Oracle Critical Patch Update Advisory - April 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 520 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at April 2022 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Engineered Systems Utilities, versions 12.1.0.2, 19c, 21c	Oracle Autonomous Health Framework
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0	Enterprise Manager

Affected Products and Versions	Patch Availability Document
Enterprise Manager for Peoplesoft, versions 13.4.1.1, 13.5.1.1	Enterprise Manager
Enterprise Manager for Storage Management, version 13.4.0.0	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
Helidon, versions 1.4.7, 1.4.10, 2.0.0-RC1	Helidon
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineeri Suite
JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.3	JD Edwards
JD Edwards World Security, version A9.4	JD Edwards
Management Cloud Engine, versions 1.5.0 and prior	Oracle Management Cloud Engine
Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
MySQL Cluster, versions 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior, 8.0.28 and prior	MySQL
MySQL Connectors, versions 8.0.28 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.29 and prior	MySQL
MySQL Server, versions 5.7.37 and prior, 8.0.28 and prior	MySQL
MySQL Workbench, versions 8.0.28 and prior	MySQL
Oracle Advanced Supply Chain Planning, versions 12.1, 12.2	Oracle Supply Chain Products
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 PLM MCAD Connector, version 3.6	Oracle Supply Chain Products
Oracle Application Development Framework (ADF), versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Application Express, versions prior to 22.1	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 Deposits and Lines of Credit Servicing, version 2.12.0	Contact Support
Oracle Banking Enterprise Default Management, versions 2.7.1, 2.10.0, 2.12.0	Oracle Banking Platform
Oracle Banking Loans Servicing, version 2.12.0	Contact Support
Oracle Banking Party Management, version 2.7.0	Oracle Banking Platform
Oracle Banking Payments, version 14.5	Contact Support

Affected Products and Versions	Patch Availability Document
Oracle Banking Platform, versions 2.6.2, 2.7.1, 2.12.0	Oracle Banking Platform
Oracle Banking Trade Finance, version 14.5	Contact Support
Oracle Banking Treasury Management, version 14.5	Contact Support
Oracle Blockchain Platform, versions prior to 21.1.2	Oracle Blockchain Platform
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 5.9.0.0.0, 12.2.1.3.0, 12.2.1.4.0	Oracle Analytics
Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Coherence, versions 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 Communications ASAP, version 7.3	Oracle Communications ASAP
Oracle Communications Billing and Revenue Management, versions 12.0.0.4, 12.0.0.5	Oracle Communications Billing an Revenue Management
Oracle Communications Cloud Native Core Automated Test Suite, versions 1.8.0, 1.9.0, 22.1.0	Oracle Communications Cloud Nat Core Automated Test Suite
Oracle Communications Cloud Native Core Binding Support Function, version 1.11.0	Oracle Communications Cloud Nat Core Binding Support Function
Oracle Communications Cloud Native Core Console, versions 1.9.0, 22.1.0	Oracle Communications Cloud Nat Core Console
Oracle Communications Cloud Native Core Network Exposure Function, version 22.1.0	Oracle Communications Cloud Nat Core Network Exposure Function
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.10.0, 22.1.0	Oracle Communications Cloud Nat Core Network Function Cloud Nati Environment
Oracle Communications Cloud Native Core Network Repository Function, versions 1.15.0, 1.15.1, 22.1.0	Oracle Communications Cloud Nat Core Network Repository Function
Oracle Communications Cloud Native Core Network Slice Selection Function, versions 1.8.0, 22.1.0	Oracle Communications Cloud Nat Core Network Slice Selection Func
Oracle Communications Cloud Native Core Policy, versions 1.14.0, 1.15.0, 22.1.0	Oracle Communications Cloud Nat Core Policy
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 1.7.0, 22.1.0	Oracle Communications Cloud Nat Core Security Edge Protection Prox
Oracle Communications Cloud Native Core Service Communication Proxy, version 1.15.0	Oracle Communications Cloud Nat Core Service Communication Prox
Oracle Communications Cloud Native Core Unified Data Repository, versions 1.15.0, 22.1.0	Oracle Communications Cloud Nat Core Unified Data Repository

Affected Products and Versions	Patch Availability Document
Oracle Communications Contacts Server, version 8.0.0.6.0	Oracle Communications Contacts Server
Oracle Communications Convergence, versions 3.0.2.2, 3.0.3.0	Oracle Communications Converge
Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.4.0.0	Oracle Communications Converge Charging Controller
Oracle Communications Design Studio, versions 7.3.5, 7.4.0-7.4.2	Oracle Communications Design Studio
Oracle Communications Diameter Intelligence Hub, versions 8.0.0-8.2.3	Oracle Communications Diameter Signaling Router
Oracle Communications Diameter Signaling Router, version 8.4.0.0	Oracle Communications Diameter Signaling Router
Oracle Communications EAGLE Application Processor	Oracle Communications EAGLE Application Processor
Oracle Communications EAGLE Element Management System, version 46.6	Oracle Communications EAGLE Element Management System
Oracle Communications EAGLE FTP Table Base Retrieval, version 4.5	Oracle Communications EAGLE FT Table Base Retrieval
Oracle Communications EAGLE LNP Application Processor, versions 10.1, 10.2	Oracle Communications EAGLE LN Application Processor
Oracle Communications EAGLE Software, versions 46.7.0, 46.8.0-46.8.2, 46.9.1-46.9.3	Oracle Communications EAGLE (Software)
Oracle Communications Element Manager, versions prior to 9.0	Oracle Communications Element Manager
Oracle Communications Evolved Communications Application Server, version 7.1	Oracle Communications Evolved Communications Application Serv
Oracle Communications Instant Messaging Server, version 10.0.1.5.0	Oracle Communications Instant Messaging Server
Oracle Communications Interactive Session Recorder, version 6.4	Oracle Communications Interactiv Session Recorder
Oracle Communications IP Service Activator, version 7.4.0	Oracle Communications IP Service Activator
Oracle Communications Messaging Server, version 8.1	Oracle Communications Messagin Server
Oracle Communications MetaSolv Solution, version 6.3.1	Oracle Communications MetaSolv Solution
Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.4.0.0	Oracle Communications Network Charging and Control

Affected Products and Versions	Patch Availability Document
Oracle Communications Network Integrity, versions 7.3.2, 7.3.5, 7.3.6	Oracle Communications Network Integrity
Oracle Communications Operations Monitor, versions 4.3, 4.4, 5.0	Oracle Communications Operation Monitor
Oracle Communications Order and Service Management, versions 7.3, 7.4	Oracle Communications Order and Service Management
Oracle Communications Performance Intelligence Center (PIC) Software, versions 10.3.0.0.0-10.3.0.2.1, 10.4.0.1.0-10.4.0.3.1	Oracle Communications Performa Intelligence Center (PIC) Software
Oracle Communications Policy Management, versions 12.5.0.0.0, 12.6.0.0.0	Oracle Communications Policy Management
Oracle Communications Pricing Design Center, versions 12.0.0.4, 12.0.0.5	Oracle Communications Pricing Design Center
Oracle Communications Services Gatekeeper, version 7.0.0.0.0	Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller, versions 8.4, 9.0	Oracle Communications Session Border Controller
Oracle Communications Session Report Manager, versions prior to 9.0	Oracle Communications Session Report Manager
Oracle Communications Session Route Manager, versions prior to 9.0	Oracle Communications Session Route Manager
Oracle Communications Unified Inventory Management, versions 7.3.4-7.3.5, ,7.4.1-7.4.2	Oracle Communications Unified Inventory Management
Oracle Communications Unified Session Manager, versions 8.2.5, 8.4.5	Oracle Communications Unified Session Manager
Oracle Communications User Data Repository, version 12.4	Oracle Communications User Data Repository
Oracle Communications WebRTC Session Controller, version 7.2.1	Oracle Communications WebRTC Session Controller
Oracle Data Integrator, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Database Server, versions 12.1.0.2, 19c, 21c	Database
Oracle Documaker, versions 12.6.0, 12.6.2-12.6.4, 12.7.0	Oracle Insurance Applications
Oracle E-Business Suite, versions 12.2.4-12.2.11, [EBS Cloud Manager and Backup Module] prior to 22.1.1.1, [Enterprise Command Center] 7.0, [Enterprise Information Discovery] 7-9	Oracle E-Business Suite
Oracle Enterprise Communications Broker, versions 3.2, 3.3	Oracle Enterprise Communications Broker
Oracle Enterprise Session Border Controller, versions 8.4, 9.0	Oracle Enterprise Session Border Controller

Affected Products and Versions	Patch Availability Document
Oracle Ethernet Switch ES1-24, version 1.3.1	Systems
Oracle Ethernet Switch TOR-72, version 1.2.2	Systems
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6.0-8.0.9.0, 8.1.0.0-8.1.2.0	Oracle Financial Services Analytica Applications Infrastructure
Oracle Financial Services Behavior Detection Platform, versions 8.0.6.0-8.0.8.0, 8.1.1.0, 8.1.1.1, 8.1.2.0	Oracle Financial Services Behavior Detection Platform
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, 8.1.1.1, 8.1.2.0	Oracle Financial Services Enterpris Case Management
Oracle Financial Services Revenue Management and Billing, versions 2.7.0.0, 2.7.0.1, 2.8.0.0	Oracle Financial Services Revenue Management and Billing
Oracle FLEXCUBE Universal Banking, versions 11.83.3, 12.1-12.4, 14.0-14.3, 14.5	Contact Support
Oracle Global Lifecycle Management OPatch	Global Lifecycle Management
Oracle GoldenGate, versions prior to 12.3.0.1.2, prior to 23.1	Database
Oracle GoldenGate Application Adapters, versions prior to 23.1	Database
Oracle GoldenGate Big Data and Application Adapters, versions prior to 23.1	Database
Oracle GraalVM Enterprise Edition, versions 20.3.5, 21.3.1, 22.0.0.2	Java SE
Oracle Health Sciences Empirica Signal, versions 9.1.0.6, 9.2.0.0	Health Sciences
Oracle Health Sciences InForm, versions 6.2.1.1, 6.3.2.1, 7.0.0.0	Health Sciences
Oracle Health Sciences InForm Publisher, versions 6.2.1.0, 6.3.1.1	Health Sciences
Oracle Health Sciences Information Manager, versions 3.0.1-3.0.4	HealthCare Applications
Oracle Healthcare Data Repository, versions 8.1.0, 8.1.1	HealthCare Applications
Oracle Healthcare Foundation, versions 7.3.0.1-7.3.0.4	HealthCare Applications
Oracle Healthcare Master Person Index, version 5.0.1	HealthCare Applications
Oracle Healthcare Translational Research, versions 4.1.0, 4.1.1	HealthCare Applications
Oracle Hospitality Suite8, versions 8.10.2, 8.11.0-8.14.0	Oracle Hospitality Suite8
Oracle Hospitality Token Proxy Service, version 19.2	Oracle Hospitality Token Proxy Ser
Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Hyperion BI+, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Hyperion Calculation Manager, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Hyperion Data Relationship Management, versions prior to 11.2.8.0, prior to 11.2.9.0	Oracle Enterprise Performance Management

