network	Low	
CVE-2022-22947	Oracle Communications Cloud Native Core Network Repository Function	NRF (Spring Cloud Gateway)	HTTP	Yes	10.0	Network	Low	
CVE-2022-22947	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (Spring Cloud Gateway)	HTTP	Yes	10.0	Network	Low	
CVE-2022-22965	Oracle Communications Cloud Native Core Binding Support Function	BSF (Spring Framework)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23219	Oracle Communications Cloud Native	BSF (glibc)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Core Binding Support Function							
CVE-2022-1154	Oracle Communications Cloud Native Core Network Exposure Function	NEF (vim)	HTTP	Yes	9.8	Network	Low	
CVE-2020-14343	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	CNE (PyYAML)	HTTP	Yes	9.8	Network	Low	
CVE-2021-3177	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	CNE (Python)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23219	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	CNE (glibc)	HTTP	Yes	9.8	Network	Low	
CVE-2022-22963	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	DBTier (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23219	Oracle Communications Cloud Native Core Network	NRF (glibc)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Repository Function							
CVE-2022-22963	Oracle Communications Cloud Native Core Policy	Policy (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23219	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (glibc)	HTTP	Yes	9.8	Network	Low	
CVE-2022-25845	Oracle Communications Cloud Native Core Unified Data Repository	UDR (fastjson)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23219	Oracle Communications Cloud Native Core Unified Data Repository	UDR (glibc)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23219	Oracle Enterprise Operations Monitor	Mediation Engine (glibc)	TCP/IP	Yes	9.8	Network	Low	
CVE-2022-24407	Oracle Communications Cloud Native Core Console	CNC Console (Cyrus SASL)	HTTP	No	8.8	Network	Low	
CVE-2022-24407	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	CNE (Cyrus SASL)	HTTP	No	8.8	Network	Low	
CVE-2022-24407	Oracle Communications Cloud Native Core Security	SEPP (Cyrus SASL)	HTTP	No	8.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Edge Protection Proxy							
CVE-2022-25636	Oracle Communications Cloud Native Core Binding Support Function	Oracle Linux	None	No	7.8	Local	Low	
CVE-2022-25636	Oracle Communications Cloud Native Core Network Exposure Function	Oracle Linux	None	No	7.8	Local	Low	
CVE-2022-25636	Oracle Communications Cloud Native Core Policy	Oracle Linux	None	No	7.8	Local	Low	
CVE-2022-24735	Oracle Communications Operations Monitor	Fraud Detection Monitor (Redis)	None	No	7.8	Local	Low	N
CVE-2020-36518	Oracle Communications Cloud Native Core Binding Support Function	BSF (jackson-databind)	HTTP	Yes	7.5	Network	Low	N
CVE-2022-23308	Oracle Communications Cloud Native Core Binding Support Function	BSF (libxml2)	HTTP	Yes	7.5	Network	Low	N
CVE-2018-25032	Oracle Communications Cloud Native Core Console	CNC Console (zlib)	HTTP	Yes	7.5	Network	Low	N
CVE-2018-25032	Oracle Communications Cloud Native	NEF (zlib)	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Core Network Exposure Function							
CVE-2019-20916	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	CNE (Package Installer for Python)	HTTP	Yes	7.5	Network	Low	
CVE-2022-23308	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	CNE (libxml2)	HTTP	Yes	7.5	Network	Low	
CVE-2021-22119	Oracle Communications Cloud Native Core Network Repository Function	NRF (Spring Security)	HTTP	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle Communications Cloud Native Core Network Repository Function	NRF (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2022-23308	Oracle Communications Cloud Native Core Network Repository Function	NRF (libxml2)	HTTP	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (jackson-databind)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2022-23308	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (libxml2)	HTTP	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2018-25032	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (zlib)	HTTP	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle Communications Cloud Native Core Unified Data Repository	UDR (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2022-23308	Oracle Communications Cloud Native Core Unified Data Repository	UDR (libxml2)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2018-25032	Oracle Communications Cloud Native Core Unified Data Repository	UDR (zlib)	HTTP	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Communications Cloud Native Core Unified Data Repository	UDR (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Communications Core Session Manager	Security (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Communications Operations Monitor	Mediation Engine (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Communications Session Border Controller	Security (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Communications Unified Session Manager	Security (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Enterprise Communications Broker	Security (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2022-0778	Oracle Enterprise Session Border Controller	Security (OpenSSL)	TLS	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle SD-WAN Edge	MGMT (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2022-1271	Oracle Communications	CNC Console (GNU Gzip)	HTTP	No	7.1	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Cloud Native Core Console							
CVE-2022-1271	Oracle Communications Cloud Native Core Unified Data Repository	UDR (GNU Gzip)	HTTP	No	7.1	Network	High	
CVE-2021-37750	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (MIT Kerberos)	HTTP	No	6.5	Network	Low	
CVE-2021-3572	Oracle Communications Cloud Native Core Policy	Policy (Package Installer for Python)	HTTP	No	5.7	Network	Low	
CVE-2022-24329	Oracle Communications Cloud Native Core Binding Support Function	BSF (JetBrains Kotlin)	HTTP	Yes	5.3	Network	Low	
CVE-2021-34141	Oracle Communications Cloud Native Core Policy	Policy (NumPy)	HTTP	Yes	5.3	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2019-20916 also addresses CVE-2021-3572.
- The patch for CVE-2020-14343 also addresses CVE-2020-1747.
- The patch for CVE-2021-3177 also addresses CVE-2018-18074, CVE-2019-20916, CVE-2019-9636, CVE-2019-9740, CVE-2020-26137, and CVE-2020-27619.
- The patch for CVE-2022-22947 also addresses CVE-2022-22946, and CVE-2022-22965.
- The patch for CVE-2022-22963 also addresses CVE-2022-22965.
- The patch for CVE-2022-23219 also addresses CVE-2021-38604, CVE-2021-43396, and CVE-2022-23218.
- The patch for CVE-2022-24735 also addresses CVE-2022-24736.

