Oracle Critical Patch Update Advisory - January 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 497 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at January 2022 Critical Patch Update: Executive Summary and Analysis.

Please note that on December 10, 2021, Oracle released a Security Alert for Apache Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers should review the Alert if they have not already done so.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite, version 3.6	Oracle Supply Chain Products
Application Performance Management, versions 13.4.1.0, 13.5.1.0	Enterprise Manager
Big Data Spatial and Graph, versions prior to 23.1	Database
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2410, prior to XCP3110	Systems
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineering Suite
JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.1	JD Edwards
MySQL Cluster, versions 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior, 8.0.27 and prior	MySQL
MySQL Connectors, versions 8.0.27 and prior	MySQL
MySQL Server, versions 5.7.36 and prior, 8.0.27 and prior	MySQL
MySQL Workbench, versions 8.0.27 and prior	MySQL
Oracle Access Manager, versions 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Agile Engineering Data Management, version 6.2.1.0	Oracle Supply Chain Products
Oracle Agile PLM, versions 9.3.3, 9.3.6	Oracle Supply Chain Products
Oracle Agile PLM MCAD Connector, versions 3.4, 3.6	Oracle Supply Chain Products
Oracle Airlines Data Model, versions 12.1.1.0.0, 12.2.0.1.0	Oracle Airlines Data Model
Oracle Application Express, versions prior to 21.1.4	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle Argus Analytics, versions 8.2.1, 8.2.2, 8.2.3	Health Sciences
Oracle Argus Insight, versions 8.2.1, 8.2.2, 8.2.3	Health Sciences
Oracle Argus Mart, versions 8.2.1, 8.2.2, 8.2.3	Health Sciences
Oracle Argus Safety, versions 8.2.1, 8.2.2, 8.2.3	Health Sciences
Oracle Banking APIs, versions 18.1-18.3, 19.1, 19.2, 20.1, 21.1	Contact Support
Oracle Banking Deposits and Lines of Credit Servicing, version 2.12.0	Contact Support
Oracle Banking Digital Experience, versions 17.2, 18.1-18.3, 19.1, 19.2, 20.1, 21.1	Contact Support

Affected Products and Versions	Patch Availability Document
Oracle Banking Enterprise Default Management, versions 2.3.0-2.4.1, 2.6.2, 2.7.0, 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 Platform, versions 2.3.0-2.4.1, 2.6.2, 2.7.0, 2.7.1	Oracle Banking Platform
Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Activity Monitoring, version 12.2.1.4.0	Fusion Middleware
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	Fusion Middleware
Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Clinical, versions 5.2.1, 5.2.2	Health Sciences
Oracle Commerce Guided Search, version 11.3.2	Oracle Commerce
Oracle Commerce Platform, versions 11.3.0, 11.3.1, 11.3.2	Oracle Commerce
Oracle Communications Billing and Revenue Management, versions 12.0.0.3, 12.0.0.4	Oracle Communications Billing and Revenue Management
Oracle Communications BRM - Elastic Charging Engine, versions 11.3, 12.0	Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Calendar Server, version 8.0.0.5.0	Oracle Communications Calendar Ser
Oracle Communications Cloud Native Core Automated Test Suite, version 1.8.0	Oracle Communications Cloud Native Core Automated Test Suite
Oracle Communications Cloud Native Core Binding Support Function, versions 1.9.0, 1.10.0	Oracle Communications Cloud Native Core Binding Support Function
Oracle Communications Cloud Native Core Console, version 1.7.0	Communications Cloud Native Core Console
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, version 1.9.0	Oracle Communications Cloud Native Core Network Function Cloud Native Environment
Oracle Communications Cloud Native Core Network Repository Function, version 1.14.0	Oracle Communications Cloud Native Core Network Repository Function
Oracle Communications Cloud Native Core Policy, version 1.14.0	Communications Cloud Native Core Policy
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 1.5.0, 1.6.0, 1.15.0	Communications Cloud Native Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Service Communication Proxy, version 1.14.0	Communications Cloud Native Core Service Communication Proxy

Affected Products and Versions	Patch Availability Document
Oracle Communications Cloud Native Core Unified Data Repository, version 1.14.0	Communications Cloud Native Core Unified Data Repository
Oracle Communications Contacts Server, version 8.0.0.3.0	Oracle Communications Contacts Ser
Oracle Communications Convergence, version 3.0.2.2.0	Oracle Communications Convergence
Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.4.0.0	Oracle Communications Convergent Charging Controller
Oracle Communications Data Model, versions 11.3.2.1.0, 11.3.2.2.0, 11.3.2.3.0, 12.1.0.1.0, 12.1.2.0.0	Oracle Communications Data Model
Oracle Communications Design Studio, versions 7.3.4, 7.3.5, 7.4.0, 7.4.1, 7.4.2	Oracle Communications Design Studi
Oracle Communications Diameter Signaling Router, versions 8.0.0.0-8.5.1.0	Oracle Communications Diameter Signaling Router
Oracle Communications EAGLE Application Processor, versions 16.1-16.4	Oracle Communications EAGLE Application Processor
Oracle Communications Instant Messaging Server, version 10.0.1.5.0	Oracle Communications Instant Messaging Server
Oracle Communications Interactive Session Recorder, versions 6.3, 6.4	Oracle Communications Interactive Session Recorder
Oracle Communications Messaging Server, version 8.1	Oracle Communications Messaging Server
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
Oracle Communications Network Integrity, versions 7.3.5, 7.3.6	Oracle Communications Network Integrity
Oracle Communications Offline Mediation Controller, version 12.0.0.3	Oracle Communications Offline Mediation Controller
Oracle Communications Operations Monitor, versions 3.4, 4.2, 4.3, 4.4, 5.0	Oracle Communications Operations Monitor
Oracle Communications Pricing Design Center, versions 12.0.0.3.0, 12.0.0.4.0	Oracle Communications Pricing Desig Center
Oracle Communications Service Broker, version 6.2	Oracle Communications Service Brok
Oracle Communications Services Gatekeeper, version 7.0	Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller, versions 8.2, 8.3, 8.4, 9.0	Oracle Communications Session Borc Controller
Oracle Communications Unified Inventory Management, versions 7.3.0, 7.3.4, 7.3.5, 7.4.0, 7.4.1, 7.4.2, 7.5.0	Oracle Communications Unified Inventory Management

Affected Products and Versions	Patch Availability Document
Oracle Communications WebRTC Session Controller, versions 7.2.0, 7.2.1	Oracle Communications WebRTC Ses 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, 12.2.0.1, 19c, 21c	Database
Oracle Demantra Demand Management, versions 12.2.6-12.2.11	Oracle Supply Chain Products
Oracle E-Business Suite, versions 12.2.3-12.2.11	Oracle E-Business Suite
Oracle Enterprise Communications Broker, version 3.3	Oracle Enterprise Communications Broker
Oracle Enterprise Data Quality, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Enterprise Session Border Controller, versions 8.4, 9.0	Oracle Enterprise Session Border Controller
Oracle Essbase, versions prior to 11.1.2.4.47, prior to 21.3	Database
Oracle Essbase Administration Services, versions prior to 11.1.2.4.47	Database
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7-8.1.1	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Behavior Detection Platform, versions 8.0.7, 8.0.8, 8.1.1	Oracle Financial Services Behavior Detection Platform
Oracle Financial Services Enterprise Case Management, versions 8.0.7, 8.0.8, 8.1.1	Oracle Financial Services Enterprise C Management
Oracle Financial Services Foreign Account Tax Compliance Act Management, versions 8.0.7, 8.0.8, 8.1.1	Contact Support
Oracle Financial Services Model Management and Governance, versions 8.0.8-8.1.1	Oracle Financial Services Model Management and Governance
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, versions 8.0.7, 8.0.8	Oracle Financial Services Trade-Base Anti Money Laundering Enterprise Edition
Oracle FLEXCUBE Investor Servicing, versions 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.4.0, 14.5.0	Contact Support
Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0	Contact Support
Oracle Fusion Middleware, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Fusion Middleware MapViewer, version 12.2.1.4.0	Fusion Middleware
Oracle GoldenGate, versions prior to 12.3.0.1, prior to 19.1.0.0.220118, prior to 21.4.0.0.0, prior to 21.5.0.0.220118	Database
Oracle GraalVM Enterprise Edition, versions 20.3.4, 21.3.0	Java SE
Oracle Graph Server and Client, versions prior to 21.4	Database