Affected Products and Versions	Patch Availability Document
Oracle Hyperion Financial Management, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Hyperion Infrastructure Technology, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Hyperion Planning, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Hyperion Profitability and Cost Management, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Hyperion Tax Provision, versions prior to 11.2.8.0	Oracle Enterprise Performance Management
Oracle Identity Management Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Identity Manager Connector, versions 9.1.0	Fusion Middleware
Oracle iLearning, versions 6.2, 6.3	iLearning
Oracle Insurance Data Gateway, version 1.0.1	Oracle Insurance Applications
Oracle Insurance Insbridge Rating and Underwriting, versions 5.2.0, 5.4.0-5.6.0, 5.6.1	Oracle Insurance Applications
Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0, 11.2.8, 11.3.0, 11.3.1	Oracle Insurance Applications
Oracle Insurance Rules Palette, versions 11.0.2, 11.1.0, 11.2.8, 11.3.0, 11.3.1	Oracle Insurance Applications
Oracle Internet Directory, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Java SE, versions 7u331, 8u321, 11.0.14, 17.0.2, 18	Java SE
Oracle JDeveloper, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0	Fusion Middleware
Oracle NoSQL Database	NoSQL Database
Oracle Outside In Technology, versions 8.5.5, 8.5.6	Fusion Middleware
Oracle Payment Interface, versions 19.1, 20.3	Oracle Payment Interface
Oracle Product Lifecycle Analytics, version 3.6.1.0	Oracle Supply Chain Products
Oracle REST Data Services, versions prior to 21.2	Database
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 17.0-19.0	Retail Applications

Affected Products and Versions	Patch Availability Document
Oracle Retail Data Extractor for Merchandising, versions 15.0.2, 16.0.2	Retail Applications
Oracle Retail EFTLink, versions 17.0.2, 18.0.1, 19.0.1, 20.0.1, 21.0.0	Retail Applications
Oracle Retail Extract Transform and Load, version 13.2.8	Retail Applications
Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1	Retail Applications
Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1	Retail Applications
Oracle Retail Invoice Matching, version 16.0.3	Retail Applications
Oracle Retail Merchandising System, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1	Retail Applications
Oracle Retail Store Inventory Management, versions 14.0.4.13, 14.1.3.5, 14.1.3.14, 15.0.3.3, 15.0.3.8, 16.0.3.7	Retail Applications
Oracle Retail Xstore Office Cloud Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1	Retail Applications
Oracle Retail Xstore Point of Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1, 21.0.0	Retail Applications
Oracle SD-WAN Edge, versions 9.0, 9.1	Oracle SD-WAN Edge
Oracle Secure Backup	Oracle Secure Backup
Oracle Secure Global Desktop, version 5.6	Virtualization
Oracle Solaris, version 11	Systems
Oracle Solaris Cluster, version 4	Systems
Oracle SQL Developer, versions prior to 21.99	Database
Oracle StorageTek ACSLS, version 8.5.1	Systems
Oracle StorageTek Tape Analytics (STA), version 2.4	Systems
Oracle Taleo Platform, versions prior to 22.1	Oracle Taleo
Oracle Transportation Management, versions 6.4.3, 6.5.1	Oracle Supply Chain Products
Oracle Tuxedo, version 12.2.2.0.0	Fusion Middleware
Oracle Utilities Framework, versions 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.34	Virtualization
Oracle Web Services Manager, 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

Affected Products and Versions	Patch Availability Document
Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebLogic Server, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
OSS Support Tools, versions 2.12.42, 18.3	Oracle Support Tools
PeopleSoft Enterprise CS Academic Advisement, version 9.2	PeopleSoft
PeopleSoft Enterprise FIN Cash Management, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59	PeopleSoft
PeopleSoft Enterprise PRTL Interaction Hub, version 9.1	PeopleSoft
Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12, 21.12	Oracle Construction and Engineeri Suite

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-2022-21441
- Adi Farshteindiker: CVE-2022-21487, CVE-2022-21488
- Ahmed Shah of Red Canari: CVE-2022-21481
- Alexander Kornbrust of Red Database Security: CVE-2022-21410
- AnhNH of Sacombank: CVE-2022-21419, CVE-2022-21448, CVE-2022-21492
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2022-21482, CVE-2022-21490
- Anthony Weems: CVE-2022-21496
- Aobo Wang of Chaitin Security Research Lab: CVE-2022-21465, CVE-2022-21471
- bendtheory: CVE-2022-21468
- ChauUHM of Sacombank: CVE-2022-21419, CVE-2022-21448, CVE-2022-21492
- Cl0und of Syclover Security Team: CVE-2022-21420
- Dimitris Doganos of COSMOTE - Mobile Telecommunications S.A.: CVE-2022-21466
- Emad Al-Mousa: CVE-2022-21410
- Harrison Neal: CVE-2022-21411
- HolyBugx: CVE-2022-21468
- Iustin Ladunca (youstin): CVE-2022-21468

- Janggggg of VNPT: CVE-2022-21445, CVE-2022-21497
- Karan Lyons: CVE-2022-21496
- Kun Yang of Chaitin Security Research Lab: CVE-2022-21465, CVE-2022-21471
- lc working with Trend Micro Zero Day Initiative: CVE-2022-21483, CVE-2022-21484, CVE-2022-21489
- Liboheng of Tophant Starlight laboratory: CVE-2022-21420
- Lucas Leong (wmliang) of Trend Micro Zero Day Initiative: CVE-2022-21485, CVE-2022-21486
- Luo Likang of NSFocus Security Team: CVE-2022-21487
- Markus Loewe: CVE-2022-21443
- Michael MOSKOPP of Sogeti: CVE-2022-21469
- Natalia Trojanowska of SecuRing: CVE-2022-21467
- Neil Madden of ForgeRock: CVE-2022-21449
- Niels van Gijzen of HackDefense: CVE-2022-21470
- Oliver Bachtik of NVISO: CVE-2022-21491
- Omar Younis of Cysiv: CVE-2022-21477
- osword from SGLAB of Legendsec at Qi'anxin Group: CVE-2022-21434
- Paulino Calderon of websec mx: CVE-2022-21404
- peterjson - Security Engineering - VNG Corporation: CVE-2022-21445, CVE-2022-21497
- r00t4dm: CVE-2022-21421, CVE-2022-21441
- Sander Meijering of HackDefense: CVE-2022-21470
- Shihao Wen: CVE-2022-21438, CVE-2022-21459
- TuanNT of Sacombank: CVE-2022-21419, CVE-2022-21448, CVE-2022-21492
- TungHT of Sacombank: CVE-2022-21419, CVE-2022-21448, CVE-2022-21492
- Vikas Khanna: CVE-2022-21450
- wangze from Codesafe Team of Legendsec at Qi: CVE-2022-21453
- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2021-2427

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:

- Charles Korn
- John Jiang of Tencent.com
- thiscodecc of MoyunSec V-Lab
- Tugay Aslan of Beam Teknoloji

On-Line Presence Security Contributors

Oracle acknowledges people who have contributed to our On-Line Presence Security program (see FAQ). People are acknowledged for contributions relating to Oracle's on-line presence if they provide information, observations or suggestions pertaining to security-related issues that result in significant modification to Oracle's on-line external-facing systems.

For this quarter, Oracle recognizes the following for contributions to Oracle's On-Line Presence Security program:

- Aakash Adhikari (dark_haxor)
- Abdiwahab Ahmed
- Adarsh Sreedhar
- Ahmad Henry Mansour
- Ahmed Al-Saleem
- Aitor Herrero Fuentes
- Andrea NaD
- Anis Haboubi
- AR Movies A
- Fahad Anwar Hussain
- George Crook
- Hamoud Al-Helmani
- Het Vikam
- Houssem Belhadj Ahmed
- Hunt4r Bug
- J Jebarson Immanuel
- Joaquín Pochat
- Juhanák, Petr of Accenture

- Luca Ottoni
- Manjil Ghimire
- Marvi Alex
- Michoel Chaikin of Carsales.com Ltd
- Mohamed Veten of Resecurity, Inc.
- Mohamed Selem
- Mohammed Adam
- Mohammed Awez Kagdi
- Nagliy Kot
- Pankaj Kumar Thakur of Green Tick Nepal Pvt. Ltd.
- Pim Dieleman of Cadran Consultancy B.V. [2 reports]
- Prathamesh Bagul
- Rahul Singh
- Sagar Elias
- SEINT
- Shuvam Adhikari [4 reports]
- Tarun Garg
- Tejas Pagare
- Vikas Srivastava [2 reports]
- Vismit Sudhir Rakhecha (Druk)
- Vitali Lavrentikov

Critical Patch Update Schedule

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

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

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins

- Critical Patch Update - April 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
2024-December-23	Rev 9. Updated the addtional CVE for ZFS CVE-2021-39275
2024-September-20	Rev 8. Product Name and details changes for CVE-2022-21445.
2022-June-16	Rev 7. Added credit for CVE-2022-21438.
2022-May-20	Rev 6. Added version 8.5.6 to Outside In Technology. Changed the Component of Middleware Common Libraries and Tools to FMW Remote Diagnostic Agent for CVE-2021-30129. Updated credit name.
2022-May-4	Rev 5. Removed affected version 11.1.1.5.0 of Oracle Identity Manager Connector for CV 2022-23305. Added a footnote for the change.
2022-May-2	Rev 4. Updated the affected versions Oracle Health Sciences InForm Publisher and Or Communications Unified Inventory Management. Note added for MySQL Enterprise Monitor. Note Removed for CVE-2022-21449. Credit Name Updated for CVE-2022-214
2022-April-29	Rev 3. Updated EM Ops Center additional CVEs for CVE-2021-40438. Updated Oracle additional CVEs for CVE-2021-39275
2022-April-21	Rev 2. Updated the affected versions for CVE-2022-21449
2022-April-19	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 29 new security patches for Oracle Database Products divided as follows:

- 5 new security patches for Oracle Database Products
- 1 new security patch for Oracle Autonomous Health Framework
- 15 new security patches for Oracle Blockchain Platform
- No new security patches for Oracle Global Lifecycle Management, but third party patches are provided
- 5 new security patches for Oracle GoldenGate
- No new security patches for Oracle NoSQL Database, but third party patches are provided
- 1 new security patch for Oracle REST Data Services
- No new security patches for Oracle Secure Backup, but third party patches are provided
- 2 new security patches for Oracle SQL Developer

Oracle Database Server Risk Matrix

This Critical Patch Update contains 5 new security patches plus additional third party patches noted below for Oracle Database Products. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2022-21410	Oracle Database - Enterprise Edition Sharding	Create Any Procedure	Oracle Net	No	7.2	Network	Low	High	
CVE-2022-21498	Java VM	Create Procedure	Multiple	No	6.5	Network	Low	Low	
CVE-2021-41165	Oracle Application Express (CKEditor)	Valid User Account	HTTP	No	5.4	Network	Low	Low	I
CVE-2022-21411	RDBMS Gateway / Generic ODBC Connectivity	Create Session	Oracle Net	No	5.4	Network	Low	Low	

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-22569	Oracle Spatial and Graph MapViewer (protobuf-java)	Local Logon	Local Logon	No	2.8	Local	Low	Low	I

Additional CVEs addressed are:

- The patch for CVE-2021-41165 also addresses CVE-2021-41164.