- The patch for CVE-2022-25636 also addresses CVE-2018-25032, CVE-2020-0404, CVE-2020-13974, CVE-2020-27820, CVE-2020-4788, CVE-2021-20322, CVE-2021-21781, CVE-2021-29154, CVE-2021-3612, CVE-2021-3672, CVE-2021-37159, CVE-2021-3737, CVE-2021-3743, CVE-2021-3744, CVE-2021-3752, CVE-2021-3772, CVE-2021-3773, CVE-2021-4002, CVE-2021-4083, CVE-2021-4157, CVE-2021-4197, CVE-2021-4203, CVE-2021-42739, CVE-2021-43389, CVE-2021-43818, CVE-2021-43976, CVE-2021-45485, CVE-2021-45486, CVE-2022-0001, CVE-2022-0002, CVE-2022-0286, CVE-2022-0322, and CVE-2022-1011.

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

- Oracle Communications Cloud Native Core Network Slice Selection Function
  - NSSF (glibc): CVE-2022-23219, CVE-2021-38604, CVE-2021-43396 and CVE-2022-23218.
- Oracle Communications Cloud Native Core Security Edge Protection Proxy
  - SEPP (Spring Framework): CVE-2022-22968 and CVE-2022-22965.
- Oracle Communications Cloud Native Core Service Communication Proxy
  - SCP (Spring Boot): CVE-2022-22968 and CVE-2022-22965.
- Oracle Communications Cloud Native Core Unified Data Repository
  - UDR (Libgcrypt): CVE-2021-33560.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 7 new security patches plus additional third party patches noted below for Oracle Construction and Engineering. 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			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2022-21558	Oracle Crystal Ball	Installation	None	No	7.8	Local	High	Lov
CVE-2020-36518	Primavera Gateway	Admin (jackson-databind)	HTTP	Yes	7.5	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-36518	Primavera Unifier	Document Management (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2022-23437	Primavera Gateway	Admin (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	Nor
CVE-2020-36518	Primavera P6 Enterprise Project Portfolio Management	Web Access (jackson-databind)	HTTP	No	6.5	Network	Low	Lo
CVE-2022-23437	Primavera Unifier	Platform, User Interface (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	Nor
CVE-2022-30126	Primavera Unifier	Document Management (Apache Tika)	None	No	5.5	Local	Low	Nor

Additional CVEs addressed are:

- The patch for CVE-2022-30126 also addresses CVE-2021-33813, and CVE-2022-25169.

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

- Primavera Gateway
    - Admin (Spring Framework): CVE-2022-22965.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle E-Business Suite. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

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 July 2022 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 (July 2022), My Oracle Support Note 2484000.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2022-23305	Oracle E-Business Suite Information Discovery	Packaging issues (Apache Log4j)	HTTP	Yes	9.8	Network	Low	Non
CVE-2022-21566	Oracle Applications Framework	Diagnostics	HTTP	Yes	7.5	Network	Low	Non
CVE-2022-21500	Oracle User Management	Proxy User Delegation	HTTP	Yes	7.5	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2022-21567	Oracle Workflow	Worklist	HTTP	Yes	7.5	Network	Low	None
CVE-2022-21568	Oracle iReceivables	Access Request	HTTP	No	6.5	Network	Low	Low
CVE-2022-21545	Oracle iRecruitment	Candidate Self Service Registration	HTTP	Yes	5.3	Network	Low	None

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 6 new security patches plus additional third party patches noted below for Oracle Enterprise Manager. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found here.