Affected Products and Versions	Patch Availability Document
Oracle Health Sciences Clinical Development Analytics, version 4.0.1	Health Sciences
Oracle Health Sciences InForm CRF Submit, version 6.2.1	Health Sciences
Oracle Health Sciences Information Manager, versions 3.0.2, 3.0.3	HealthCare Applications
Oracle Healthcare Data Repository, versions 7.0.2, 8.1.0, 8.1.1	HealthCare Applications
Oracle Healthcare Foundation, versions 7.3.0.0-7.3.0.2, 8.0.0-8.0.2, 8.1.0-8.1.1	HealthCare Applications
Oracle Healthcare Translational Research, version 4.1.0	HealthCare Applications
Oracle Hospitality Cruise Shipboard Property Management System, version 20.1.0	Oracle Hospitality Cruise Shipboard Property Management System
Oracle Hospitality OPERA 5, version 5.6	Oracle Hospitality OPERA 5 Property Services
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle Hospitality Suite8, versions 8.10.2, 8.11.0, 8.12.0, 8.13.0, 8.14.0	Oracle Hospitality Suite8
Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Hyperion Infrastructure Technology, version 11.2.7.0	Fusion Middleware
Oracle iLearning, versions 6.2, 6.3	iLearning
Oracle Insurance Data Gateway, versions 11.0.2, 11.1.0, 11.2.7, 11.3.0, 11.3.1	Oracle Insurance Applications
Oracle Insurance Insbridge Rating and Underwriting, versions 5.2.0, 5.4.0-5.6.0	Oracle Insurance Applications
Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0, 11.2.7, 11.3.0, 11.3.1	Oracle Insurance Applications
Oracle Insurance Policy Administration J2EE, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0-11.3.0	Oracle Insurance Applications
Oracle Insurance Rules Palette, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0-11.3.0, 11.3.1	Oracle Insurance Applications
Oracle Java SE, versions 7u321, 8u311, 11.0.13, 17.0.1	Java SE
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle NoSQL Database, versions prior to 21.1.12	NoSQL Database
Oracle Policy Automation, versions 12.2.0-12.2.24	Oracle Policy Automation
Oracle Product Lifecycle Analytics, version 3.6.1	Oracle Supply Chain Products
Oracle Rapid Planning, versions 12.2.6-12.2.11	Oracle Supply Chain Products

Affected Products and Versions	Patch Availability Document
Oracle Real User Experience Insight, versions 13.4.1.0, 13.5.1.0	Enterprise Manager
Oracle REST Data Services, versions prior to 21.2.4	Database
Oracle Retail Allocation, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Analytics, versions 16.0.0-16.0.2	Retail Applications
Oracle Retail Assortment Planning, version 16.0.3	Retail Applications
Oracle Retail Back Office, version 14.1	Retail Applications
Oracle Retail Central Office, version 14.1	Retail Applications
Oracle Retail Customer Insights, versions 16.0.0-16.0.2	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0	Retail Applications
Oracle Retail EFTLink, versions 16.0.3, 17.0.2, 18.0.1, 19.0.1, 20.0.1	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, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Fiscal Management, version 14.2	Retail Applications
Oracle Retail Integration Bus, versions 14.1.3.0, 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, versions 15.0.3, 16.0.3	Retail Applications
Oracle Retail Merchandising System, version 19.0.1	Retail Applications
Oracle Retail Order Broker, versions 16.0, 18.0, 19.1	Retail Applications
Oracle Retail Order Management System, version 19.5	Retail Applications
Oracle Retail Point-of-Service, version 14.1	Retail Applications
Oracle Retail Predictive Application Server, versions 14.1.3, 14.1.3.46, 15.0.3, 15.0.3.115, 16.0.3, 16.0.3.240	Retail Applications
Oracle Retail Price Management, versions 13.2, 14.0.4, 14.1, 14.1.3, 15, 15.0.3, 16, 16.0.3	Retail Applications
Oracle Retail Returns Management, version 14.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1.3.0, 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1	Retail Applications
Oracle Retail Size Profile Optimization, version 16.0.3	Retail Applications
Oracle Retail Xstore Point of Service, versions 17.0.4, 18.0.3, 19.0.2, 20.0.1	Retail Applications
Oracle SD-WAN Aware, version 8.2	Oracle SD-WAN Aware

Affected Products and Versions	Patch Availability Document
Oracle SD-WAN Edge, versions 9.0, 9.1	Oracle SD-WAN Edge
Oracle Secure Backup, versions prior to 18.1.0.1.0	Oracle Secure Backup
Oracle Solaris, versions 10, 11	Systems
Oracle Spatial Studio, versions prior to 21.2.1	Database
Oracle Thesaurus Management System, versions 5.2.3, 5.3.0, 5.3.1	Health Sciences
Oracle TimesTen In-Memory Database, versions prior to 11.2.2.8.27, prior to 21.1.1.1.0	Database
Oracle Utilities Framework, versions 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0	Oracle Utilities Applications
Oracle Utilities Testing Accelerator, versions 6.0.0.1.1, 6.0.0.2.2, 6.0.0.3.1	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.32	Virtualization
Oracle WebCenter Portal, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebLogic Server, versions 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
Oracle ZFS Storage Application Integration Engineering Software, version 1.3.3	Systems
OSS Support Tools, versions prior to 2.12.42	Oracle Support Tools
PeopleSoft Enterprise CS SA Integration Pack, versions 9.0, 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.59	PeopleSoft
Primavera Analytics, versions 18.8.3.3, 19.12.11.1, 20.12.12.0	Oracle Construction and Engineering Suite
Primavera Data Warehouse, versions 18.8.3.3, 19.12.11.1, 20.12.12.0	Oracle Construction and Engineering Suite
Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.13, 19.12.0-19.12.12, 20.12.0-20.12.7, 21.12.0	Oracle Construction and Engineering Suite
Primavera P6 Enterprise Project Portfolio Management, versions 17.12.0.0-17.12.20.0, 18.8.0.0-18.8.24.0, 19.12.0.0-19.12.18.0, 20.12.0.0-20.12.12.0, 21.12.0.0	Oracle Construction and Engineering Suite
Primavera P6 Professional Project Management, versions 17.12.0.0-17.12.20.0, 18.8.0.0-18.8.24.0, 19.12.0.0-19.12.17.0, 20.12.0.0-20.12.9.0	Oracle Construction and Engineering Suite
Primavera Portfolio Management, versions 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0, 20.0.0.1	Oracle Construction and Engineering Suite

Affected Products and Versions	Patch Availability Document
Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12, 21.12	Oracle Construction and Engineering Suite
Siebel Applications, versions 21.12 and prior	Siebel

Note:

- Vulnerabilities affecting either Oracle Database or Oracle Fusion Middleware may affect Oracle Fusion Applications, so Oracle customers should refer to Oracle Fusion Applications Critical Patch Update Knowledge Document, My Oracle Support Note 1967316.1 for information on patches to be applied to Fusion Application environments.
- Vulnerabilities affecting Oracle Solaris may affect Oracle ZFSSA so Oracle customers should refer to the Oracle and Sun Systems Product Suite Critical Patch Update Knowledge Document, My Oracle Support Note 2160904.1 for information on minimum revisions of security patches required to resolve ZFSSA issues published in Critical Patch Updates and Solaris Third Party bulletins.
- Solaris Third Party Bulletins are used to announce security patches for third party software distributed with Oracle Solaris. Solaris 10 customers should refer to the latest patch-sets which contain critical security 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:

- Abdelrhman Yousri: CVE-2022-21246, CVE-2022-21402, CVE-2022-21403
- Alexander Kornbrust of Red Database Security: CVE-2022-21247
- Andrej Simko of Accenture: CVE-2022-21251
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2022-21279, CVE-2022-21280, CVE-2022-21284, CVE-2022-21285, CVE-2022-21286, CVE-2022-21287, CVE-2022-21288, CVE-2022-21289, CVE-2022-21290, CVE-2022-21307, CVE-2022-21308, CVE-2022-21309, CVE-2022-21346
- Aobo Wang of Chaitin Security Research Lab: CVE-2022-21295
- Dan Rabe: CVE-2022-21296
- Dinh Ho Anh Khoa of Viettel Cyber Security: CVE-2022-21306
- Fabian Meumertzheim of Code Intelligence: CVE-2022-21360, CVE-2022-21366
- Frederic Quenneville of videotron.com: CVE-2022-21338
- Hamed Ashraf: CVE-2022-21395, CVE-2022-21396, CVE-2022-21397, CVE-2022-21398, CVE-2022-21399, CVE-2022-21400, CVE-2022-21401
- Hans Christian Woithe: CVE-2021-43395
- Harold Siyu Zang of Trustwave: CVE-2022-21381, CVE-2022-21382, CVE-2022-21383
- Jangggg of VNPT: CVE-2021-35587
- Jeremy Nunn of Trustwave: CVE-2022-21383
- Jie Liang of WingTecher Lab of Tsinghua University: CVE-2022-21303, CVE-2022-21304
- Jingzhou Fu of WingTecher Lab of Tsinghua University: CVE-2022-21303, CVE-2022-21304

- Jonah T: CVE-2022-21371
- Jonni Passki of Apple Information Security: CVE-2022-21282
- Kun Yang of Chaitin Security Research Lab: CVE-2022-21295
- Liboheng of Tophant Starlight laboratory: CVE-2022-21261
- Longofo of Knownsec 404 Team: CVE-2022-21252, CVE-2022-21260
- Lucas Leong (wmliang) of Trend Micro Zero Day Initiative: CVE-2022-21310, CVE-2022-21311, CVE-2022-21312, CVE-2022-21313, CVE-2022-21314, CVE-2022-21315, CVE-2022-21316, CVE-2022-21317, CVE-2022-21318, CVE-2022-21319, CVE-2022-21320, CVE-2022-21321, CVE-2022-21322, CVE-2022-21323, CVE-2022-21324, CVE-2022-21325, CVE-2022-21326, CVE-2022-21327, CVE-2022-21328, CVE-2022-21329, CVE-2022-21330, CVE-2022-21331, CVE-2022-21332, CVE-2022-21333, CVE-2022-21334, CVE-2022-21335, CVE-2022-21336, CVE-2022-21337, CVE-2022-21355, CVE-2022-21356, CVE-2022-21357, CVE-2022-21380
- Markus Loewe: CVE-2022-21293, CVE-2022-21294
- Matei "Mal" Badanoiu: CVE-2022-21392
- osword from SGLAB of Legendsec at Qi'anxin Group: CVE-2022-21347
- Patrick Star of BMH Security Team: CVE-2022-21353
- peterjson - Security Engineering - VNG Corporation: CVE-2021-35587
- r00t4dm: CVE-2022-21252, CVE-2022-21257, CVE-2022-21258, CVE-2022-21259, CVE-2022-21260, CVE-2022-21261, CVE-2022-21262
- RE:HACK: CVE-2022-21373
- Reno Robert working with Trend Micro Zero Day Initiative: CVE-2022-21355, CVE-2022-21356, CVE-2022-21357, CVE-2022-21380
- Ryota Shiga (Ga_ryo_) of Flatt Security working with Trend Micro Zero Day Initiative: CVE-2022-21394
- Sander Meijering of HackDefense: CVE-2022-21371
- Thijmen Kooy of HackDefense: CVE-2022-21371
- thiscodecc of MoyunSec V-Lab: CVE-2022-21292, CVE-2022-21350, CVE-2022-21361
- Victor Rodriguez: CVE-2022-21364
- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2022-21303, CVE-2022-21304
- Zhiqiang Zang of University of Texas at Austin: CVE-2022-21305
- Zhiyong Wu of WingTecher Lab of Tsinghua University: CVE-2022-21303, CVE-2022-21304

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:

- Huixin Ma of Tencent.com [2 reports]
- Liying Wang
- Longofo of Knownsec 404 Team
- r00t4dm
- Robin Textor

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:

- Abderrahmane Elghoul
- Abilash V L
- Abisheik M
- Adam Willard
- Aleena Avarachan
- Ali Alzahrani
- Aniket Nimkar
- Ashik Kunjumon
- B.Dhiyaneshwaran aka (Geek Freak) [2 reports]
- Dhanesh Sivasamy
- Dor Tumarkin, Principal Application Security Researcher at Checkmarx
- Gaurang Maheta [2 reports]
- Jangggg of VNPT
- Kishore Hariram

- Lidor Ben Shitrit from Orca Security
- Lokesh Rulz
- Malicious.Group
- Mohit Ahir
- N3td1v3r
- Nightwatch Cybersecurity Research
- peterjson - Security Engineering - VNG Corporation
- pinkflower
- Quan Doan of R&D Center - VinCSS LLC (a member of Vingroup)
- Rahul PS
- Rob Evans of Fortinet, Inc.
- Rounak Sharma
- Sakhare Vinayak
- Samprit Das (sampritdas8)
- Saptak Saha
- Shubham Choudhery
- Shuvam Adhikari [4 reports]
- Srikar V - exp1o1t9r
- Truffle Security Co
- Yeswanth Reddy

Critical Patch Update Schedule

Critical Patch Updates are released on the Tuesday closest to the 17th day of January, April, July and October. The next four dates are:

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

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - January 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
- Map of CVE to Advisory/Alert
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2024-December-23	Rev 7. Corrected the CVE credits for WebLogic bugs
2022-March-14	Rev 6. Updated the version details and addtional CVEs (CVE-2022-23302, CVE-2022 23305 and CVE-2022-23307) for Oracle WebLogic Server
2022-Januray-31	Rev 5. Version details updated for Oracle HTTP Server and Oracle Business Activity Monitoring
2022-Januray-27	Rev 4. Retail matrix version changes and added credit for CVE-2022-21353
2022-Januray-24	Rev 3. CVSS update for CVE-2022-21392 and aded credit for CVE-2022-21346
2022-January-18	Rev 2. Updated Siebel Applications versions and added couple of credit names
2022-January-18	Rev 1. Initial Release

Oracle Database Products Risk Matrices

This Critical Patch Update contains 28 new security patches for Oracle Database Products divided as follows:

- 4 new security patches for Oracle Database Products
- 1 new security patch for Oracle Airlines Data Model
- 2 new security patches for Oracle Big Data Graph
- 1 new security patch for Oracle Communications Data Model
- 4 new security patches for Oracle Essbase

- 3 new security patches for Oracle GoldenGate
- 2 new security patches for Oracle Graph Server and Client
- 1 new security patch for Oracle NoSQL Database
- 2 new security patches for Oracle REST Data Services
- 2 new security patches for Oracle Secure Backup
- 1 new security patch for Oracle Spatial Studio
- 5 new security patches for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 4 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 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-37695	Oracle Application Express (CKEditor)	Valid User Account	HTTP	No	5.4	Network	Low	Low	
CVE-2022-21393	Java VM	Create Procedure	Oracle Net	No	4.3	Network	Low	Low	
CVE-2021-32723	Oracle Application Express (Prism)	Valid User Account	HTTP	No	3.5	Network	Low	Low	
CVE-2022-21247	Core RDBMS	Create Session, Execute Catalog Role	Oracle Net	No	2.7	Network	Low	High	

Additional CVEs addressed are:

- The patch for CVE-2021-37695 also addresses CVE-2021-32808 and CVE-2021-32809.

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

- Oracle Database Configuration Assistant (Apache Commons Compress): CVE-2021-36090, CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.
- Oracle Spatial and Graph (Apache Log4j): CVE-2021-45105.
- Trace file analyzer (Apache Log4j): CVE-2021-45105.
- Workload Manager (Guava): CVE-2020-8908.
- Workload Manager (Jetty): CVE-2021-28165, CVE-2021-28169 and CVE-2021-34428.

Oracle Airlines Data Model Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Airlines Data Model. 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 (se				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2021-2351	Oracle Airlines Data Model	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	None	Requ

Oracle Big Data Graph Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-2351	Big Data Spatial and Graph	Big Data Graph (JDBC)	Oracle Net	Yes	8.3	Network	High	None	Re
CVE-2021-30639	Big Data Spatial and Graph	Big Data Graph (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None	N

Oracle Communications Data Model Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Communications Data Model. 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			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-2351	Oracle Communications Data Model	Utilities (JDBC)	Oracle Net	Yes	8.3	Network	High	No

Oracle Essbase Risk Matrix

This Critical Patch Update contains 4 new security patches plus additional third party patches noted below for Oracle Essbase. 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 VER		
					Base Score	Attack Vector	Atta Comp
CVE-2021-35683	Oracle Essbase Administration Services	EAS Console	HTTP	No	9.9	Network	Lov
CVE-2021-3711	Oracle Essbase	Infrastructure (OpenSSL)	HTTPS	Yes	9.8	Network	Lov
CVE-2021-22901	Oracle Essbase	Build (cURL)	HTTPS	Yes	7.5	Network	Hig
CVE-2021-20718	Oracle Essbase	Infrastructure (mod_auth_openidc)	Multiple	Yes	7.5	Network	Lov

Additional CVEs addressed are:

- The patch for CVE-2021-22901 also addresses CVE-2021-22897 and CVE-2021-22898.
- The patch for CVE-2021-3711 also addresses CVE-2021-3712.