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

- Oracle Database - Enterprise Edition Portable Clusterware (Apache MINA SSHD): CVE-2021-30129.
- Oracle Database - Enterprise Edition RDBMS (LibExpat): CVE-2022-23990 and CVE-2022-23852.
- Oracle Database Configuration Assistant (Apache Commons Compress): CVE-2019-12402.
- Oracle Database Enterprise Edition (Apache Tomcat): CVE-2021-42340.

Oracle Autonomous Health Framework Risk Matrix

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

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2021-2464	Engineered Systems Utilities	Local Logon	Local Logon	No	7.8	Local	Low	Low	Nc

Oracle Blockchain Platform Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle Blockchain Platform. 14 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-23017	Oracle Blockchain Platform	Backend (nginx)	UDP	Yes	9.8	Network	Low	None
CVE-2020-5245	Oracle Blockchain Platform	Backend (Dropwizard-Validation)	HTTP	No	8.8	Network	Low	Low
CVE-2021-2351	Oracle Blockchain Platform	BCS Console (JDBC, OCCI)	Oracle Net	Yes	8.3	Network	High	None
CVE-2020-8174	Oracle Blockchain Platform	BCS Console (Node.js)	HTTP	Yes	8.1	Network	High	None
CVE-2020-24750	Oracle Blockchain Platform	BCS Console (jackson-databind)	HTTP	Yes	8.1	Network	High	None
CVE-2020-28052	Oracle Blockchain Platform	BCS Console (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	None
CVE-2019-12399	Oracle Blockchain Platform	BCS Console (Apache Kafka)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-17527	Oracle Blockchain Platform	BCS Console (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-11612	Oracle Blockchain Platform	BCS Console (Netty)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-13565	Oracle Blockchain	Backend (OpenLDAP)	LDAP	Yes	7.5	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	Platform							
CVE-2020-8203	Oracle Blockchain Platform	BCS Console (Lodash)	HTTP	Yes	7.4	Network	High	None
CVE-2019-10086	Oracle Blockchain Platform	BCS Console (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	None
CVE-2020-11022	Oracle Blockchain Platform	Backend (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-29425	Oracle Blockchain Platform	BCS Console (Apache Commons IO)	HTTP	Yes	4.8	Network	High	None
CVE-2020-27218	Oracle Blockchain Platform	BCS Console (Eclipse Jetty)	HTTP	Yes	4.8	Network	High	None

Notes:

1. This is a hotfix on top of version 21.1.2

Additional CVEs addressed are:

- The patch for CVE-2019-13565 also addresses CVE-2017-14159, CVE-2017-17740, CVE-2017-9287, CVE-2019-13057, CVE-2020-12243, and CVE-2020-15719.
- The patch for CVE-2020-17527 also addresses CVE-2020-13935.
- The patch for CVE-2020-24750 also addresses CVE-2020-24616, CVE-2020-25649, and CVE-2020-36189.
- The patch for CVE-2020-8174 also addresses CVE-2020-10531, CVE-2020-11080, CVE-2020-8172, and CVE-2020-8277.

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains no new security patches but does include third party patches noted below for Oracle Global Lifecycle Management. Please refer to previous Critical

Patch Update Advisories if the last Critical Patch Update was not applied for Oracle Global Lifecycle Management. The English text form of this Risk Matrix can be found here.

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

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

- Oracle Global Lifecycle Management OPatch
  - Centralized Third Party Jars (Apache Commons Compress): CVE-2021-36090, CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.

Oracle GoldenGate Risk Matrix

This Critical Patch Update contains 5 new security patches plus additional third party patches noted below for Oracle GoldenGate. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-26291	Oracle GoldenGate Big Data and Application Adapters	General (Apache Maven)	HTTP	Yes	9.1	Network	Low	None
CVE-2022-21442	Oracle GoldenGate	OGG Core Library	None	No	8.8	Local	Low	Low
CVE-2021-2351	Oracle GoldenGate Application Adapters	General (OCCI)	Oracle Net	Yes	8.3	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-12086	Oracle GoldenGate	Internal Framework (jackson-databind)	HTTP	Yes	7.5	Network	Low	None
CVE-2019-14862	Oracle GoldenGate	Internal Framework (Knockout)	HTTP	Yes	6.1	Network	Low	None

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

- Oracle GoldenGate Application Adapters
  - General (Apache Log4j): CVE-2022-23305, CVE-2019-17571, CVE-2021-4104 and CVE-2022-23302.

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 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 NoSQL Database
  - Administration (Netty): CVE-2021-37137, CVE-2021-21290, CVE-2021-21295, CVE-2021-21409, CVE-2021-30129 and CVE-2021-37136.
  - Administration (Apache MINA SSHD): CVE-2021-30129.

Oracle REST Data Services Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle REST Data Services. 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	U Int
CVE-2021-29425	Oracle REST Data Services	General (Apache Commons IO)	HTTP	No	4.2	Network	High	Low	N

Oracle Secure Backup Risk Matrix

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

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

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

- Oracle Secure Backup
  - Oracle Secure Backup (Apache HTTP Server): CVE-2021-44790, CVE-2021-32785, CVE-2021-32786, CVE-2021-32791, CVE-2021-32792 and CVE-2021-44224.
  - Oracle Secure Backup (PHP): CVE-2021-21703.

Oracle SQL Developer Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2021-44832	Oracle SQL Developer	Installation (Apache Log4j)	HTTP	No	6.6	Network	High	High	
CVE-2020-13956	Oracle SQL Developer	Thirdparty Database support (Apache HTTPClient)	HTTP	Yes	5.3	Network	Low	None	

Oracle Commerce Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Commerce. 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 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-39139	Oracle Commerce Guided Search	Content Acquisition System (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2021-22118	Oracle Commerce Guided Search	Content Acquisition System (Spring Framework)	None	No	7.8	Local	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-42340	Oracle Commerce Guided Search	Content Acquisition System (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-21466	Oracle Commerce Guided Search	Tools and Frameworks	HTTP	Yes	7.5	Network	Low	None
CVE-2021-41165	Oracle Commerce Guided Search	Content Acquisition System (CKEditor)	HTTP	No	5.4	Network	Low	Low
CVE-2020-13956	Oracle Commerce Guided Search	Workbench (HTTPClient)	HTTP	Yes	5.3	Network	Low	None
CVE-2020-8908	Oracle Commerce Guided Search	Workbench (Guava)	None	No	3.3	Local	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2021-22118 also addresses CVE-2020-5421.
- 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-2021-41165 also addresses CVE-2021-41164.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 39 new security patches for Oracle Communications Applications. 22 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21431	Oracle Communications Billing and Revenue Management	Connection Manager	TCP	Yes	10.0	Network	Low
CVE-2022-23305	Oracle Communications Messaging Server	ISC (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2022-23990	Oracle Communications MetaSolv Solution	User Interface (LibExpat)	HTTP	Yes	9.8	Network	Low
CVE-2022-23305	Oracle Communications Network Integrity	Cartridge Deployer Tool (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2022-23305	Oracle Communications Unified Inventory Management	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2020-13936	Oracle Communications Network Integrity	TL1 Cartridge (Apache Velocity Engine)	HTTP	No	8.8	Network	Low
CVE-2022-21430	Oracle Communications Billing and Revenue Management	Connection Manager	TCP	No	8.5	Network	High
CVE-2021-2351	Oracle Communications Billing and Revenue Management	Pipeline Configuration Center, Oracle Data Manager, Rated Event Loader (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2022-21424	Oracle Communications	Connection Manager	TCP	No	8.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
	Billing and Revenue Management						
CVE-2021-2351	Oracle Communications IP Service Activator	Service Activator (OCCI)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Oracle Communications Pricing Design Center	Cloud Native Deployment (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-22118	Oracle Communications Network Integrity	MSS Cartridge (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-36090	Oracle Communications Billing and Revenue Management	Billing Care (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2022-21422	Oracle Communications Billing and Revenue Management	Connection Manager	TCP	No	7.5	Network	High
CVE-2021-42340	Oracle Communications Instant Messaging Server	DBPlugin (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2021-40690	Oracle Communications Messaging Server	ISC (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low
CVE-2021-33813	Oracle Communications Messaging Server	ISC (Apache Tika)	HTTP	Yes	7.5	Network	Low
CVE-2019-10086	Oracle Communications	User Interface (Apache	HTTP	Yes	7.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
	Network Integrity	Commons BeanUtils)					
CVE-2021-44832	Oracle Communications ASAP	SRP (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Billing and Revenue Management	Rated Event Manager, Business Operations Center, Kafka Data Manager (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Convergence	Configuration (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Convergent Charging Controller	Network Gateway (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications IP Service Activator	Logging (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Messaging Server	ISC (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Network Charging and Control	Gateway (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Network Integrity	Cartridge Deployer Tool (Apache Log4j)	HTTP	No	6.6	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
CVE-2021-44832	Oracle Communications Pricing Design Center	REST Services Manager (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Unified Inventory Management	Logging (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-43797	Oracle Communications Messaging Server	ISC (Netty)	HTTP	Yes	6.5	Network	Low
CVE-2020-6950	Oracle Communications Network Integrity	Installer (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low
CVE-2019-3740	Oracle Communications Network Integrity	Installer (RSA BSAFE Crypto-J)	HTTPS	Yes	6.5	Network	Low
CVE-2021-36374	Oracle Communications Order and Service Management	Installer, OSM SDK (Apache Ant)	None	No	5.5	Local	Low
CVE-2022-24329	Oracle Communications Pricing Design Center	REST Services Manager (Kotlin)	HTTP	Yes	5.3	Network	Low
CVE-2021-29425	Oracle Communications Contacts Server	File Upload (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2021-29425	Oracle Communications Design Studio	OSM Plugin (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2021-29425	Oracle Communications Order and	OSM SDK (Apache Commons IO)	HTTP	Yes	4.8	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
	Service Management						
CVE-2021-29425	Oracle Communications Pricing Design Center	REST Service Manager (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2021-21275	Oracle Communications Pricing Design Center	REST Service Manager (Jacoco)	HTTP	Yes	4.3	Network	Low
CVE-2020-8908	Oracle Communications Pricing Design Center	REST Services Manager (Guava)	None	No	3.3	Local	Low

Additional CVEs addressed are:

- The patch for CVE-2019-3740 also addresses CVE-2019-3738, and CVE-2019-3739.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.
- The patch for CVE-2021-36374 also addresses CVE-2021-36373.
- The patch for CVE-2022-23305 also addresses CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.
- The patch for CVE-2022-23990 also addresses CVE-2022-23852.