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the July 2022 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 July 2022 Patch Availability Document for Oracle Products, My Oracle Support Note 2867874.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2022-22721	Enterprise Manager Ops Center	Networking (Apache	HTTP	Yes	9.8	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
		HTTP Server)						
CVE-2022-1292	Enterprise Manager Ops Center	Networking (OpenSSL)	HTTPS	Yes	9.8	Network	Low	None
CVE-2022-21536	Enterprise Manager Base Platform	Policy Framework	HTTP	Yes	8.1	Network	High	None
CVE-2020-5258	Oracle Application Testing Suite	Load Testing for Web Apps (Dojo)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-21516	Enterprise Manager Base Platform	Enterprise Manager Install	HTTP	Yes	7.3	Network	Low	None
CVE-2022-29577	Enterprise Manager Base Platform	Enterprise Manager Install (AntiSamy)	HTTP	Yes	6.1	Network	Low	None

Additional CVEs addressed are:

- The patch for CVE-2022-1292 also addresses CVE-2021-4160, and CVE-2022-0778.
- The patch for CVE-2022-22721 also addresses CVE-2022-22720.

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

- Enterprise Manager for MySQL Database
    - EM Plugin: General (Spring Framework): CVE-2022-22965.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 59 new security patches for Oracle Financial Services Applications. 38 of these vulnerabilities may be remotely exploitable without authentication,

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-22963	Oracle Banking Branch	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Cash Management	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Corporate Lending Process Management	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Credit Facilities Process Management	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Electronic Data Exchange for Corporates	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Liquidity Management	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Origination	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Supply Chain Finance	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-22963	Oracle Banking Trade Finance Process Management	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22963	Oracle Banking Virtual Account Management	Common (Spring Cloud Function)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2021-41303	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache Shiro)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2018-1273	Oracle Financial Services Crime and Compliance Management Studio	Studio (Spring Data Commons)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2022-22978	Oracle Financial Services Crime and Compliance Management Studio	Studio (Spring Security)	HTTP	Yes	9.8	Network	Low	Nc
CVE-2020-9492	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache Hadoop)	HTTP	No	8.8	Network	Low	Lc
CVE-2020-9492	Oracle Financial Services	Studio (Apache Solr)	HTTP	No	8.8	Network	Low	Lc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Crime and Compliance Management Studio							
CVE-2022-24729	Oracle Financial Services Analytical Applications Infrastructure	Others (CKEditor)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2020-36518	Oracle Financial Services Analytical Applications Infrastructure	Others (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2022-24729	Oracle Financial Services Behavior Detection Platform	Third Party (CKEditor)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2020-36518	Oracle Financial Services Behavior Detection Platform	Web UI (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-36090	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-38296	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache Spark)	HTTP	Yes	7.5	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-25647	Oracle Financial Services Crime and Compliance Management Studio	Studio (Google GSON)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2020-36518	Oracle Financial Services Crime and Compliance Management Studio	Studio (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-37714	Oracle Financial Services Crime and Compliance Management Studio	Studio (jsoup)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2022-24729	Oracle Financial Services Enterprise Case Management	Installers (CKEditor)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2020-36518	Oracle Financial Services Enterprise Case Management	Installers (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2022-24729	Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition	User Interface (CKEditor)	HTTP	Yes	7.5	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-36518	Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition	User Interface (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-40690	Oracle FLEXCUBE Private Banking	Infrastructure (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-43859	Oracle FLEXCUBE Private Banking	Infrastructure (XStream)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2020-7712	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache ZooKeeper)	HTTP	No	7.2	Network	Low	Hi
CVE-2021-23337	Oracle Financial Services Crime and Compliance Management Studio	Studio (Lodash)	HTTP	No	7.2	Network	Low	Hi
CVE-2022-21544	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	7.1	Network	High	Lc
CVE-2022-23181	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache Tomcat)	None	No	7.0	Local	High	Lc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-21582	Oracle Banking Trade Finance	Infrastructure	HTTP	No	6.7	Network	High	Lo
CVE-2022-21585	Oracle Banking Trade Finance	Infrastructure	HTTP	No	6.7	Network	High	Lo
CVE-2022-21428	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.7	Network	High	Lo
CVE-2022-21578	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.7	Network	High	Lo
CVE-2021-44832	Oracle FLEXCUBE Private Banking	Infrastructure (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2022-23437	Oracle Banking Deposits and Lines of Credit Servicing	Web UI (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2021-43797	Oracle Banking Deposits and Lines of Credit Servicing	Web UI (Netty)	HTTP	Yes	6.5	Network	Low	No
CVE-2022-23437	Oracle Banking Party Management	Web UI (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2021-43797	Oracle Banking Party Management	Web UI (Netty)	HTTP	Yes	6.5	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-43797	Oracle Banking Platform	SECURITY (Netty)	HTTP	Yes	6.5	Network	Low	No
CVE-2022-23437	Oracle Financial Services Crime and Compliance Management Studio	Studio (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2022-22971	Oracle Financial Services Crime and Compliance Management Studio	Studio (Spring Framework)	HTTP	No	6.5	Network	Low	Lo
CVE-2022-23437	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2022-21583	Oracle Banking Trade Finance	Infrastructure	HTTP	No	6.4	Network	High	Lo
CVE-2022-21584	Oracle Banking Trade Finance	Infrastructure	HTTP	No	6.4	Network	High	Lo
CVE-2022-21586	Oracle Banking Trade Finance	Infrastructure	HTTP	No	6.4	Network	High	Lo
CVE-2022-21576	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.4	Network	High	Lo
CVE-2022-21577	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.4	Network	High	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-21579	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	6.4	Network	High	Lo
CVE-2021-41184	Oracle Banking Platform	SECURITY (jQueryUI)	HTTP	Yes	6.1	Network	Low	No
CVE-2022-21581	Oracle Banking Trade Finance	Infrastructure	HTTP	No	5.9	Network	High	Lo
CVE-2022-21580	Oracle Financial Services Revenue Management and Billing	Infrastructure	HTTP	No	5.9	Network	High	Lo
CVE-2022-24823	Oracle Financial Services Crime and Compliance Management Studio	Studio (Netty)	None	No	5.5	Local	Low	Lo
CVE-2021-34429	Oracle Financial Services Crime and Compliance Management Studio	Studio (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	No
CVE-2021-29425	Oracle FLEXCUBE Core Banking	Securities (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No