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

- Oracle Essbase
  - Infrastructure (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 3 new security patches for Oracle GoldenGate. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-23017	Oracle GoldenGate	GG Market Place for Support (nginx)	UDP	Yes	9.4	Network	Low	None
CVE-2021-2351	Oracle GoldenGate	Database (OCCI)	Oracle Net	Yes	8.3	Network	High	None
CVE-2018-1311	Oracle GoldenGate	Build Request (Apache Xerces-C++)	HTTP	Yes	8.1	Network	High	None

Oracle Graph Server and Client Risk Matrix

This Critical Patch Update contains 2 new security patches plus additional third party patches noted below for Oracle Graph Server and Client. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Graph Server and Client	Packaging/install issues (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-33037	Oracle Graph Server and Client	Packaging/Install (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	None

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

- Oracle Graph Server and Client
  - Packaging/Install (Apache Commons IO): CVE-2021-29425.

Oracle NoSQL Database Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle NoSQL Database. 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 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2021-21409	Oracle NoSQL Database	Administration (Netty)	Local Logon	No	5.5	Local	Low	Low	

Oracle REST Data Services Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle REST Data Services. 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	U Int
CVE-2021-28165	Oracle REST Data Services	General (Eclipse Jetty)	Multiple	Yes	7.5	Network	Low	None	N
CVE-2021-32014	Oracle REST Data Services	General (SheetJS)	Local Logon	No	3.3	Local	Low	None	Re

Additional CVEs addressed are:

- The patch for CVE-2021-28165 also addresses CVE-2021-28169 and CVE-2021-34428.
- The patch for CVE-2021-32014 also addresses CVE-2021-32012 and CVE-2021-32013.

Oracle Secure Backup Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2021-26691	Oracle Secure Backup	Oracle Secure Backup (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	None	N
CVE-2021-3712	Oracle Secure Backup	Oracle Secure Backup (OpenSSL)	HTTPS	Yes	7.4	Network	High	None	N

Additional CVEs addressed are:

- The patch for CVE-2021-26691 also addresses CVE-2021-33193 and CVE-2021-42013.

Oracle Spatial Studio Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Spatial Studio. 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 (se				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2021-2351	Oracle Spatial Studio	Install (JDBC)	Oracle Net	Yes	8.3	Network	High	None	Requ

Oracle TimesTen In-Memory Database Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle TimesTen In-Memory Database	EM TimesTen plug-in (JDBC,OCCI)	OracleNet	Yes	8.3	Network	High	None
CVE-2021-29923	Oracle TimesTen In-Memory Database	EM TimesTen plug-in (Go)	TCP/IP	Yes	7.5	Network	Low	None
CVE-2021-29923	Oracle TimesTen In-Memory Database	Install (Go)	TCP/IP	Yes	7.5	Network	Low	None
CVE-2020-7712	Oracle TimesTen In-Memory Database	TimesTen Infrastructure (Apache ZooKeeper)	HTTP	No	7.2	Network	Low	High
CVE-2020-11979	Oracle TimesTen In-	Install (Apache Ant)	Local Logon	No	6.5	Network	Low	Low

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

Additional CVEs addressed are:

- The patch for CVE-2020-11979 also addresses CVE-2020-1945, CVE-2021-36373 and CVE-2021-36374.
- The patch for CVE-2021-29923 also addresses CVE-2021-34558 and CVE-2021-36221.

Oracle Commerce Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Commerce Platform	Dynamo Application Framework (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-36090	Oracle Commerce Guided Search	Content Acquisition System (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-37137	Oracle Commerce Guided Search	Content Acquisition System (Netty)	HTTP	Yes	7.5	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-13935	Oracle Commerce Guided Search	Endeca Application Controller (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None
CVE-2022-21387	Oracle Commerce Platform	Dynamo Application Framework	HTTP	Yes	5.3	Network	Low	None
CVE-2021-29425	Oracle Commerce Guided Search	Content Acquisition System (Apache Commons IO)	HTTP	Yes	4.8	Network	High	None

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-2021-37137 also addresses CVE-2021-37136.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 33 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 VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21275	Oracle Communications Billing and Revenue Management	Connection Manager	HTTP	Yes	10.0	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21389	Oracle Communications Billing and Revenue Management	Connection Manager	HTTP	Yes	10.0	Network	Low
CVE-2022-21390	Oracle Communications Billing and Revenue Management	Webservices Manager	HTTP	Yes	10.0	Network	Low
CVE-2022-21276	Oracle Communications Billing and Revenue Management	Connection Manager	HTTP	No	9.9	Network	Low
CVE-2022-21391	Oracle Communications Billing and Revenue Management	Connection Manager	HTTP	No	9.9	Network	Low
CVE-2021-39139	Oracle Communications BRM - Elastic Charging Engine	Updater (XStream)	TCP	No	8.8	Network	Low
CVE-2021-29505	Oracle Communications Unified Inventory Management	Rulesets (XStream)	HTTP	No	8.8	Network	Low
CVE-2021-2351	Oracle Communications Calendar Server	Administration (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Oracle Communications Contacts Server	Database (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Oracle Communications Convergent Charging Controller	ACS (JDBC)	Oracle Net	Yes	8.3	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-2351	Oracle Communications Design Studio	OSM, NI Plugins (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Oracle Communications Network Charging and Control	ACS (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Oracle Communications Network Integrity	Installer (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2020-28052	Oracle Communications Convergence	Messaging (Bouncy Castle Java Library)	S/MIME	Yes	8.1	Network	High
CVE-2020-24750	Oracle Communications Instant Messaging Server	PresenceApi (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-24750	Oracle Communications Offline Mediation Controller	Installer (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-24750	Oracle Communications Pricing Design Center	Installation (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2021-22118	Oracle Communications Unified Inventory Management	TMF API (Spring Framework)	None	No	7.8	Local	Low
CVE-2022-21266	Oracle Communications Billing and Revenue Management	Pipeline Manager	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2021-25122	Oracle Communications Instant Messaging Server	DBPlugin (Apache Tomcat)	XMPP	Yes	7.5	Network	Low
CVE-2021-37714	Oracle Communications Messaging Server	ISC (jsoup)	HTTP	Yes	7.5	Network	Low
CVE-2021-36090	Oracle Communications Unified Inventory Management	Inventory Organizer (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2019-10086	Oracle Communications Convergence	Message Store (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2019-10086	Oracle Communications Design Studio	Inventory (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2020-5421	Oracle Communications Design Studio	Inventory (Spring Framework)	HTTP	No	6.5	Network	High
CVE-2021-36374	Oracle Communications Unified Inventory Management	Build Tool (Apache Ant)	None	No	5.5	Local	Low
CVE-2021-29425	Oracle Communications BRM - Elastic Charging Engine	Charging Controller (Apache Commons IO)	TCP	Yes	4.8	Network	High
CVE-2021-29425	Oracle Communications Convergence	Convergence Server (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2021-29425	Oracle Communications	Installation (Apache	HTTP	Yes	4.8	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Offline Mediation Controller	Commons IO)					
CVE-2022-21338	Oracle Communications Convergence	General Framework	HTTP	No	4.6	Network	Low
CVE-2022-21267	Oracle Communications Billing and Revenue Management	Pipeline Manager	None	No	3.3	Local	Low
CVE-2022-21268	Oracle Communications Billing and Revenue Management	Pipeline Manager	None	No	3.3	Local	Low
CVE-2022-21388	Oracle Communications Pricing Design Center	On Premise Install	None	No	3.3	Local	Low

Additional CVEs addressed are:

- The patch for CVE-2020-24750 also addresses CVE-2020-24616, CVE-2020-25649 and CVE-2020-36189.
- The patch for CVE-2021-25122 also addresses CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25329 and CVE-2021-33037.
- The patch for CVE-2021-29505 also addresses CVE-2021-39154.
- 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 Communications Risk Matrix

This Critical Patch Update contains 84 new security patches plus additional third party patches noted below for Oracle Communications. 50 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-2021-23440	Oracle Communications Cloud Native Core Policy	Policy (set-value)	HTTP	Yes	9.8	Network	Low
CVE-2021-21783	Oracle Communications EAGLE Application Processor	Platform (gSOAP)	HTTP	Yes	9.8	Network	Low
CVE-2021-32827	Oracle Communications Cloud Native Core Policy	Policy (MockServer)	HTTP	Yes	9.6	Network	Low
CVE-2021-27568	Oracle Communications Cloud Native Core Policy	Policy (netplex json-smart)	HTTP	Yes	9.1	Network	Low
CVE-2021-39139	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (XStream)	HTTP	No	8.8	Network	Low
CVE-2019-13734	Oracle Communications Cloud Native Core Network Repository Function	NRF (SQLite)	HTTP	Yes	8.8	Network	Low
CVE-2020-13936	Oracle Communications Cloud Native Core Policy	Policy (Apache Velocity Engine)	HTTP	No	8.8	Network	Low
CVE-2020-15824	Oracle Communications Cloud Native Core Policy	Policy (Kotlin)	HTTP	No	8.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2020-10878	Oracle Communications EAGLE Application Processor	Platform (Perl)	HTTP	Yes	8.6	Network	Low
CVE-2021-39153	Oracle Communications Cloud Native Core Policy	Signaling (XStream)	HTTP	No	8.5	Network	High
CVE-2020-36189	Oracle Communications Cloud Native Core Policy	Policy (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2021-22118	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22118	Oracle Communications Cloud Native Core Policy	Policy (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22118	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22118	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22118	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Spring Framework)	None	No	7.8	Local	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-33909	Oracle Communications Session Border Controller	Core (Kernel)	None	No	7.8	Local	Low
CVE-2022-21382	Oracle Enterprise Session Border Controller	WebUI	HTTP	No	7.7	Network	Low
CVE-2020-17527	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2021-37137	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (Netty)	TCP	Yes	7.5	Network	Low
CVE-2021-33560	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	Configuration (libgcrypt)	TCP	Yes	7.5	Network	Low
CVE-2020-13949	Oracle Communications Cloud Native Core Policy	Policy (Apache Thrift)	HTTP	Yes	7.5	Network	Low
CVE-2020-17527	Oracle Communications Cloud Native Core Policy	Policy (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2021-28165	Oracle Communications Cloud Native Core Policy	Policy (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2021-22119	Oracle Communications	Policy (Spring Security)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Cloud Native Core Policy						
CVE-2020-28469	Oracle Communications Cloud Native Core Policy	Policy (glob-parent)	HTTP	Yes	7.5	Network	Low
CVE-2021-25122	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2021-36090	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2021-36090	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2021-37137	Oracle Communications Diameter Signaling Router	API Gateway (Netty)	HTTP	Yes	7.5	Network	Low
CVE-2021-42340	Oracle Communications Diameter Signaling Router	Platform (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2021-42340	Oracle SD-WAN Edge	Management (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2021-23337	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (Lodash)	HTTP	No	7.2	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21395	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	7.2	Network	Low
CVE-2021-23337	Oracle Communications Services Gatekeeper	Policy service (Lodash)	HTTP	No	7.2	Network	Low
CVE-2021-21703	Oracle Communications Diameter Signaling Router	Platform (PHP)	None	No	7.0	Local	High
CVE-2021-44832	Oracle Communications Diameter Signaling Router	Virtual Network Function Manager, API Gateway (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Oracle Communications Interactive Session Recorder	RSS (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2022-21399	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	6.6	Network	Low
CVE-2022-21401	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	6.6	Network	Low
CVE-2022-21403	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	6.6	Network	Low
CVE-2022-21381	Oracle Enterprise Session Border Controller	WebUI	HTTP	No	6.4	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2020-11022	Oracle Communications EAGLE Application Processor	Platform (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-11022	Oracle Communications Services Gatekeeper	API Portal (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2021-21409	Oracle Communications Cloud Native Core Console	Console (Netty)	HTTP	Yes	5.9	Network	High
CVE-2020-14340	Oracle Communications Cloud Native Core Network Repository Function	Network Repository Function (XNIO)	HTTP	Yes	5.9	Network	High
CVE-2020-14340	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (XNIO)	HTTP	Yes	5.9	Network	High
CVE-2021-33880	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (aaugustin websockets)	HTTP	Yes	5.9	Network	High
CVE-2021-3326	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (glibc)	HTTP	Yes	5.9	Network	High
CVE-2020-14340	Oracle Communications Cloud Native Core Service	SCP (XNIO)	HTTP	Yes	5.9	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Communication Proxy						
CVE-2021-33880	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (aaugustin websockets)	HTTP	Yes	5.9	Network	High
CVE-2020-14340	Oracle Communications Cloud Native Core Unified Data Repository	UDR (XNIO)	HTTP	Yes	5.9	Network	High
CVE-2021-33880	Oracle Communications Cloud Native Core Unified Data Repository	UDR (aaugustin websockets)	HTTP	Yes	5.9	Network	High
CVE-2021-45105	Oracle Communications Service Broker	Integration (Apache Log4j)	HTTP	Yes	5.9	Network	High
CVE-2021-45105	Oracle Communications Services Gatekeeper	API Portal (Apache Log4j)	HTTP	Yes	5.9	Network	High
CVE-2021-45105	Oracle Communications WebRTC Session Controller	Signaling Engine, Media Engine (Apache Log4j)	HTTP	Yes	5.9	Network	High
CVE-2021-3426	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (Python)	Multiple	No	5.7	Adjacent Network	Low
CVE-2021-23017	Oracle Communications Session Border Controller	Routing (nginx)	HTTP	Yes	5.6	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-23017	Oracle Enterprise Communications Broker	Routing (nginx)	HTTP	Yes	5.6	Network	High
CVE-2021-23017	Oracle Enterprise Session Border Controller	Routing (nginx)	HTTP	Yes	5.6	Network	High
CVE-2020-27618	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (glibc)	None	No	5.5	Local	Low
CVE-2022-21246	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	5.4	Network	Low
CVE-2022-21396	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	5.4	Network	Low
CVE-2022-21397	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	5.4	Network	Low
CVE-2022-21398	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	5.4	Network	Low
CVE-2022-21400	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	5.4	Network	Low
CVE-2021-34429	Oracle Communications Cloud Native Core Binding Support Function	Binding Support Function (Eclipse Jetty)	TCP	Yes	5.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-34429	Oracle Communications Cloud Native Core Security Edge Protection Proxy	SEPP (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2020-13956	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Apache HttpClient)	HTTP	Yes	5.3	Network	Low
CVE-2021-33037	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Apache Tomcat)	HTTP	Yes	5.3	Network	Low
CVE-2021-34429	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2020-29582	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Kotlin)	HTTP	Yes	5.3	Network	Low
CVE-2021-34429	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2021-34429	Oracle Communications Diameter Signaling Router	API Gateway (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2021-21705	Oracle SD-WAN Aware	Management (PHP)	HTTP	Yes	5.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2020-8554	Oracle Communications Cloud Native Core Service Communication Proxy	SCP (Kubernetes API)	HTTP	No	5.0	Network	High
CVE-2020-8554	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Kubernetes API)	HTTP	No	5.0	Network	High
CVE-2021-29921	Oracle Communications Cloud Native Core Automated Test Suite	ATS Framework (Python)	HTTP	No	4.9	Network	Low
CVE-2021-29425	Oracle Communications Cloud Native Core Network Repository Function	NRF (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2021-29425	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2022-21402	Oracle Communications Operations Monitor	Mediation Engine	HTTP	No	4.8	Network	Low
CVE-2022-21383	Oracle Enterprise Session Border Controller	Log	HTTP	No	4.3	Network	Low
CVE-2021-3448	Oracle Communications Cloud Native Core Network Function Cloud	Configuration (dnsmasq)	TCP	Yes	4.0	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Native Environment						
CVE-2020-8908	Oracle Communications Cloud Native Core Unified Data Repository	UDR (Guava)	None	No	3.3	Local	Low

Notes:

1. This patch also addresses vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers need not apply the patches/mitigations of Security Alert CVE-2021-44228 and CVE-2021-45046 for this product.