Oracle Communications Risk Matrix

This Critical Patch Update contains 149 new security patches plus additional third party patches noted below for Oracle Communications. 98 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 V		
					Base Score	Attack Vector	At Co
CVE-2022-22947	Oracle Communications Cloud Native Core Network Exposure Function	NEF (Spring Cloud Gateway)	HTTP	Yes	10.0	Network	L
CVE-2022-22947	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (Spring Cloud Gateway)	HTTP	Yes	10.0	Network	L
CVE-2017-1000353	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite (Jenkins)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Cloud Native Core Automated Test Suite	Automation Test Suite (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2021-29921	Oracle Communications Cloud Native Core Binding Support Function	BSF (Python)	HTTP	Yes	9.8	Network	L
CVE-2021-43527	Oracle Communications Cloud Native Core Binding Support Function	BSF (NSS)	HTTPS	Yes	9.8	Network	L
CVE-2022-23221	Oracle Communications Cloud Native Core Console	CNC Console (H2)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications	CNC Console (Spring Framework)	HTTP	Yes	9.8	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Cloud Native Core Console						
CVE-2022-22965	Oracle Communications Cloud Native Core Network Exposure Function	NEF (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	DB Tier (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2020-14343	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (PyYAML)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Cloud Native Core Network Repository Function	OCNRF (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2021-43527	Oracle Communications Cloud Native Core Network Repository Function	OCNRF (NSS)	HTTPS	Yes	9.8	Network	L
CVE-2021-29921	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (Python)	HTTP	Yes	9.8	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2022-22965	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2021-43527	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (NSS)	HTTPS	Yes	9.8	Network	L
CVE-2021-42392	Oracle Communications Cloud Native Core Policy	Policy (H2)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Cloud Native Core Policy	Policy (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2021-35574	Oracle Communications Cloud Native Core Policy	Policy (glibc)	HTTP	Yes	9.8	Network	L
CVE-2021-3520	Oracle Communications Cloud Native Core Policy	Policy (lz4)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Cloud Native Core Security Edge Protection Proxy	OC SEPP (Spring framework)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2020-17530	Oracle Communications	Visualization (Apache Struts)	HTTP	Yes	9.8	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Diameter Intelligence Hub						
CVE-2022-23305	Oracle Communications EAGLE FTP Table Base Retrieval	Core (Apache Log4j)	HTTP	Yes	9.8	Network	L
CVE-2020-35198	Oracle Communications EAGLE Software	Measurements (VxWorks)	HTTP	Yes	9.8	Network	L
CVE-2021-44790	Oracle Communications Element Manager	Security (Apache HTTP Server)	HTTP	Yes	9.8	Network	L
CVE-2021-44790	Oracle Communications Operations Monitor	Mediation Engine (Apache HTTP Server)	HTTP	Yes	9.8	Network	L
CVE-2022-22965	Oracle Communications Policy Management	CMP (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2021-23450	Oracle Communications Policy Management	CMP (dojo)	HTTP	Yes	9.8	Network	L
CVE-2021-43527	Oracle Communications Policy Management	CMP (NSS)	HTTPS	Yes	9.8	Network	L
CVE-2021-44790	Oracle Communications Session Report Manager	General (Apache HTTP Server)	HTTP	Yes	9.8	Network	L
CVE-2021-44790	Oracle Communications Session Route Manager	Third Party (Apache HTTP Server)	HTTP	Yes	9.8	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2022-22965	Oracle SD-WAN Edge	Management (Spring Framework)	HTTP	Yes	9.8	Network	L
CVE-2020-36242	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (python-cryptography)	HTTP	Yes	9.1	Network	L
CVE-2021-3518	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (libxml2)	HTTP	Yes	8.8	Network	L
CVE-2021-32626	Oracle Communications Operations Monitor	FDP (Redis)	TCP	No	8.8	Network	L
CVE-2020-10878	Oracle Communications EAGLE LNP Application Processor	Platform (Perl)	HTTP	Yes	8.6	Network	L
CVE-2020-10878	Oracle Communications Performance Intelligence Center (PIC) Software	Platform (Perl)	HTTP	Yes	8.6	Network	L
CVE-2021-39153	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite Framework (XStream)	HTTP	No	8.5	Network	H
CVE-2021-2351	Oracle Communications Diameter Intelligence Hub	Integrated DIH (JDBC, OCCI)	Oracle Net	Yes	8.3	Network	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2021-2351	Oracle Communications Services Gatekeeper	Third party software/products (JDBC)	Oracle Net	Yes	8.3	Network	H
CVE-2019-16789	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (ceph)	HTTP	Yes	8.2	Network	L
CVE-2019-18276	Oracle Communications Cloud Native Core Policy	Policy (GNU Bash)	None	No	7.8	Local	L
CVE-2021-22118	Oracle Communications Diameter Intelligence Hub	Visualization, Mediation (Spring Framework)	None	No	7.8	Local	L
CVE-2021-3156	Oracle Communications Performance Intelligence Center (PIC) Software	Platform (Sudo)	None	No	7.8	Local	L
CVE-2021-42340	Management Cloud Engine	Security (Apache Tomcat)	HTTP	Yes	7.5	Network	L
CVE-2021-35515	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite (Apache Commons Compress)	HTTP	Yes	7.5	Network	L
CVE-2021-22946	Oracle Communications Cloud Native Core Binding Support Function	CNC BSF (cURL)	HTTP	Yes	7.5	Network	L
CVE-2020-36518	Oracle Communications	CNC Console (jackson-databind)	HTTP	Yes	7.5	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Cloud Native Core Console						
CVE-2021-22946	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (cURL)	HTTP	Yes	7.5	Network	L
CVE-2021-22946	Oracle Communications Cloud Native Core Network Repository Function	OCNRF (cURL)	HTTP	Yes	7.5	Network	L
CVE-2021-3690	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (Undertow)	HTTP	Yes	7.5	Network	L
CVE-2021-22946	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (cURL)	HTTPS	Yes	7.5	Network	L
CVE-2020-28196	Oracle Communications Cloud Native Core Policy	Policy (MIT Kerberos)	HTTP	Yes	7.5	Network	L
CVE-2021-3807	Oracle Communications Cloud Native Core Policy	Policy (ansi-regex)	HTTP	Yes	7.5	Network	L
CVE-2020-8231	Oracle Communications Cloud Native Core Policy	Policy (libcurl)	HTTP	Yes	7.5	Network	L
CVE-2020-29363	Oracle Communications	Policy (p11-kit)	HTTP	Yes	7.5	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Cloud Native Core Policy						
CVE-2021-42340	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Apache Tomcat)	HTTP	Yes	7.5	Network	L
CVE-2021-22946	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (cURL)	HTTP	Yes	7.5	Network	L
CVE-2021-36090	Oracle Communications Diameter Intelligence Hub	Integrated DIH (Apache Commons Compress)	HTTP	Yes	7.5	Network	L
CVE-2020-11971	Oracle Communications Diameter Intelligence Hub	Mediation (Apache Camel)	HTTP	Yes	7.5	Network	L
CVE-2021-43859	Oracle Communications Diameter Intelligence Hub	Visualization, Database (XStream)	HTTP	Yes	7.5	Network	L
CVE-2021-30468	Oracle Communications Diameter Intelligence Hub	Visualization, Mediation (Apache CXF)	SOAP	Yes	7.5	Network	L
CVE-2021-42340	Oracle Communications Element Manager	Security (Apache Tomcat)	HTTP	Yes	7.5	Network	L
CVE-2021-43859	Oracle Communications Policy Management	CMP (XStream)	HTTP	Yes	7.5	Network	L
CVE-2021-42340	Oracle Communications	General (Apache Tomcat)	HTTP	Yes	7.5	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Session Report Manager						
CVE-2021-42340	Oracle Communications Session Route Manager	Third Party (Apache Tomcat)	HTTP	Yes	7.5	Network	L
CVE-2020-25638	Oracle Communications Cloud Native Core Console	CNC Console (hibernate-core)	HTTP	Yes	7.4	Network	H
CVE-2021-3712	Oracle Communications Cloud Native Core Console	CNC Console (OpenSSL)	HTTPS	Yes	7.4	Network	H
CVE-2021-3712	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (OpenSSL)	HTTP	Yes	7.4	Network	H
CVE-2021-3712	Oracle Communications Cloud Native Core Unified Data Repository	UDR (OpenSSL)	HTTPS	Yes	7.4	Network	H
CVE-2021-3712	Oracle Communications Session Border Controller	Security (OpenSSL)	TLS	Yes	7.4	Network	H
CVE-2021-3712	Oracle Communications Unified Session Manager	Security (OpenSSL)	TLS	Yes	7.4	Network	H
CVE-2021-3712	Oracle Enterprise Communications Broker	Security (OpenSSL)	TLS	Yes	7.4	Network	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2021-3712	Oracle Enterprise Session Border Controller	Security (OpenSSL)	TLS	Yes	7.4	Network	H
CVE-2022-23181	Oracle Communications Cloud Native Core Policy	Policy (Apache Tomcat)	None	No	7.0	Local	H
CVE-2021-44832	Management Cloud Engine	Security (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Console	CNC Console (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	DBTier (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Network Repository Function	OCNRF (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Policy	Policy (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Security	SEPP (Apache Log4j)	HTTP	No	6.6	Network	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Edge Protection Proxy						
CVE-2021-44832	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications EAGLE Element Management System	Platform (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications EAGLE FTP Table Base Retrieval	Core (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Element Manager	Security (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Evolved Communications Application Server	SDC,SCF (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Performance Intelligence Center (PIC) Software	Management (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications	OCSG common services - CORE	HTTP	No	6.6	Network	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Services Gatekeeper	(Apache Log4j)					
CVE-2021-44832	Oracle Communications Session Report Manager	General (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications Session Route Manager	Third Party (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications User Data Repository	Security (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-44832	Oracle Communications WebRTC Session Controller	Admin console, LWPR (Apache Log4j)	HTTP	No	6.6	Network	H
CVE-2021-43797	Oracle Communications Cloud Native Core Binding Support Function	Policy (Netty)	HTTP	Yes	6.5	Network	L
CVE-2021-30129	Oracle Communications Cloud Native Core Console	CNC Console (Apache MINA SSHD)	HTTP	No	6.5	Network	L
CVE-2021-43797	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (Netty)	HTTP	Yes	6.5	Network	L
CVE-2021-43797	Oracle Communications Cloud Native Core Policy	Policy (Netty)	HTTP	Yes	6.5	Network	L
CVE-2019-3799	Oracle Communications	Policy (Spring Cloud Config)	HTTP	Yes	6.5	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Cloud Native Core Policy						
CVE-2021-43797	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (Netty)	HTTP	Yes	6.5	Network	L
CVE-2021-43797	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Netty)	HTTP	Yes	6.5	Network	L
CVE-2022-23437	Oracle Communications Element Manager	Security (Apache Xerces-J)	HTTP	Yes	6.5	Network	L
CVE-2022-23437	Oracle Communications Session Report Manager	General (Apache Xerces-J)	HTTP	Yes	6.5	Network	L
CVE-2022-23437	Oracle Communications Session Route Manager	Third Party (Apache Xerces-J)	HTTP	Yes	6.5	Network	L
CVE-2021-39140	Oracle Communications Cloud Native Core Policy	Policy (XStream)	HTTP	No	6.3	Network	H
CVE-2021-41184	Oracle Communications Interactive Session Recorder	Dashboard (jQueryUI)	HTTP	Yes	6.1	Network	L
CVE-2021-41184	Oracle Communications Operations Monitor	Mediation Engine (jQueryUI)	HTTP	Yes	6.1	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2021-2471	Oracle Communications Cloud Native Core Console	CNC Console (MySQL Connectors)	HTTP	No	5.9	Network	H
CVE-2020-14340	Oracle Communications Cloud Native Core Console	CNC Console (XNIO)	HTTP	Yes	5.9	Network	H
CVE-2020-1971	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (OpenSSL)	HTTPS	Yes	5.9	Network	H
CVE-2021-2471	Oracle Communications Cloud Native Core Network Slice Selection Function	NSSF (MySQL)	TCP	No	5.9	Network	H
CVE-2021-21409	Oracle Communications Cloud Native Core Policy	Policy (Netty)	HTTP	Yes	5.9	Network	H
CVE-2021-38153	Oracle Communications Cloud Native Core Policy	Policy (Apache Kafka)	HTTP	Yes	5.9	Network	H
CVE-2021-2471	Oracle Communications Cloud Native Core Policy	Policy (MySQL)	HTTP	No	5.9	Network	H
CVE-2020-14340	Oracle Communications Cloud Native Core Policy	Policy (XNIO)	HTTP	Yes	5.9	Network	H
CVE-2021-33880	Oracle Communications Cloud Native Core Policy	Policy (aaugustin websockets)	HTTP	Yes	5.9	Network	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2020-16135	Oracle Communications Cloud Native Core Policy	Policy (libssh)	HTTP	Yes	5.9	Network	H
CVE-2021-2471	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (MySQL)	TCP	No	5.9	Network	H
CVE-2021-3572	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	OC-CNE (python-pip)	HTTP	No	5.7	Network	L
CVE-2021-3572	Oracle Communications Cloud Native Core Policy	Policy (python-pip)	HTTP	No	5.7	Network	L
CVE-2021-36374	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite (Apache Ant)	None	No	5.5	Local	L
CVE-2021-36374	Oracle Communications Cloud Native Core Binding Support Function	CNC BSF (Apache Ant)	None	No	5.5	Local	L
CVE-2021-22569	Oracle Communications Cloud Native Core Console	CNC Console (protobuf-java)	None	No	5.5	Local	L
CVE-2021-22569	Oracle Communications Cloud Native Core Network	OCNRF (protobuf-java)	None	No	5.5	Local	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Repository Function						
CVE-2020-13434	Oracle Communications Cloud Native Core Policy	Policy (SQLite)	None	No	5.5	Local	L
CVE-2020-15250	Oracle Communications Cloud Native Core Policy	Policy (JUnit)	None	No	5.5	Local	L
CVE-2021-28168	Oracle Communications Cloud Native Core Policy	Policy (Eclipse Jersey)	None	No	5.5	Local	L
CVE-2021-22569	Oracle Communications Cloud Native Core Policy	Policy (protobuf-java)	None	No	5.5	Local	L
CVE-2021-28168	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Eclipse Jersey)	None	No	5.5	Local	L
CVE-2021-36374	Oracle Communications Diameter Intelligence Hub	Visualization (Apache Ant)	None	No	5.5	Local	L
CVE-2020-17521	Oracle Communications Diameter Signaling Router	API Gateway (Apache Groovy)	None	No	5.5	Local	L
CVE-2022-20615	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite Framework (Jenkins Matrix Project)	HTTP	No	5.4	Network	L
CVE-2021-20289	Oracle Communications Cloud Native Core Console	CNC Console (RESTEasy)	HTTP	Yes	5.3	Network	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
CVE-2020-14155	Oracle Communications Cloud Native Core Policy	Policy (PCRE)	HTTP	Yes	5.3	Network	L
CVE-2021-28169	Oracle Communications Cloud Native Core Policy	Policy (Eclipse Jetty)	HTTP	Yes	5.3	Network	L
CVE-2021-28170	Oracle Communications Cloud Native Core Policy	Policy (Jakarta)	HTTP	Yes	5.3	Network	L
CVE-2020-29582	Oracle Communications Cloud Native Core Policy	Policy (Kotlin)	HTTP	Yes	5.3	Network	L
CVE-2020-8554	Oracle Communications Cloud Native Core Policy	Policy (Kubernetes)	HTTP	No	5.0	Network	H
CVE-2021-22132	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite Framework (Elasticsearch)	HTTP	No	4.8	Network	H
CVE-2021-29425	Oracle Communications Cloud Native Core Policy	Policy (Apache Commons IO)	HTTP	Yes	4.8	Network	H
CVE-2021-29425	Oracle Communications Diameter Intelligence Hub	Database (Apache Commons IO)	Oracle Net	Yes	4.8	Network	H
CVE-2021-29425	Oracle Communications Policy Management	CMP (Apache Commons IO)	HTTP	Yes	4.8	Network	H
CVE-2021-3521	Oracle Communications Cloud Native	OC-CNE (rpm)	None	No	4.4	Local	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS V		
					Base Score	Attack Vector	At Co
	Core Network Function Cloud Native Environment						
CVE-2022-20613	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite (Jenkins Mailer)	HTTP	Yes	4.3	Network	L
CVE-2022-20612	Oracle Communications Cloud Native Core Automated Test Suite	Automated Test Suite Framework (Jenkins)	HTTP	Yes	4.3	Network	L
CVE-2021-22096	Oracle Communications Cloud Native Core Console	CNC Console (Spring boot)	HTTP	No	4.3	Network	L
CVE-2021-22096	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Spring Framework)	HTTP	No	4.3	Network	L
CVE-2021-3200	Oracle Communications Cloud Native Core Policy	Signaling (libsolv)	None	No	3.3	Local	L