Additional CVEs addressed are:

- The patch for CVE-2018-1273 also addresses CVE-2018-1259, and CVE-2018-1274.
- The patch for CVE-2021-23337 also addresses CVE-2020-28500.

- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.
- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.
- The patch for CVE-2022-22971 also addresses CVE-2022-22970.
- The patch for CVE-2022-22978 also addresses CVE-2022-22976.
- The patch for CVE-2022-24729 also addresses CVE-2022-24728.

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Food and Beverage 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Hospitality Inventory Management	Installation (ODP for .NET)	Oracle Net	Yes	7.5	Network	High	None
CVE-2021-41184	Oracle Hospitality Inventory Management	Receipt (jQueryUI)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-41184	Oracle Hospitality Materials Control	Receipt (jQueryUI)	HTTP	Yes	6.1	Network	Low	None

Additional CVEs addressed are:

- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 38 new security patches plus additional third party patches noted below for Oracle Fusion Middleware. 32 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 July 2022 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 July 2022 Patch Availability Document for Oracle Products, My Oracle Support Note 2880163.2.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-42575	Oracle Middleware Common Libraries and Tools	Third Party Patch (AntiSamy)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23457	Oracle WebLogic Server	Centralized Third Party Jars (OWASP Enterprise Security API)	HTTP	Yes	9.8	Network	Low	N
CVE-2021-23450	Oracle WebLogic Server	Sample apps (Dojo)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-22965	Oracle WebLogic Server	Third Party Tools, Samples (Spring Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10082	Oracle HTTP Server	SSL Module (Apache HTTP Server)	HTTP	Yes	9.1	Network	Low	N
CVE-2020-35169	Oracle HTTP Server	SSL Module (Dell BSAFE Micro Edition Suite)	HTTPS	Yes	9.1	Network	Low	N
CVE-2021-23926	Oracle Middleware	Thirdparty Patch (Apache	HTTP	Yes	9.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Common Libraries and Tools	XMLBeans)						
CVE-2020-35169	Oracle Security Service	C Oracle SSL API (Dell BSAFE Micro Edition Suite)	HTTPS	Yes	9.1	Network	Low	N
CVE-2021-26291	Oracle WebLogic Server	Centralized Third Party Jars (Apache Maven)	HTTP	Yes	9.1	Network	Low	N
CVE-2020-35169	Oracle Weblogic Server Proxy Plug-in	SSL Module (Dell BSAFE Micro Edition Suite)	HTTPS	Yes	9.1	Network	Low	N
CVE-2021-39139	Oracle WebCenter Portal	Security Framework (XStream)	HTTP	No	8.8	Network	Low	L
CVE-2021-2351	Oracle WebLogic Server	Installer (OCCI)	Oracle Net	Yes	8.3	Network	High	N
CVE-2020-11987	Oracle WebLogic Server	Centralized Third Party Jars (Apache Batik)	HTTP	Yes	8.2	Network	Low	N
CVE-2019-0227	Oracle BI Publisher	BI Publisher Security (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	N
CVE-2020-36518	Oracle Coherence	Centralized Thirdparty Jars (jackson-databind)	HTTP	Yes	7.5	Network	Low	N
CVE-2022-21570	Oracle Coherence	Core	T3, IIOP	Yes	7.5	Network	Low	N
CVE-2020-36518	Oracle Global Lifecycle Management	NextGen Installer issues (jackson-databind)	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	NextGen OUI Framework							
CVE-2021-42340	Oracle Managed File Transfer	MFT Runtime Server (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-37714	Oracle Middleware Common Libraries and Tools	Thirdparty Patch (jsoup)	HTTP	Yes	7.5	Network	Low	N