Additional CVEs addressed are:

- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723.
- The patch for CVE-2020-11022 also addresses CVE-2019-11358 and CVE-2020-11023.
- The patch for CVE-2020-17527 also addresses CVE-2020-13934, CVE-2020-13935, CVE-2020-9484, CVE-2021-25122, CVE-2021-25329, CVE-2021-30369, CVE-2021-30640 and CVE-2021-33037.
- The patch for CVE-2020-36189 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 and CVE-2020-36188.
- The patch for CVE-2021-23337 also addresses CVE-2020-28500.
- The patch for CVE-2021-25122 also addresses CVE-2021-25329.
- 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-2021-39139 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-2021-39153 also addresses CVE-2021-39139, 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 and CVE-2021-39154.

- The patch for CVE-2021-42340 also addresses CVE-2021-33037.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

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

- Oracle Communications Cloud Native Core Network Repository Function
    - NRF (Apache Commons Compress): CVE-2021-36090, CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 22 new security patches for Oracle Construction and Engineering. 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 VERSI		
					Base Score	Attack Vector	Attack Complex
CVE-2021-44790	Instantis EnterpriseTrack	Core (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low
CVE-2021-42575	Primavera Unifier	Platform, Data Persistence (OWASP Java HTML Sanitizer)	HTTP	Yes	9.8	Network	Low
CVE-2021-2351	Primavera Analytics	ETL (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Primavera Data Warehouse	ETL (JDBC)	Oracle Net	Yes	8.3	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2021-2351	Primavera P6 Enterprise Project Portfolio Management	Web Access (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Primavera P6 Professional Project Management	API component of P6 Pro (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Primavera Unifier	Platform,Data Access,Data Persistence (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-37714	Primavera Unifier	Platform,Data Parsing (jsoup)	HTTP	Yes	7.5	Network	Low
CVE-2021-44832	Primavera Gateway	Admin (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Primavera P6 Enterprise Project Portfolio Management	Web Access (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2021-44832	Primavera Unifier	Logging (Apache Log4j)	HTTP	No	6.6	Network	High
CVE-2022-21269	Primavera Portfolio Management	Web Access	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2021-45105	Instantis EnterpriseTrack	Logging (Apache Log4j)	HTTP	Yes	5.9	Network	High
CVE-2021-38153	Primavera Unifier	Event Streams and Communications (Apache Kafka)	HTTP	Yes	5.9	Network	High
CVE-2022-21377	Primavera Portfolio Management	Web API	HTTP	Yes	5.4	Network	Low
CVE-2022-21242	Primavera Portfolio Management	Web Access	HTTP	No	5.4	Network	Low
CVE-2022-21376	Primavera Portfolio Management	Web Access	HTTP	Yes	5.4	Network	Low
CVE-2022-21281	Primavera Portfolio Management	Web Access	HTTP	No	4.8	Network	Low
CVE-2021-29425	Primavera Unifier	Platform (Apache Commons IO)	HTTP	Yes	4.8	Network	High
CVE-2022-21243	Primavera Portfolio Management	Web Access	HTTP	No	4.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSI		
					Base Score	Attack Vector	Attack Comple
CVE-2022-21244	Primavera Portfolio Management	Web Access	HTTP	Yes	4.3	Network	Low
CVE-2020-8908	Primavera Unifier	Data Service (Guava)	None	No	3.3	Local	Low

Notes:

1. This patch also addresses vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers need not apply the patches/mitigations of Security Alert CVE-2021-44228 and CVE-2021-45046 for this product.

Additional CVEs addressed are:

- The patch for CVE-2021-44790 also addresses CVE-2021-33193, CVE-2021-34798, CVE-2021-36160, CVE-2021-39275, CVE-2021-40438, CVE-2021-41524, CVE-2021-41773, CVE-2021-42013 and CVE-2021-44224.
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle E-Business Suite. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle E-Business Suite products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle E-Business Suite products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that

customers apply the January 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 (January 2022), My Oracle Support Note 2484000.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2022-21255	Oracle Configurator	UI Servlet	HTTP	No	8.1	Network	Low	Low
CVE-2022-21273	Oracle Project Costing	Expenses, Currency Override	HTTP	No	8.1	Network	Low	Low
CVE-2022-21274	Oracle Sourcing	Intelligence, RFx Creation	HTTP	No	8.1	Network	Low	Low
CVE-2022-21250	Oracle Trade Management	GL Accounts	HTTP	No	8.1	Network	Low	Low
CVE-2022-21251	Oracle Installed Base	Instance Main	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-10086	Oracle Time and Labor	Timecard (Apache Commons Beanutils)	HTTP	Yes	7.3	Network	Low	Non
CVE-2020-6950	Oracle Time and Labor	Timecard (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low	Non
CVE-2022-21354	Oracle iStore	User Interface	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21373	Oracle Partner Management	Reseller Locator	HTTP	Yes	6.1	Network	Low	Non

Additional CVEs addressed are:

- The patch for CVE-2020-6950 also addresses CVE-2019-17091.

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Enterprise Manager. 6 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found here.

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the January 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 January 2022 Patch Availability Document for Oracle Products, My Oracle Support Note 2817011.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-3177	Enterprise Manager Ops Center	Networking (Python)	HTTP	Yes	9.8	Network	Low	Non
CVE-2022-21392	Enterprise Manager Base Platform	Policy Framework	None	No	8.8	Local	Low	Lov
CVE-2021-2351	Application Performance Management	End User Experience Management (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Enterprise Manager Base Platform	Enterprise Manager Install (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Enterprise Manager Ops Center	Networking (JDBC)	Oracle Net	Yes	8.3	Network	High	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-2351	Oracle Application Testing Suite	Load Testing for Web Apps (JDBC, OCCI)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Real User Experience Insight	End User Experience Management (OCCI)	Oracle Net	Yes	8.3	Network	High	Non

Additional CVEs addressed are:

- The patch for CVE-2021-3177 also addresses CVE-2021-23336.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 48 new security patches for Oracle Financial Services Applications. 37 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2019-17495	Oracle Banking APIs	Framework (Swagger UI)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-17495	Oracle Banking Digital Experience	Framework (Swagger UI)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-13936	Oracle Banking Deposits and Lines of Credit Servicing	Web UI (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-13936	Oracle Banking Enterprise Default Management	Collections (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	L
CVE-2020-13936	Oracle Banking Loans Servicing	Web UI (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	L
CVE-2020-13936	Oracle Banking Party Management	Web UI (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	L
CVE-2020-13936	Oracle Banking Platform	Security (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	L
CVE-2021-2351	Oracle Banking APIs	Framework (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Banking Digital Experience	Framework (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Financial Services Analytical Applications Infrastructure	Rate Management (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Financial Services Behavior Detection Platform	Third Party (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Financial Services Enterprise	Installers (JDBC)	Oracle Net	Yes	8.3	Network	High	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Case Management							
CVE-2021-2351	Oracle Financial Services Foreign Account Tax Compliance Act Management	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2021-2351	Oracle Financial Services Model Management and Governance	Installer & Configuration (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2021-2351	Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition	User Interface (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2021-2351	Oracle FLEXCUBE Investor Servicing	Infrastructure Code (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2021-2351	Oracle FLEXCUBE Private Banking	Miscellaneous (JDBC)	Oracle Net	Yes	8.3	Network	High	No
CVE-2020-11987	Oracle Banking APIs	Framework (Apache Batik)	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-11987	Oracle Banking Digital Experience	Framework (Apache Batik)	HTTP	Yes	8.2	Network	Low	N
CVE-2021-22118	Oracle Financial Services Analytical Applications Infrastructure	Others (Spring Framework)	None	No	7.8	Local	Low	L
CVE-2021-36090	Oracle Banking APIs	Framework (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-25649	Oracle Banking APIs	Framework (jackson-databind)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-37137	Oracle Banking APIs	Framework (Netty)	Multiple	Yes	7.5	Network	Low	N
CVE-2021-36090	Oracle Banking Digital Experience	Framework (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-37137	Oracle Banking Digital Experience	Framework (Netty)	Multiple	Yes	7.5	Network	Low	N
CVE-2021-36090	Oracle Banking Enterprise Default Management	Collections (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-36090	Oracle Banking Party Management	Web UI (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2021-35043	Oracle Banking Enterprise	Collections (AntiSamy)	HTTP	Yes	6.1	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Default Management							
CVE-2020-9281	Oracle Banking Enterprise Default Management	Collections (CKEditor)	HTTP	Yes	6.1	Network	Low	No
CVE-2021-35043	Oracle Banking Party Management	Web UI (AntiSamy)	HTTP	Yes	6.1	Network	Low	No
CVE-2021-35043	Oracle Banking Platform	SECURITY (AntiSamy)	HTTP	Yes	6.1	Network	Low	No
CVE-2021-45105	Oracle Financial Services Analytical Applications Infrastructure	Others (Apache Log4j)	HTTP	Yes	5.9	Network	High	No
CVE-2021-45105	Oracle Financial Services Model Management and Governance	Installer & Configuration (Apache Log4j)	HTTP	Yes	5.9	Network	High	No
CVE-2021-41165	Oracle Banking APIs	Framework (CKEditor)	HTTP	No	5.4	Network	Low	L
CVE-2021-41165	Oracle Banking Digital Experience	Framework (CKEditor)	HTTP	No	5.4	Network	Low	L
CVE-2021-37695	Oracle Banking Party Management	Web UI (CKEditor)	HTTP	No	5.4	Network	Low	L
CVE-2021-37695	Oracle Financial Services	Others (CKEditor)	HTTP	No	5.4	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Analytical Applications Infrastructure							
CVE-2021-28164	Oracle Banking APIs	Framework (Apache Ignite)	HTTP	Yes	5.3	Network	Low	No
CVE-2021-28164	Oracle Banking Digital Experience	Framework (Apache Ignite)	HTTP	Yes	5.3	Network	Low	No
CVE-2021-35687	Oracle Financial Services Analytical Applications Infrastructure	Unified Metadata Manager	HTTP	Yes	5.3	Network	Low	No
CVE-2021-29425	Oracle Banking APIs	Framework (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No
CVE-2021-29425	Oracle Banking Digital Experience	Framework (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No
CVE-2021-29425	Oracle Banking Enterprise Default Management	Collections (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No
CVE-2021-29425	Oracle Banking Party Management	Web UI (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No
CVE-2021-29425	Oracle Banking Platform	Security (Apache Commons IO)	HTTP	Yes	4.8	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-29425	Oracle Financial Services Analytical Applications Infrastructure	Others (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N
CVE-2021-29425	Oracle Financial Services Model Management and Governance	Installer & Configuration (Apache Commons IO)	HTTP	Yes	4.8	Network	High	N
CVE-2021-35686	Oracle Financial Services Analytical Applications Infrastructure	Unified Metadata Manager	HTTP	No	4.3	Network	Low	L

Notes:

1. This patch also addresses vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers need not apply the patches/mitigations of Security Alert CVE-2021-44228 and CVE-2021-45046 for this product.

Additional CVEs addressed are:

- The patch for CVE-2021-28164 also addresses CVE-2021-28163.
- 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-2021-37695 also addresses CVE-2021-32808 and CVE-2021-32809.
- The patch for CVE-2021-41165 also addresses CVE-2021-41164.

Oracle Food and Beverage Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-10086	Oracle Hospitality Reporting and Analytics	Reporting (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	None

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 39 new security patches for Oracle Fusion Middleware. 35 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security updates are not listed in the Oracle Fusion Middleware risk matrix. However, since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the Critical Patch Update January 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 January 2022 Patch Availability Document for Oracle Products, My Oracle Support Note 2817011.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-35587	Oracle Access Manager	OpenSSO Agent	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-17530	Oracle Business	Installation (Apache	HTTP	Yes	9.8	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
	Intelligence Enterprise Edition	Struts2)						
CVE-2022-21306	Oracle WebLogic Server	Core	T3	Yes	9.8	Network	Low	Non
CVE-2021-40438	Oracle HTTP Server	OSSL Module (Apache HTTP Server)	HTTP	Yes	9.0	Network	High	Non
CVE-2021-39154	Oracle Business Activity Monitoring	Centralized Thirdparty Jars (XStream)	HTTP	No	8.5	Network	High	Low
CVE-2021-2351	Oracle Data Integrator	Runtime Java agent for ODI (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Enterprise Data Quality	General (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Fusion Middleware	Centralized Third-party Jars (JDBC, OCCI, ODP for .NET)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2022-21346	Oracle BI Publisher	BI Publisher Security	HTTP	Yes	7.5	Network	Low	Non
CVE-2019-17566	Oracle Business Intelligence Enterprise Edition	Analytics Web Answers (Apache Batik)	HTTP	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'
CVE-2021-36090	Oracle Business Process Management Suite	Installer (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	Non
CVE-2021-4104	Oracle WebLogic Server	Centralized Thirdparty Jars (Apache Log4j)	HTTP	No	7.5	Network	High	Low
CVE-2022-21292	Oracle WebLogic Server	Samples	HTTP	Yes	7.5	Network	Low	Non
CVE-2020-5258	Oracle WebLogic Server	Samples (dojo)	HTTP	Yes	7.5	Network	Low	Non
CVE-2022-21371	Oracle WebLogic Server	Web Container	HTTP	Yes	7.5	Network	Low	Non
CVE-2021-27568	Oracle WebLogic Server	Web Services (json-smart)	HTTP	Yes	7.5	Network	Low	Non
CVE-2021-44832	Oracle WebLogic Server	Centralized Thirdparty Jars (Apache Log4j)	HTTP	No	6.6	Network	High	High
CVE-2022-21252	Oracle WebLogic Server	Samples	HTTP	Yes	6.5	Network	Low	Non
CVE-2022-21347	Oracle WebLogic Server	Core	T3	Yes	6.5	Network	Low	Non
CVE-2022-21350	Oracle WebLogic Server	Core	T3	Yes	6.5	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2022-21353	Oracle WebLogic Server	Core	T3	Yes	6.5	Network	Low	Non
CVE-2020-2934	Oracle WebLogic Server	Datasource (MySQL Connector)	SQL	Yes	6.3	Network	Low	Non
CVE-2022-21361	Oracle WebLogic Server	Sample apps	HTTP	Yes	6.1	Network	Low	Non
CVE-2020-11023	Oracle WebLogic Server	Sample apps (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21257	Oracle WebLogic Server	Samples	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21258	Oracle WebLogic Server	Samples	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21259	Oracle WebLogic Server	Samples	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21260	Oracle WebLogic Server	Samples	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21261	Oracle WebLogic Server	Samples	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21262	Oracle WebLogic Server	Samples	HTTP	Yes	6.1	Network	Low	Non
CVE-2022-21386	Oracle WebLogic Server	Web Container	HTTP	Yes	6.1	Network	Low	Non
CVE-2019-10219	Oracle WebLogic Server	Web Services (JBoss Enterprise	HTTP	Yes	6.1	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
		Application Platform)						
CVE-2021-45105	Oracle Business Intelligence Enterprise Edition	Analytics Server (Apache Log4j)	HTTP	Yes	5.9	Network	High	Non
CVE-2021-45105	Oracle Managed File Transfer	MFT Runtime Server (Apache Log4j)	HTTP	Yes	5.9	Network	High	Non
CVE-2021-45105	Oracle WebCenter Portal	Security Framework (Apache Log4j)	HTTP	Yes	5.9	Network	High	Non
CVE-2018-1324	Oracle WebLogic Server	WLST (Apache Commons Compress)	None	No	5.5	Local	Low	Non
CVE-2020-13956	Oracle WebLogic Server	Samples (Apache HttpClient)	HTTP	Yes	5.3	Network	Low	Non
CVE-2021-29425	Oracle Fusion Middleware MapViewer	Install (Apache Commons IO)	HTTP	Yes	4.8	Network	High	Non
CVE-2021-29425	Oracle WebLogic Server	Third Party Tools (Apache Commons IO)	HTTP	Yes	4.8	Network	High	Non

Notes:

1. This patch also addresses vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers need not apply the patches/mitigations of Security Alert CVE-2021-44228 and CVE-2021-45046 for this product.