Additional CVEs addressed are:

- The patch for CVE-2017-1000353 also addresses CVE-2018-1000067, CVE-2018-1000068, CVE-2018-1000192, CVE-2018-1000193, CVE-2018-1000194, CVE-2018-1000195, CVE-2018-1999001, CVE-2018-1999002, CVE-2018-1999003, CVE-2018-1999004, CVE-2018-1999005, CVE-2018-1999007, CVE-2018-6356, CVE-2019-1003049, CVE-2019-1003050, CVE-2019-10383, and CVE-2019-10384.
- The patch for CVE-2019-16789 also addresses CVE-2019-16785, CVE-2019-16786, and CVE-2019-16792.
- The patch for CVE-2019-18276 also addresses CVE-2021-27568.
- The patch for CVE-2020-10878 also addresses CVE-2020-10543, and CVE-2020-12723.

- The patch for CVE-2020-13434 also addresses CVE-2020-15358.
- The patch for CVE-2020-35198 also addresses CVE-2020-28895.
- The patch for CVE-2020-36242 also addresses CVE-2020-25659.
- The patch for CVE-2020-8231 also addresses CVE-2020-8284, CVE-2020-8285, and CVE-2020-8286.
- The patch for CVE-2021-21409 also addresses CVE-2021-21295.
- The patch for CVE-2021-22132 also addresses CVE-2021-22134, CVE-2021-22144, and CVE-2021-22145.
- The patch for CVE-2021-22946 also addresses CVE-2021-22897, CVE-2021-22898, CVE-2021-22901, CVE-2021-22947, and CVE-2021-33560.
- The patch for CVE-2021-28169 also addresses CVE-2019-10247.
- The patch for CVE-2021-30468 also addresses CVE-2021-22696, and CVE-2021-40690.
- The patch for CVE-2021-32626 also addresses CVE-2021-32627, CVE-2021-32628, CVE-2021-32672, CVE-2021-32675, CVE-2021-32687, CVE-2021-32762, and CVE-2021-41099.
- The patch for CVE-2021-3518 also addresses CVE-2019-20388, CVE-2020-24977, CVE-2020-7595, CVE-2021-3517, and CVE-2021-3537.
- The patch for CVE-2021-35515 also addresses CVE-2021-35516, CVE-2021-35517, and CVE-2021-36090.
- The patch for CVE-2021-35574 also addresses CVE-2019-13750, CVE-2019-13751, CVE-2019-18218, CVE-2019-19603, CVE-2019-20838, CVE-2019-5827, CVE-2020-13435, CVE-2020-14155, CVE-2021-20231, CVE-2021-20232, CVE-2021-23840, CVE-2021-23841, CVE-2021-27645, CVE-2021-33574, CVE-2021-3445, CVE-2021-3580, CVE-2021-35942, CVE-2021-36084, CVE-2021-36085, CVE-2021-36086, and CVE-2021-36087.
- The patch for CVE-2021-3572 also addresses CVE-2019-20916.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.
- The patch for CVE-2021-36374 also addresses CVE-2021-36373.
- The patch for CVE-2021-3712 also addresses CVE-2021-3711.
- The patch for CVE-2021-39153 also addresses CVE-2021-39139, 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-2021-39154, and CVE-2021-43859.
- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.
- The patch for CVE-2021-44790 also addresses CVE-2021-44224.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.
- The patch for CVE-2022-20613 also addresses CVE-2022-20614.
- The patch for CVE-2022-22965 also addresses CVE-2022-22963.

- 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 Cloud Native Core Policy
  - Policy (Apache Santuario XML Security For Java): CVE-2021-40690.
  - Policy (Spring Integration): CVE-2020-5413.
- Oracle Communications EAGLE Application Processor
  - Platform (Perl): CVE-2020-10878, CVE-2020-10543 and CVE-2020-12723.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Construction and Engineering. 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.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-23450	Primavera Unifier	Platform (dojo)	HTTP	No	7.6	Network	Low	L
CVE-2021-44832	Instantis EnterpriseTrack	Logging (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-41184	Primavera Unifier	User Interface (jQueryUI)	HTTP	Yes	6.1	Network	Low	N

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle E-Business Suite. 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.

Oracle E-Business Suite products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle E-Business Suite products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that customers apply the April 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 (April 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	Privs Req'd
CVE-2022-23305	Oracle E-Business Suite Cloud Manager and Cloud Backup Module	Logging (Apache Log4j)	HTTP	Yes	9.8	Network	Low	None
CVE-2021-44832	Oracle E-Business Suite Information Discovery	Logging (Apache Log4j)	HTTP	No	6.6	Network	High	High
CVE-2021-44832	Oracle Enterprise Command Center Framework	Logging (Apache Log4j)	HTTP	No	6.6	Network	High	High
CVE-2022-21468	Oracle Applications Framework	Popups	HTTP	Yes	6.1	Network	Low	None
CVE-2022-21477	Oracle Applications Framework	Attachments, File Upload	HTTP	No	5.4	Network	Low	Low

Notes:

1. Oracle E-Business Suite version is 12.2

Additional CVEs addressed are:

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

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 10 new security patches for Oracle Enterprise Manager. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found here.