CVE-2022-21562	Oracle SOA Suite	Fabric Layer	HTTP	Yes	7.5	Network	Low	N
CVE-2020-36518	Oracle WebLogic Server	Centralized Third Party Jars (jackson-databind)	HTTP	Yes	7.5	Network	Low	N
CVE-2022-24839	Oracle WebLogic Server	Centralized Third Party Jars (NekoHTML)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-28491	Oracle WebLogic Server	Centralized Third Party Jars (jackson-dataformats-binary)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-40690	Oracle WebLogic Server	Centralized Thirdparty Jars (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2022-21552	Oracle WebCenter Content	Search	HTTP	Yes	7.2	Network	Low	N
CVE-2021-35940	Oracle HTTP Server	SSL Module (Apache Portable Runtime)	None	No	7.1	Local	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-30129	Oracle Global Lifecycle Management NextGen OUI Framework	NextGen Installer issues (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	L
CVE-2022-23437	Oracle Global Lifecycle Management NextGen OUI Framework	NextGen Installer issues (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2022-21548	Oracle WebLogic Server	Core	T3, IIOP	Yes	6.5	Network	Low	N
CVE-2020-11023	Oracle Business Intelligence Enterprise Edition	Service Administration UI (JQuery)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-1927	Oracle HTTP Server	SSL Module (Apache HTTP Server)	HTTP	Yes	6.1	Network	Low	N
CVE-2022-29577	Oracle WebLogic Server	Centralized Third Party Jars (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2022-21575	Oracle WebCenter Sites Support Tools	User Interface	HTTP	No	6.0	Network	Low	H
CVE-2022-21557	Oracle WebLogic Server	Web Container	None	No	5.7	Local	High	H
CVE-2019-0220	Oracle HTTP Server	Web Listener (Apache HTTP Server)	HTTP	Yes	5.3	Network	Low	N
CVE-2022-21560	Oracle WebLogic Server	Core	T3, IIOP	Yes	5.3	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2022-21564	Oracle WebLogic Server	Web Services	T3, IIOP	Yes	5.3	Network	Low	N
CVE-2022-21523	Oracle BI Publisher	BI Publisher Security	HTTP	No	4.3	Network	Low	L

Additional CVEs addressed are:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2020-11023 also addresses CVE-2020-11022.
- The patch for CVE-2020-35169 also addresses CVE-2020-26184, CVE-2020-26185, and CVE-2020-29507.
- The patch for CVE-2021-39139 also addresses CVE-2021-39140, CVE-2021-39141, CVE-2021-39144, CVE-2021-39145, CVE-2021-39146, CVE-2021-39147, CVE-2021-39148, CVE-2021-39149, CVE-2021-39150, CVE-2021-39151, CVE-2021-39152, CVE-2021-39153, and CVE-2021-39154.
- The patch for CVE-2021-42340 also addresses CVE-2020-9484, and CVE-2022-23181.
- The patch for CVE-2021-42575 also addresses CVE-2021-35043.
- The patch for CVE-2022-23457 also addresses CVE-2022-24891.

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

- Oracle BI Publisher
  - Web Service API (Spring Framework): CVE-2022-22965, CVE-2020-5397 and CVE-2020-5398.
- Oracle Business Intelligence Enterprise Edition
  - Analytics Server (Spring Framework): CVE-2022-22965, CVE-2020-5397 and CVE-2020-5398.
- Oracle Data Integrator
  - Runtime Java agent for ODI (Spring Framework): CVE-2022-22965, CVE-2020-5397 and CVE-2020-5398.
- Oracle Identity Management Suite
  - Installer (Spring Framework): CVE-2022-22965, CVE-2020-5397 and CVE-2020-5398.

- Oracle Identity Manager Connector
  - General and Misc (Spring Framework): CVE-2022-22965, CVE-2020-5397 and CVE-2020-5398.
- Oracle Middleware Common Libraries and Tools
  - Third Party Patch (Spring Framework): CVE-2022-22965, CVE-2020-5397 and CVE-2020-5398.