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the April 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 April 2022 Patch Availability Document for Oracle Products, My Oracle Support Note 2844807.1 .

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2022-23305	Enterprise Manager Base Platform	Oracle Management Service (Apache Log4j)	HTTP	Yes	9.8	Network	Low	Nor
CVE-2018-1285	Oracle Application Testing Suite	Load Testing for Web Apps	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	Pri Rec
		(Apache log4net)						
CVE-2021-40438	Enterprise Manager Ops Center	User Interface (Apache HTTP Server)	HTTP	Yes	9.0	Network	High	Nor
CVE-2021-3518	Enterprise Manager Base Platform	Enterprise Manager Install (libxml2)	HTTP	Yes	8.8	Network	Low	Nor
CVE-2021-2351	Enterprise Manager Ops Center	Networking (OCCI)	Oracle Net	Yes	8.3	Network	High	Nor
CVE-2021-3450	Enterprise Manager for Storage Management	Privilege Management (OpenSSL)	HTTPS	Yes	7.4	Network	High	Nor
CVE-2021-44832	Enterprise Manager Base Platform	Enterprise Manager Install (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Enterprise Manager for Peoplesoft	PSEM Plugin (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Enterprise Manager Ops Center	Networking (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2022-21469	Enterprise Manager Base Platform	UI Framework	HTTP	Yes	4.7	Network	Low	Nor

Additional CVEs addressed are:

- The patch for CVE-2021-3450 also addresses CVE-2020-1971, CVE-2021-23839, CVE-2021-23840, CVE-2021-23841, and CVE-2021-3449.
- The patch for CVE-2021-3518 also addresses CVE-2019-20388, CVE-2020-24977, CVE-2020-7595, CVE-2021-3517, and CVE-2021-3537.
- The patch for CVE-2021-40438 also addresses CVE-2021-44224, and CVE-2021-44790.

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

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 41 new security patches for Oracle Financial Services Applications. 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 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2022-22965	Oracle Financial Services Analytical Applications Infrastructure	Others (Spring Framework)	HTTP	Yes	9.8	Network	Low	No
CVE-2022-22965	Oracle Financial Services Behavior Detection Platform	BD (Spring Framework)	HTTP	Yes	9.8	Network	Low	No
CVE-2022-22965	Oracle Financial Services Enterprise Case Management	Installers (Spring Framework)	HTTP	Yes	9.8	Network	Low	No
CVE-2022-23305	Oracle Financial Services Revenue Management and Billing	Infrastructure (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2021-2351	Oracle Banking Enterprise Default Management	Collections (JDBC)	Oracle Net	Yes	8.3	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-2351	Oracle Banking Platform	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2021-36090	Oracle Banking Payments	Infrastructure (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-36090	Oracle Banking Trade Finance	Infrastructure (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-37714	Oracle Banking Trade Finance	Infrastructure (jsoup)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-36090	Oracle Banking Treasury Management	Infrastructure (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-37714	Oracle Banking Treasury Management	Infrastructure (jsoup)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-36090	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-37714	Oracle FLEXCUBE Universal Banking	Infrastructure (jsoup)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-44832	Oracle Banking Deposits and Lines of Credit Servicing	Web UI (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle Banking Enterprise	Collections (Apache Log4j)	HTTP	No	6.6	Network	High	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
	Default Management							
CVE-2021-44832	Oracle Banking Loans Servicing	Web UI (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle Banking Party Management	Web UI (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle Banking Payments	Infrastructure (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle Banking Platform	SECURITY (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle Banking Trade Finance	Infrastructure (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle Banking Treasury Management	Infrastructure (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-44832	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache Log4j)	HTTP	No	6.6	Network	High	Hi
CVE-2021-30129	Oracle Banking Payments	Infrastructure (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	Lo
CVE-2021-30129	Oracle Banking Trade Finance	Infrastructure (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	Lo
CVE-2021-30129	Oracle Banking Treasury Management	Infrastructure (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2022-23437	Oracle Financial Services Analytical Applications Infrastructure	Others (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2022-23437	Oracle Financial Services Behavior Detection Platform	Third Party (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2022-23437	Oracle Financial Services Enterprise Case Management	Installers (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	No
CVE-2021-30129	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	Lo
CVE-2022-21475	Oracle Banking Payments	Infrastructure	HTTP	No	5.9	Network	High	Lo
CVE-2022-21474	Oracle Banking Trade Finance	Infrastructure	HTTP	No	5.9	Network	High	Lo
CVE-2022-21473	Oracle Banking Treasury Management	Infrastructure	HTTP	No	5.9	Network	High	Lo
CVE-2021-38153	Oracle Financial Services Analytical Applications Infrastructure	Others (Apache Kafka)	HTTP	Yes	5.9	Network	High	No
CVE-2021-38153	Oracle Financial	Third Party (Apache	HTTP	Yes	5.9	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
	Services Behavior Detection Platform	Kafka)						
CVE-2021-38153	Oracle Financial Services Enterprise Case Management	Installers (Apache Kafka)	HTTP	Yes	5.9	Network	High	No
CVE-2022-21472	Oracle FLEXCUBE Universal Banking	Infrastructure	HTTP	No	5.9	Network	High	Lo
CVE-2021-36374	Oracle Banking Trade Finance	Infrastructure (Apache Ant)	None	No	5.5	Local	Low	No
CVE-2021-31812	Oracle Banking Trade Finance	Infrastructure (Apache PDFBox)	None	No	5.5	Local	Low	No
CVE-2021-36374	Oracle Banking Treasury Management	Infrastructure (Apache Ant)	None	No	5.5	Local	Low	No
CVE-2021-31812	Oracle Banking Treasury Management	Infrastructure (Apache PDFBox)	None	No	5.5	Local	Low	No
CVE-2021-31812	Oracle FLEXCUBE Universal Banking	Infrastructure (Apache PDFBox)	None	No	5.5	Local	Low	No

Additional CVEs addressed are:

- The patch for CVE-2021-31812 also addresses CVE-2021-27807, CVE-2021-27906, and CVE-2021-31811.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.

- The patch for CVE-2021-36374 also addresses CVE-2021-36373.
- The patch for CVE-2021-38153 also addresses CVE-2021-26291.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.
- The patch for CVE-2022-23305 also addresses CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 54 new security patches plus additional third party patches noted below for Oracle Fusion Middleware. 41 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security updates are not listed in the Oracle Fusion Middleware risk matrix. However, since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the Critical Patch Update April 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 April 2022 Patch Availability Document for Oracle Products, My Oracle Support Note 2853458.2.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2022-21445	Oracle Application Development Framework (ADF)	ADF Faces	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Business Intelligence Enterprise Edition	Analytics Server (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Business Intelligence	BI Platform Security	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Enterprise Edition	(Apache Log4j)						
CVE-2022-23305	Oracle Business Intelligence Enterprise Edition	Storage Service Integration (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Business Process Management Suite	Runtime Engine (JBoss Enterprise Application Platform)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-21420	Oracle Coherence	Core	T3	Yes	9.8	Network	Low	N
CVE-2021-39275	Oracle HTTP Server	Web Listener (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Identity Management Suite	Installer (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Identity Manager Connector	General and Misc (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle JDeveloper	Oracle JDeveloper (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Middleware Common Libraries and Tools	Third Party Patch (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle Tuxedo	Third Party Patch (Apache Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2022-23305	Oracle WebLogic	Centralized Third Party	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Server	Jars (Apache Log4j)						
CVE-2022-21404	Helidon	Reactive WebServer	HTTP	Yes	8.1	Network	High	N
CVE-2021-22901	Oracle HTTP Server	SSL Module (cURL)	HTTPS	Yes	8.1	Network	High	N
CVE-2022-21497	Oracle Web Services Manager	Web Services Security	HTTP	Yes	8.1	Network	Low	N
CVE-2022-21421	Oracle Business Intelligence Enterprise Edition	Analytics Web General	HTTP	Yes	7.5	Network	Low	N
CVE-2021-37714	Oracle Business Process Management Suite	Installer (jsoup)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-0227	Oracle Internet Directory	Oracle Directory Services Mngr (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	N
CVE-2021-40690	Oracle Outside In Technology	Installation (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-36090	Oracle WebCenter Portal	Security Framework (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-37137	Oracle WebCenter Portal	Security Framework (Netty)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-25649	Oracle WebCenter Portal	Security Framework (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
CVE-2021-37714	Oracle WebCenter Portal	Security Framework (jsoup)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-7226	Oracle WebCenter Sites	WebCenter Sites (Cryptacular)	HTTP	Yes	7.5	Network	Low	N
CVE-2022-21441	Oracle WebLogic Server	Core	T3/IIOP	Yes	7.5	Network	Low	N
CVE-2021-44832	Oracle Data Integrator	Runtime Java agent for ODI (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-44832	Oracle Identity Management Suite	Installer (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-44832	Oracle Identity Manager Connector	General and Misc (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-44832	Oracle JDeveloper	Oracle JDeveloper (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-44832	Oracle Managed File Transfer	MFT Runtime Server (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-44832	Oracle WebCenter Portal	Security Framework (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-44832	Oracle WebCenter Sites	Advanced UI (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-43797	Helidon	Reactive WebServer (Netty)	HTTP	Yes	6.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-30129	Middleware Common Libraries and Tools	FMW Remote Diagnostic Agent (Apache MINA SSHD and Apache MINA)	HTTP	No	6.5	Network	Low	L
CVE-2021-43797	Oracle Coherence	Configuration and Parsing (Netty)	HTTP	Yes	6.5	Network	Low	N
CVE-2020-24977	Oracle HTTP Server	SSL Module (libxml2)	HTTPS	Yes	6.5	Network	Low	N
CVE-2021-44224	Oracle HTTP Server	SSL Module (Apache HTTP Server)	HTTPS	Yes	6.5	Network	Low	N
CVE-2022-23437	Oracle WebLogic Server	Third Party Tools (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2022-21492	Oracle Business Intelligence Enterprise Edition	Analytics Server	HTTP	Yes	6.1	Network	Low	N
CVE-2022-21419	Oracle Business Intelligence Enterprise Edition	Visual Analyzer	HTTP	Yes	6.1	Network	Low	N
CVE-2022-21448	Oracle Business Intelligence Enterprise Edition	Visual Analyzer	HTTP	Yes	6.1	Network	Low	N
CVE-2022-21453	Oracle WebLogic Server	Console	HTTP	Yes	6.1	Network	Low	N
CVE-2021-41184	Oracle WebLogic Server	Console, Samples (jQueryUI)	HTTP	Yes	6.1	Network	Low	N
CVE-2020-17521	Oracle Business	BPM Studio (Apache	None	No	5.5	Local	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Process Management Suite	Groovy)						
CVE-2021-31812	Oracle WebCenter Portal	Security Framework (Apache PDFbox)	None	No	5.5	Local	Low	N
CVE-2021-28657	Oracle WebCenter Portal	Security Framework (Apache Tika)	None	No	5.5	Local	Low	N
CVE-2021-41165	Oracle WebCenter Portal	Security Framework (CKEditor)	HTTP	No	5.4	Network	Low	L
CVE-2018-11212	Oracle Internet Directory	Oracle Directory Services Manager (libjpeg)	HTTP	Yes	5.3	Network	Low	N
CVE-2021-33037	Oracle Managed File Transfer	MFT Runtime Server (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	N
CVE-2021-28170	Oracle WebLogic Server	Centralized Third Party Jars (JBoss Enterprise Application Platform)	HTTP	Yes	5.3	Network	Low	N
CVE-2021-29425	Helidon	CDI support (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N
CVE-2021-29425	Oracle WebCenter Portal	Security Framework (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N
CVE-2020-8908	Oracle WebLogic Server	Third Party Tools (Guava)	None	No	3.3	Local	Low	L

Notes:

1. Oracle Application Development Framework (ADF) is downloaded via Oracle JDeveloper Product. Please refer to Fusion Middleware Patch Advisor for more details.

2. The supported versions of Oracle Identity Manager Connector are not impacted by CVE-2022-23305, CVE-2022-23302, CVE-2022-23307, and CVE-2021-4104.

3. The patch for CVE-2019-0227 also addresses CVE-2018-2601 for Oracle Internet Directory 12.2.1.4.0.

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

Additional CVEs addressed are:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2020-24977 also addresses CVE-2021-22901, CVE-2021-39275, and CVE-2021-44224.
- 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-2021-28170 also addresses CVE-2020-10693.
- The patch for CVE-2021-30129 also addresses CVE-2021-41973.
- The patch for CVE-2021-31812 also addresses CVE-2021-31811.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.
- The patch for CVE-2021-37137 also addresses CVE-2021-37136.
- The patch for CVE-2021-41165 also addresses CVE-2021-41164.
- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.
- The patch for CVE-2021-43797 also addresses CVE-2021-21409, CVE-2021-37136, and CVE-2021-37137.
- 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 WebCenter Sites
    - WebCenter Sites (Bouncy Castle Java Library): CVE-2020-28052.

Oracle Health Sciences Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-3711	Oracle Health Sciences InForm Publisher	Connector (OpenSSL)	TLS	Yes	9.8	Network	Low	None	
CVE-2021-44832	Oracle Health Sciences Empirica Signal	Logging (Apache Log4j)	HTTP	No	6.6	Network	High	High	
CVE-2021-44832	Oracle Health Sciences InForm	Cognos logging (Apache Log4j)	HTTP	No	6.6	Network	High	High	

Additional CVEs addressed are:

- The patch for CVE-2021-3711 also addresses CVE-2021-3712, and CVE-2021-4160.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

Oracle HealthCare Applications Risk Matrix

This Critical Patch Update contains 10 new security patches for Oracle HealthCare Applications. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2022-23305	Oracle Healthcare Data Repository	FHIR (Apache Log4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2021-36090	Oracle Healthcare Data Repository	FHIR Commandline (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2021-44832	Oracle Health Sciences Information Manager	Record Locator (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Oracle Healthcare Data Repository	FHIR (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Oracle Healthcare Foundation	RPD Generation (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Oracle Healthcare Master Person Index	IHE (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-44832	Oracle Healthcare Translational Research	Datastudio (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2021-33037	Oracle Healthcare Translational Research	Datastudio (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	No
CVE-2021-29425	Oracle Health Sciences Information Manager	Health Policy Engine (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2021-29425	Oracle Healthcare Data Repository	FHIR Comandline (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No

Additional CVEs addressed are:

- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.
- The patch for CVE-2022-23305 also addresses CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Hospitality Applications. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-13936	Oracle Hospitality Token Proxy Service	TPS Service (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	Low
CVE-2021-37714	Oracle Hospitality Token Proxy Service	TPS Service (jsoup)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-44832	Oracle Hospitality Suite8	Leisure (Apache Log4j)	TCP	No	6.6	Network	High	High
CVE-2021-44832	Oracle Hospitality	TPS Service (Apache	HTTP	No	6.6	Network	High	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	Token Proxy Service	Log4j)						
CVE-2021-44832	Oracle Payment Interface	OPI Core (Apache Log4j)	HTTP	No	6.6	Network	High	High
CVE-2021-41184	Oracle Hospitality Suite8	WebConnect (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.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Hyperion. 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		
					Base Score	Attack Vector	C
CVE-2022-23305	Oracle Hyperion Data Relationship Management	Installation/Configuration (Apache Log4j)	HTTP	Yes	9.8	Network	
CVE-2022-23305	Oracle Hyperion Infrastructure Technology	Installation and Configuration (Apache Log4j)	HTTP	Yes	9.8	Network	
CVE-2021-44832	Oracle Hyperion BI+	Architect (Apache Log4j)	HTTP	No	6.6	Network	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS		
					Base Score	Attack Vector	C
CVE-2021-44832	Oracle Hyperion Data Relationship Management	Installation/Configuration (Apache Log4j)	HTTP	No	6.6	Network	
CVE-2021-44832	Oracle Hyperion Financial Management	Security (Apache Log4j)	HTTP	No	6.6	Network	
CVE-2021-44832	Oracle Hyperion Infrastructure Technology	Installation and Configuration (Apache Log4j)	HTTP	No	6.6	Network	
CVE-2021-44832	Oracle Hyperion Planning	Security (Apache Log4j)	HTTP	No	6.6	Network	
CVE-2021-44832	Oracle Hyperion Profitability and Cost Management	Install (Apache Log4j)	HTTP	No	6.6	Network	
CVE-2021-44832	Oracle Hyperion Tax Provision	Tax Provision (Apache Log4j)	HTTP	No	6.6	Network	
CVE-2020-6950	Oracle Hyperion Calculation Manager	General (Eclipse Mojarra)	HTTP	Yes	6.5	Network	
CVE-2021-31812	Oracle Hyperion Infrastructure Technology	Installation and Configuration (Apache PDFbox)	None	No	5.5	Local	
CVE-2020-7760	Oracle Hyperion Data Relationship Management	Web Client - Unicode (CodeMirror)	HTTP	Yes	5.3	Network	

Additional CVEs addressed are:

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

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

Oracle iLearning Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2022-23437	Oracle iLearning	Installation (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	None	R

Oracle Insurance Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2351	Oracle Documaker	Development Tools (JDBC, OCCI)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-36090	Oracle Insurance Policy Administration	Architecture (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-44832	Oracle Insurance Data Gateway	Security (Apache Log4j)	HTTP	No	6.6	Network	High	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-44832	Oracle Insurance Insbridge Rating and Underwriting	Framework Administrator IBFA (Apache Log4j)	HTTP	No	6.6	Network	High	H
CVE-2021-35043	Oracle Insurance Policy Administration	Architecture (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2021-29425	Oracle Insurance Policy Administration	Architecture (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N
CVE-2021-29425	Oracle Insurance Rules Palette	Architecture (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N

Additional CVEs addressed are:

- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516, and CVE-2021-35517.

Oracle Java SE Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2022-0778	Oracle GraalVM Enterprise Edition	Node (OpenSSL)	HTTPS	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	I
CVE-2022-21449	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	7.5	Network	Low	None	
CVE-2022-21476	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	7.5	Network	Low	None	
CVE-2022-21426	Oracle Java SE, Oracle GraalVM Enterprise Edition	JAXP	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21496	Oracle Java SE, Oracle GraalVM Enterprise Edition	JNDI	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-2022-21434	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21443	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	3.7	Network	High	None	

Notes:

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, 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.

Additional CVEs addressed are:

- The patch for CVE-2022-0778 also addresses CVE-2021-44531, CVE-2021-44532, CVE-2021-44533, and CVE-2022-21824.

Oracle JD Edwards Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-42013	JD Edwards EnterpriseOne Tools	Upgrade SEC (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	No
CVE-2021-3711	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure (OpenSSL)	JDENET	Yes	9.8	Network	Low	No
CVE-2021-3711	JD Edwards World Security	World Software Security (OpenSSL)	HTTPS	Yes	9.8	Network	Low	No
CVE-2021-2351	JD Edwards EnterpriseOne Tools	Database and Comm SEC (OCCI)	Oracle Net	Yes	8.3	Network	High	No
CVE-2021-2351	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics SEC (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2022-21464	JD Edwards EnterpriseOne Tools	Business Logic Infra SEC	HTTP	Yes	8.2	Network	Low	No
CVE-2021-32066	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech-Cloud (Ruby)	HTTP	Yes	7.4	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2022-21409	JD Edwards EnterpriseOne Tools	Web Runtime	HTTP	Yes	6.1	Network	Low	Nc

Additional CVEs addressed are:

- The patch for CVE-2021-32066 also addresses CVE-2021-31799, and CVE-2021-31810.
- The patch for CVE-2021-3711 also addresses CVE-2021-3712.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 43 new security patches for Oracle MySQL. 11 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2022-23305	MySQL Enterprise Monitor	Monitoring: General (Apache Log4j)	Multiple	Yes	9.8	Network	Low
CVE-2022-22965	MySQL Enterprise Monitor	Monitoring: General (Spring Framework)	Multiple	Yes	9.8	Network	Low
CVE-2022-0778	MySQL Connectors	Connector/C++ (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low
CVE-2022-0778	MySQL Connectors	Connector/ODBC (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low
CVE-2021-42340	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	Multiple	Yes	7.5	Network	Low
CVE-2022-0778	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	Multiple	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-22570	MySQL Server	Server: Compiling (protobuf)	MySQL Protocol	Yes	7.5	Network	Low
CVE-2022-0778	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	Yes	7.5	Network	Low
CVE-2022-0778	MySQL Workbench	Workbench: libssh (OpenSSL)	MySQL Workbench	Yes	7.5	Network	Low
CVE-2022-23181	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	Multiple	No	7.0	Local	High
CVE-2021-44832	MySQL Enterprise Monitor	Monitoring: General (Apache Log4j)	Multiple	No	6.6	Network	High
CVE-2022-21454	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	6.5	Network	Low
CVE-2022-21482	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21483	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21489	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21490	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-41184	MySQL Enterprise Monitor	Monitoring: General (jQueryUI)	Multiple	Yes	6.1	Network	Low
CVE-2022-21457	MySQL Server	Server: PAM Auth Plugin	FIDO protocols	Yes	5.9	Network	High
CVE-2022-21425	MySQL Server	Server: DDL	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21440	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21459	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21478	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21479	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21418	MySQL Server	InnoDB	MySQL Protocol	No	5.0	Network	High
CVE-2022-21417	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21413	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21427	MySQL Server	Server: FTS	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21412	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21414	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21435	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21436	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21437	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21438	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21452	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21462	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21415	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21451	MySQL Server	InnoDB	MySQL Protocol	No	4.4	Network	High
CVE-2022-21444	MySQL Server	Server: DDL	MySQL Protocol	No	4.4	Network	High
CVE-2022-21460	MySQL Server	Server: Logging	MySQL Protocol	No	4.4	Network	High
CVE-2022-21484	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21485	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21486	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21423	MySQL Server	InnoDB	MySQL Protocol	No	2.7	Network	Low