Oracle Health Sciences Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-36518	Oracle Health Sciences Empirica Signal	Web Services (jackson-databind)	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-10086	Oracle Health Sciences Data Management Workbench	User Interface (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	Non
CVE-2021-23337	Oracle Health Sciences Data Management Workbench	User Interface (Lodash)	HTTP	No	7.2	Network	Low	High
CVE-2021-44832	Oracle Health Sciences Data Management Workbench	User Interface (Apache Log4j)	HTTP	No	6.6	Network	High	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2022-21518	Oracle Health Sciences Data Management Workbench	User Interface	HTTP	No	6.5	Network	Low	Low
CVE-2021-29425	Oracle Health Sciences Data Management Workbench	User Interface (Apache Commons IO)	HTTP	Yes	4.8	Network	High	Non

Additional CVEs addressed are:

- The patch for CVE-2021-23337 also addresses CVE-2020-28500.

Oracle HealthCare Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-33813	Oracle Healthcare Foundation	Upload Service (Apache Tika)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-23437	Oracle Health Sciences Information Manager	Health Policy Engine (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	None
CVE-2021-36374	Oracle Health	Health Policy	None	No	5.5	Local	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	Sciences Information Manager	Engine (Apache Ant)						

Additional CVEs addressed are:

- The patch for CVE-2021-36374 also addresses CVE-2021-36373.

Oracle Hospitality Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-31805	Oracle Hospitality OPERA 5	Login (Apache Struts)	HTTP	Yes	9.8	Network	Low	Non
CVE-2022-29885	Oracle Hospitality Cruise Shipboard Property Management System	Next-Gen SPMS (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	Non

Oracle Java SE Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle Java SE. 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2022-34169	Oracle Java SE, Oracle GraalVM Enterprise Edition	JAXP (Xalan-J)	Multiple	Yes	7.5	Network	Low	None	
CVE-2022-25647	Oracle GraalVM Enterprise Edition	Native Image (Gson)	None	No	6.2	Local	Low	None	
CVE-2022-21541	Oracle Java SE, Oracle GraalVM Enterprise Edition	Hotspot	Multiple	Yes	5.9	Network	High	None	
CVE-2022-21540	Oracle Java SE, Oracle GraalVM Enterprise Edition	Hotspot	Multiple	Yes	5.3	Network	Low	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-2022-21549	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.3	Network	Low	None	

Notes:

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

Oracle JD Edwards Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-22931	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech - Cloud (Node.js)	HTTP	Yes	9.8	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-31684	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator (JSON Smart)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2022-21542	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	No	7.4	Network	Low	Lov
CVE-2022-21561	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	No	6.5	Network	Low	Lov
CVE-2021-41184	JD Edwards EnterpriseOne Tools	Web Runtime (jQueryUI)	HTTP	Yes	6.1	Network	Low	Nor
CVE-2022-21532	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator	HTTP	No	4.3	Network	Low	Lov

Additional CVEs addressed are:

- The patch for CVE-2021-22931 also addresses CVE-2021-22939, and CVE-2021-22940.
- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 34 new security patches plus additional third party patches noted below 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			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-31805	MySQL Enterprise Monitor	Monitoring: General (Apache Struts)	Multiple	Yes	9.8	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-1292	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	Yes	9.8	Network	Low	Nc
CVE-2022-1292	MySQL Workbench	Workbench (OpenSSL)	MySQL Workbench	Yes	9.8	Network	Low	Nc
CVE-2022-21824	MySQL Cluster	Cluster: General (Node.js)	Multiple	Yes	8.2	Network	Low	Nc
CVE-2022-27778	MySQL Server	Server: Packaging (cURL)	MySQL Protocol	Yes	8.1	Network	Low	Nc
CVE-2021-22119	MySQL Enterprise Monitor	Monitoring: General (Spring Security)	Multiple	Yes	7.5	Network	Low	Nc
CVE-2018-25032	MySQL Server	Server: Compiling (zlib)	MySQL Protocol	Yes	7.5	Network	Low	Nc
CVE-2022-23308	MySQL Workbench	Workbench (libxml2)	MySQL Workbench	Yes	7.5	Network	Low	Nc
CVE-2020-26237	MySQL Enterprise Monitor	Monitoring: General (highlight.js)	Multiple	No	6.8	Network	Low	Lc
CVE-2022-21556	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Hi
CVE-2022-21569	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lc
CVE-2022-21550	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High	Hi
CVE-2022-21519	MySQL Cluster	Cluster: General	Multiple	Yes	5.9	Network	High	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-21527	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low	Hi
CVE-2022-21528	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low	Hi
CVE-2022-21509	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low	Hi
CVE-2022-22968	MySQL Enterprise Monitor	Service Manager (Spring Framework)	Multiple	Yes	5.3	Network	Low	No
CVE-2022-21539	MySQL Server	InnoDB	MySQL Protocol	No	5.0	Network	High	Lo
CVE-2022-21517	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21537	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21547	MySQL Server	Server: Federated	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21525	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21526	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21529	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21530	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21531	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21553	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21515	MySQL Server	Server: Options	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21455	MySQL Server	Server: PAM Auth Plugin	MySQL Protocol	No	4.9	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-21534	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2022-21522	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2022-21555	MySQL Shell for VS Code	Shell: GUI	None	No	4.2	Local	Low	Hi
CVE-2022-21538	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	3.1	Network	High	Lo
CVE-2022-21535	MySQL Shell	Shell: General/Core Client	None	No	2.5	Local	High	No