Notes:

1. The patch for CVE-2022-22965 also addresses CVE-2022-22968.

Additional CVEs addressed are:

- The patch for CVE-2021-41184 also addresses CVE-2021-41182, and CVE-2021-41183.
- The patch for CVE-2022-23305 also addresses CVE-2019-17571, CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 14 new security patches for Oracle PeopleSoft. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-3518	PeopleSoft Enterprise PeopleTools	PeopleSoft CDA (libxml2)	HTTP	Yes	8.8	Network	Low	Non
CVE-2021-37714	PeopleSoft Enterprise PeopleTools	Elastic Search (jsoup)	HTTP	Yes	7.5	Network	Low	Non
CVE-2021-40690	PeopleSoft Enterprise PeopleTools	Security (Apache Santuario XML	HTTPS	Yes	7.5	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
		Security for Java)						
CVE-2021-44832	PeopleSoft Enterprise PeopleTools	Security (Apache Log4j)	HTTP	No	6.6	Network	High	Hig
CVE-2022-21447	PeopleSoft Enterprise CS Academic Advisement	Advising Notes	HTTP	No	6.5	Network	Low	Lov
CVE-2021-43797	PeopleSoft Enterprise PeopleTools	Elastic Search (Netty)	HTTP	Yes	6.5	Network	Low	Non
CVE-2022-21458	PeopleSoft Enterprise PeopleTools	Navigation Pages, Portal, Query	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21470	PeopleSoft Enterprise PeopleTools	Process Scheduler	HTTP	Yes	6.1	Network	Low	Non
CVE-2021-4160	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	TLS	Yes	5.9	Network	High	Non
CVE-2022-21481	PeopleSoft Enterprise FIN Cash Management	Financial Gateway	HTTP	No	5.4	Network	Low	Lov
CVE-2021-41165	PeopleSoft Enterprise PeopleTools	Rich Text Editor (CKEditor)	HTTP	No	5.4	Network	Low	Lov
CVE-2022-21450	PeopleSoft Enterprise PRTL Interaction Hub	My Links	HTTP	No	5.4	Network	Low	Lov
CVE-2021-44533	PeopleSoft Enterprise PeopleTools	Elastic Search (Node.js)	HTTP	Yes	5.3	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-8908	PeopleSoft Enterprise PeopleTools	File Processing (Guava)	None	No	3.3	Local	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2021-3518 also addresses CVE-2019-20388, CVE-2020-24977, CVE-2020-7595, CVE-2021-3517, and CVE-2021-3537.
- The patch for CVE-2021-41165 also addresses CVE-2021-41164.
- The patch for CVE-2021-44533 also addresses CVE-2021-44531, CVE-2021-44532, and CVE-2022-21824.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 30 new security patches for Oracle Retail Applications. 15 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	R
CVE-2022-22965	Oracle Retail Xstore Point of Service	Xenvironment (Spring Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-13936	Oracle Retail Xstore Office Cloud Service	Configurator (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	
CVE-2021-39139	Oracle Retail Xstore Point of Service	Xenvironment (XStream)	HTTP	No	8.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-40690	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-37714	Oracle Retail Customer Management and Segmentation Foundation	Segment (jsoup)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-40690	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-40690	Oracle Retail Integration Bus	RIB Kernal (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-40690	Oracle Retail Merchandising System	Foundation (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-40690	Oracle Retail Service Backbone	RSB Installation (Apache Santuario XML Security For Java)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-10086	Oracle Retail Invoice Matching	Security (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	N
CVE-2021-44832	Oracle Retail Customer Insights	Other (Apache Log4j)	HTTP	No	6.6	Network	High	H

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-44832	Oracle Retail Data Extractor for Merchandising	Installer (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail EFTLink	Installation (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Integration Bus	RIB Kernal (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Merchandising System	Foundation (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Service Backbone	RSB Installation (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Store Inventory Management	SIM Integration (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2022-23437	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-30129	Oracle Retail Customer Management and Segmentation Foundation	Segment (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	
CVE-2022-23437	Oracle Retail Extract Transform and Load	Mathematical Operators (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2022-23437	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2022-23437	Oracle Retail Integration Bus	RIB Kernal (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2022-23437	Oracle Retail Merchandising System	Foundation (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2022-23437	Oracle Retail Service Backbone	RSB Installation (Apache Xerces-J)	HTTP	Yes	6.5	Network	Low	N
CVE-2021-36374	Oracle Retail EFTLink	Installation (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Invoice Matching	Security (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Xstore Point of Service	Xenvironment (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-31812	Oracle Retail Xstore Point of Service	Xstore Office (Apache PDFbox)	None	No	5.5	Local	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-34429	Oracle Retail EFTLink	Framework (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2021-31812 also addresses CVE-2021-27807, CVE-2021-27906, and CVE-2021-31811.
- The patch for CVE-2021-36374 also addresses CVE-2021-36373.
- The patch for CVE-2021-39139 also addresses CVE-2021-29505, 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.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle Supply Chain. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2022-23305	Oracle Advanced Supply Chain Planning	MscObieeSrvlt (Apache Log4j)	HTTP	Yes	9.8	Network	Low	
CVE-2022-22965	Oracle Product Lifecycle Analytics	Installer (Spring Framework)	HTTP	Yes	9.8	Network	Low	
CVE-2021-42340	Oracle Agile PLM	Security (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-44832	Oracle Agile Engineering Data Management	Installation Issues (Apache Log4j)	HTTP	No	6.6	Network	High	I
CVE-2021-44832	Oracle Agile PLM	Security (Apache Log4j)	HTTP	No	6.6	Network	High	I
CVE-2021-44832	Oracle Agile PLM MCAD Connector	CAX Client (Apache Log4j)	HTTP	No	6.6	Network	High	I
CVE-2021-44832	Oracle Autovue for Agile Product Lifecycle Management	Internal Operations (Apache Log4j)	HTTP	No	6.6	Network	High	I
CVE-2022-21467	Oracle Agile PLM	Attachments	HTTP	No	6.5	Network	Low	
CVE-2022-21480	Oracle Transportation Management	User Interface	HTTP	Yes	6.1	Network	Low	N
CVE-2021-41165	Oracle Agile PLM	Security (CKEditor)	HTTP	No	5.4	Network	Low	
CVE-2021-29425	Oracle Agile PLM	Security (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N

Additional CVEs addressed are:

- The patch for CVE-2021-41165 also addresses CVE-2021-41164.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.
- The patch for CVE-2022-23305 also addresses CVE-2021-4104, CVE-2022-23302, and CVE-2022-23307.

Oracle Support Tools Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Support Tools. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-30129	OSS Support Tools	Diagnostic Assistant (Apache MINA SSHD)	HTTP	No	6.5	Network	Low	Low	N
CVE-2021-41973	OSS Support Tools	Diagnostic Assistant (Apache MINA)	HTTP	Yes	6.5	Network	Low	None	Re
CVE-2022-21405	OSS Support Tools	Oracle Explorer	None	No	5.5	Local	Low	High	Re

Oracle Systems Risk Matrix

This Critical Patch Update contains 20 new security patches for Oracle Systems. 14 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-17195	Oracle Solaris Cluster	Tools (Nimbus JOSE+JWT)	HTTP	Yes	9.8	Network	Low	None
CVE-2021-39275	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	9.8	Network	Low	None
CVE-2021-2351	Oracle StorageTek ACSLS	Software (JDBC)	Oracle Net	Yes	8.3	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle StorageTek Tape Analytics (STA)	Application Server (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2022-21446	Oracle Solaris	Utility	Multiple	Yes	8.2	Network	Low	None
CVE-2020-11979	Oracle StorageTek ACSLS	Software (Apache Ant)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-11979	Oracle StorageTek Tape Analytics (STA)	Core (Apache Ant)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-6950	Oracle Solaris Cluster	Tools (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low	None
CVE-2020-5421	Oracle StorageTek ACSLS	Software (Spring Framework)	HTTP	No	6.5	Network	High	Low
CVE-2019-3740	Oracle StorageTek ACSLS	Software (RSA BSAFE Crypto-J)	HTTPS	Yes	6.5	Network	Low	None
CVE-2020-11022	Oracle StorageTek ACSLS	Software (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2022-21493	Oracle Solaris	Kernel	None	No	5.9	Local	Low	Low
CVE-2022-21461	Oracle Solaris	Kernel	None	No	5.5	Local	Low	Low
CVE-2022-21463	Oracle Solaris	Kernel	None	No	5.5	Local	Low	Low
CVE-2022-21416	Oracle Solaris	Utility	None	No	5.0	Local	Low	Low
CVE-2021-29425	Oracle Solaris Cluster	Tools (Apache Commons IO)	HTTP	Yes	4.8	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2022-21494	Oracle Solaris	Kernel	None	No	4.0	Local	High	High
CVE-2020-1968	Oracle Ethernet Switch ES1-24	Firmware (OpenSSL)	HTTPS	Yes	3.7	Network	High	None
CVE-2020-1968	Oracle Ethernet Switch TOR-72	Firmware (OpenSSL)	HTTPS	Yes	3.7	Network	High	None
CVE-2020-9488	Oracle StorageTek ACSLS	Software (Apache Log4j)	HTTP	Yes	3.7	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2019-3740 also addresses CVE-2019-3738, and CVE-2019-3739.
- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2021-39275 also addresses CVE-2019-13038, CVE-2019-14822, CVE-2021-25219, CVE-2021-33193, CVE-2021-34798, CVE-2021-36160, CVE-2021-4034, CVE-2021-40438, CVE-2021-41617, CVE-2021-4181, CVE-2021-4182, CVE-2021-4183, CVE-2021-4184, CVE-2021-4185, CVE-2021-42717, CVE-2021-43395, CVE-2021-43818, CVE-2021-44224, CVE-2021-44790, CVE-2022-0391, CVE-2022-0778, CVE-2022-21271, CVE-2022-21375, CVE-2022-21446, CVE-2022-21461, CVE-2022-21463, CVE-2022-21493, CVE-2022-21494, CVE-2022-21716, CVE-2022-22719, CVE-2022-22720, CVE-2022-22721, CVE-2022-23943, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314, and CVE-2022-25315.

Oracle Taleo Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Taleo. 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	In
CVE-2021-44832	Oracle Taleo Platform	Taleo Connect Client Installer (Apache Log4j)	HTTP	No	6.6	Network	High	High	N

Oracle Utilities Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-44832	Oracle Utilities Framework	General (Apache Log4j)	HTTP	No	6.6	Network	High	High

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Virtualization. 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 RISI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-40438	Oracle Secure	Web Server (Apache	HTTP	Yes	9.0	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
	Global Desktop	HTTP Server)							
CVE-2022-21491	Oracle VM VirtualBox	Core	None	No	7.8	Local	Low	Low	
CVE-2022-21465	Oracle VM VirtualBox	Core	None	No	6.7	Local	Low	High	
CVE-2022-21471	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2022-21487	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	
CVE-2022-21488	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	

Notes:

1. This vulnerability applies to Windows systems only.

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