Additional CVEs addressed are:

- The patch for CVE-2022-21824 also addresses CVE-2021-44531, CVE-2021-44532, and CVE-2021-44533.

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

- MySQL Enterprise Monitor
  - Service Manager (OpenSSL): CVE-2022-1292.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle PeopleSoft. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2022-21543	PeopleSoft Enterprise PeopleTools	Updates Environment Mgmt	HTTP	Yes	9.8	Network	Low	None
CVE-2020-36518	PeopleSoft Enterprise PeopleTools	Elastic Search (jackson-databind)	HTTP	Yes	7.5	Network	Low	None
CVE-2018-25032	PeopleSoft Enterprise PeopleTools	PeopleSoft CDA (zlib)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-24729	PeopleSoft Enterprise PeopleTools	Rich Text Editor (CKEditor)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-31684	PeopleSoft Enterprise PeopleTools	Security (JSON Smart)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-23437	PeopleSoft Enterprise PeopleTools	Security (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	None
CVE-2022-21520	PeopleSoft Enterprise PeopleTools	Fluid Core	HTTP	Yes	6.1	Network	Low	None
CVE-2020-7656	PeopleSoft Enterprise PeopleTools	PeopleSoft CDA (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-41182	PeopleSoft Enterprise PeopleTools	XML Publisher (jQueryUI)	HTTP	Yes	6.1	Network	Low	None
CVE-2022-21521	PeopleSoft Enterprise PeopleTools	XML Publisher	HTTP	No	4.9	Network	Low	High
CVE-2022-21512	PeopleSoft Enterprise PeopleTools	Integration Broker	None	No	4.4	Local	Low	High

Additional CVEs addressed are:

- The patch for CVE-2021-41182 also addresses CVE-2021-41183, and CVE-2021-41184.
- The patch for CVE-2022-24729 also addresses CVE-2022-24728.

Oracle Policy Automation Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Policy Automation. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-44832	Oracle Policy Automation	Determinations Engine (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Oracle Policy Automation for Mobile Devices	Core Functionality (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-41184	Oracle Policy Automation	Determinations Engine (jQueryUI)	HTTP	Yes	6.1	Network	Low	No

Additional CVEs addressed are:

- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 17 new security patches for Oracle Retail Applications. 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-2022-22965	Oracle Retail Bulk Data	BDI Job Scheduler	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Integration	(Spring Framework)						
CVE-2022-22965	Oracle Retail Customer Management and Segmentation Foundation	Security (Spring Framework)	HTTP	Yes	9.8	Network	Low	
CVE-2022-23305	Oracle Retail Extract Transform and Load	Mathematical Operators (Apache Log4j)	HTTP	Yes	9.8	Network	Low	
CVE-2022-22965	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Spring Framework)	HTTP	Yes	9.8	Network	Low	
CVE-2022-22965	Oracle Retail Integration Bus	RIB Kernal (Spring Framework)	HTTP	Yes	9.8	Network	Low	
CVE-2022-22965	Oracle Retail Merchandising System	Foundation (Spring Framework)	HTTP	Yes	9.8	Network	Low	
CVE-2021-29505	Oracle Retail Customer Insights	Other (XStream)	HTTP	No	8.8	Network	Low	
CVE-2021-22118	Oracle Retail Customer Insights	Other (Spring Framework)	None	No	7.8	Local	Low	
CVE-2022-25647	Oracle Retail Order Broker	System Administration (Google GSON)	HTTP	Yes	7.5	Network	Low	
CVE-2020-36518	Oracle Retail Sales Audit	others (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2019-10086	Oracle Retail Allocation	General (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 Sales Audit	others (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2021-44832	Oracle Retail Order Broker	Internal Operations (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Xstore Point of Service	Xenvironment (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-29425	Oracle Retail Merchandising System	Foundation (Apache Commons IO)	HTTP	Yes	4.8	Network	High	
CVE-2021-29425	Oracle Retail Pricing	Pricing - Security (Apache Commons IO)	HTTP	Yes	4.8	Network	High	
CVE-2021-29425	Oracle Retail Xstore Point of Service	Xenvironment (Apache Commons IO)	HTTP	Yes	4.8	Network	High	

Additional CVEs addressed are:

- The patch for CVE-2022-23305 also addresses CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Siebel CRM. 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	Use Inter
CVE-2021-31812	Siebel Apps - Field Service	Smart Answer (Apache PDFBox)	None	No	5.5	Local	Low	None	Requ

Additional CVEs addressed are:

- The patch for CVE-2021-31812 also addresses CVE-2021-31811.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 24 new security patches for Oracle Supply Chain. 19 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 Agile Engineering Data Management	Installation Issues (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2019-0219	Oracle Transportation Management	Mobile Applications (Apache cordova-plugin-inappbrowser)	HTTP	Yes	9.8	Network	Low	
CVE-2022-25762	Oracle Agile PLM	Security (Apache Tomcat)	HTTP	Yes	8.6	Network	Low	
CVE-2021-2351	Oracle Agile Product Lifecycle Management for Process	Reporting (ODP for .NET)	Oracle Net	Yes	8.3	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-11987	Oracle Agile Engineering Data Management	Installation Issues (Apache Batik)	HTTP	Yes	8.2	Network	Low	
CVE-2020-11987	Oracle Product Lifecycle Analytics	Installation Issues (Apache Batik)	HTTP	Yes	8.2	Network	Low	
CVE-2021-22118	Oracle Product Lifecycle Analytics	Installation Issues (Spring Framework)	None	No	7.8	Local	Low	
CVE-2021-42340	Oracle Agile Engineering Data Management	Installation Issues (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	
CVE-2021-40690	Oracle Agile PLM	Security (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	
CVE-2020-25649	Oracle Agile PLM	Security (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2019-0227	Oracle Product Lifecycle Analytics	Installation Issues (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	
CVE-2019-10086	Oracle Agile Engineering Data Management	Installation Issues (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Product Lifecycle Analytics	Installation Issues (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2021-44832	Oracle Product Lifecycle Analytics	Installation Issues (Apache Log4j)	HTTP	No	6.6	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2022-23437	Oracle Agile Engineering Data Management	Installation Issues (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	
CVE-2022-23437	Oracle Agile PLM	Security (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	
CVE-2022-23437	Oracle Product Lifecycle Analytics	Installation Issues (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	
CVE-2020-11022	Oracle Agile PLM	Security (jQuery)	HTTP	Yes	6.1	Network	Low	
CVE-2021-41184	Oracle Agile PLM	Security (jQueryUI)	HTTP	Yes	6.1	Network	Low	
CVE-2021-36374	Oracle Agile Engineering Data Management	Installation Issues (Apache Ant)	None	No	5.5	Local	Low	
CVE-2020-17521	Oracle Agile Engineering Data Management	Installation Issues (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2021-36374	Oracle Product Lifecycle Analytics	Installation Issues (Apache Ant)	None	No	5.5	Local	Low	
CVE-2021-34429	Oracle Autovue for Agile Product Lifecycle Management	Internal Operations (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	
CVE-2021-29425	Oracle Agile Engineering Data Management	Installation Issues (Apache Commons IO)	HTTP	Yes	4.8	Network	High	

Additional CVEs addressed are:

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

- 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-2021-36374 also addresses CVE-2021-36373.
- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.
- The patch for CVE-2021-42340 also addresses CVE-2022-23181.

Oracle Systems Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Systems. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2022-21513	Oracle ZFS Storage Appliance Kit	Core	None	No	8.2	Local	Low	High
CVE-2022-24801	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	8.1	Network	High	None
CVE-2022-21524	Oracle Solaris	Filesystem	SMB	No	7.6	Network	Low	Low
CVE-2022-21514	Oracle Solaris	Remote Administration Daemon	Multiple	Yes	7.5	Network	Low	None
CVE-2022-21533	Oracle Solaris	SMB Server	None	No	5.5	Local	Low	Low
CVE-2022-21439	Oracle Solaris	Kernel	None	No	4.2	Local	Low	High
CVE-2022-21563	Oracle ZFS	Core	None	No	3.4	Local	Low	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	Storage Appliance Kit							

Additional CVEs addressed are:

- The patch for CVE-2022-24801 also addresses CVE-2018-25032, CVE-2020-29651, CVE-2021-4115, CVE-2022-23308, and CVE-2022-29824.

Oracle Utilities Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-36518	Oracle Utilities Framework	General (jackson-databind)	HTTP	Yes	7.5	Network	Low	None

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Virtualization. Neither of these vulnerabilities may be remotely exploitable without authentication, i.e., neither 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-2022-21571	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	N
CVE-2022-21554	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	N