Additional CVEs addressed are:

- The patch for CVE-2018-1324 also addresses CVE-2018-11771.
- The patch for CVE-2020-11023 also addresses CVE-2019-11358 and CVE-2020-11022.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.
- The patch for CVE-2021-39154 also addresses CVE-2021-29505, 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 and CVE-2021-39153.
- The patch for CVE-2021-4104 also addresses CVE-2022-23302, CVE-2022-23305 and CVE-2022-23307
- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

Oracle Health Sciences Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Argus Analytics	Schema Creation (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Argus Insight	Schema Creation (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Argus Mart	Schema Creation (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Argus Safety	Schema Creation (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Clinical	Schema Creation (JDBC)	Oracle Net	Yes	8.3	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Health Sciences Clinical Development Analytics	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Health Sciences InForm CRF Submit	Installation and Configuration (JDBC, ODP for .NET)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Thesaurus Management System	Report Generation (JDBC)	Oracle Net	Yes	8.3	Network	High	None

Oracle HealthCare Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Health Sciences Information Manager	Health Policy Engine (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Healthcare Data Repository	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-2351	Oracle Healthcare Foundation	Installation (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 Healthcare Translational Research	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	None

Oracle Hospitality Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 I			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-2351	Oracle Hospitality OPERA 5	Integrations (JDBC, ODP for .NET)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Hospitality Suite8	Rest API (ODP for .NET)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-42340	Oracle Hospitality Cruise Shipboard Property Management System	Next-Gen SPMS (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	Non

Additional CVEs addressed are:

- The patch for CVE-2021-42340 also addresses CVE-2021-30640 and CVE-2021-33037.

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Hyperion. 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Hyperion Infrastructure Technology	Installation and Configuration (JDBC, OCCI, ODP for .NET)	Oracle Net	Yes	8.3	Network	High	None

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 (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2021-2351	Oracle iLearning	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	None	Rec

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Insurance Applications. 6 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-10683	Oracle Insurance Policy Administration J2EE	Architecture (dom4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2020-10683	Oracle Insurance Rules Palette	Architecture (dom4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2021-2351	Oracle Insurance Data Gateway	Security (JDBC)	HTTP	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Insurance Insbridge Rating and Underwriting	Framework Administrator IBFA (JDBC, ODP for .NET)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Insurance Policy Administration	Architecture (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-2351	Oracle Insurance Rules Palette	Architecture (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-22118	Oracle Insurance Rules Palette	Architecture (Spring Framework)	None	No	7.8	Local	Low	L

Oracle Java SE Risk Matrix

This Critical Patch Update contains 18 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-2021-22959	Oracle GraalVM Enterprise Edition	Node (Node.js)	HTTP	Yes	6.5	Network	Low	None	
CVE-2022-21349	Oracle Java SE, Oracle GraalVM Enterprise Edition	2D	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21291	Oracle Java SE, Oracle GraalVM Enterprise Edition	Hotspot	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21305	Oracle Java SE, Oracle GraalVM Enterprise Edition	Hotspot	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21277	Oracle Java SE, Oracle	ImageIO	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
	GraalVM Enterprise Edition								
CVE-2022-21360	Oracle Java SE, Oracle GraalVM Enterprise Edition	ImageIO	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21365	Oracle Java SE, Oracle GraalVM Enterprise Edition	ImageIO	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21366	Oracle Java SE, Oracle GraalVM Enterprise Edition	ImageIO	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21282	Oracle Java SE,	JAXP	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
	Oracle GraalVM Enterprise Edition								
CVE-2022-21296	Oracle Java SE, Oracle GraalVM Enterprise Edition	JAXP	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21299	Oracle Java SE, Oracle GraalVM Enterprise Edition	JAXP	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21271	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	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-2022-21283	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21293	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21294	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21340	Oracle Java SE, Oracle GraalVM Enterprise Edition	Libraries	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-2022-21341	Oracle Java SE, Oracle GraalVM Enterprise Edition	Serialization	Multiple	Yes	5.3	Network	Low	None	
CVE-2022-21248	Oracle Java SE, Oracle GraalVM Enterprise Edition	Serialization	Multiple	Yes	3.7	Network	High	None	

Notes:

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, 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-2021-22959 also addresses CVE-2021-22960.

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle JD Edwards. 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 R			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2021-23337	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech - Cloud (Lodash)	HTTP	No	7.2	Network	Low	Hig

Additional CVEs addressed are:

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

Oracle MySQL Risk Matrix

This Critical Patch Update contains 78 new security patches for Oracle MySQL. 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 VERSIOI		
					Base Score	Attack Vector	Attack Complex
CVE-2021-22946	MySQL Server	Server: Compiling (cURL)	Multiple	Yes	7.5	Network	Low
CVE-2021-3712	MySQL Connectors	Connector/C++ (OpenSSL)	MySQL Protocol	Yes	7.4	Network	High
CVE-2021-3712	MySQL Connectors	Connector/ODBC (OpenSSL)	MySQL Protocol	Yes	7.4	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21278	MySQL Server	Server: Optimizer	MySQL Protocol	No	7.1	Network	Low
CVE-2022-21351	MySQL Server	Server: Optimizer	MySQL Protocol	No	7.1	Network	Low
CVE-2022-21363	MySQL Connectors	Connector/J	MySQL Protocol	No	6.6	Network	High
CVE-2022-21358	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	6.5	Network	Low
CVE-2021-3634	MySQL Workbench	Workbench: libssh	MySQL Workbench	No	6.5	Network	Low
CVE-2022-21279	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21280	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21284	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21285	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-2022-21286	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21287	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21288	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21289	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21290	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21307	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-2022-21308	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21309	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21310	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21314	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21315	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21316	MySQL Cluster	Cluster: General	Multiple	No	6.3	Local	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21318	MySQL Cluster	Cluster: General	Multiple	No	6.3	Local	High
CVE-2022-21320	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21322	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21326	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21327	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21328	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-2022-21329	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21330	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21332	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21334	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21335	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21336	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21337	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-2022-21356	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21380	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2022-21352	MySQL Server	InnoDB	MySQL Protocol	No	5.9	Network	High
CVE-2022-21367	MySQL Server	Server: Compiling	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21301	MySQL Server	Server: DML	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21378	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2022-21302	MySQL Server	InnoDB	MySQL Protocol	No	5.3	Network	High
CVE-2022-21254	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.3	Network	High
CVE-2022-21348	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21270	MySQL Server	Server: Federated	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21256	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21379	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21362	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21374	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21253	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21264	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21297	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21339	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21342	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21370	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21304	MySQL Server	Server: Parser	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21344	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low
CVE-2022-21303	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21368	MySQL Server	Server: Components Services	MySQL Protocol	No	4.7	Network	Low
CVE-2022-21245	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.3	Network	Low
CVE-2022-21265	MySQL Server	Server: Optimizer	MySQL Protocol	No	3.8	Network	Low
CVE-2022-21311	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21312	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21313	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21317	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21319	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-2022-21321	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21323	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21324	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21325	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21331	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIOI		
					Base Score	Attack Vector	Attack Complex
CVE-2022-21333	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21355	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21357	MySQL Cluster	Cluster: General	Multiple	No	2.9	Adjacent Network	High
CVE-2022-21249	MySQL Server	Server: DDL	MySQL Protocol	No	2.7	Network	Low
CVE-2022-21372	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	2.7	Network	Low

Additional CVEs addressed are:

- The patch for CVE-2021-22946 also addresses CVE-2021-22947.
- The patch for CVE-2021-3712 also addresses CVE-2021-3711.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 13 new security patches for Oracle PeopleSoft. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-22931	PeopleSoft Enterprise PeopleTools	Elastic Search (Node.js)	HTTP	Yes	9.8	Network	Low	None
CVE-2021-2351	PeopleSoft Enterprise PeopleTools	Change Impact Analyzer (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2022-21300	PeopleSoft Enterprise CS SA Integration Pack	Snapshot Integration	HTTP	Yes	7.5	Network	Low	None
CVE-2021-37137	PeopleSoft Enterprise PeopleTools	Elastic Search (Netty)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-22946	PeopleSoft Enterprise PeopleTools	File Processing (cURL)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-3712	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	Multiple	Yes	7.4	Network	High	None
CVE-2021-23337	PeopleSoft Enterprise PeopleTools	Elastic Search (Lodash)	HTTP	No	7.2	Network	Low	High
CVE-2022-21345	PeopleSoft Enterprise PeopleTools	Security	HTTP	No	6.5	Network	Low	Low
CVE-2022-21359	PeopleSoft Enterprise PeopleTools	Optimization Framework	HTTP	Yes	6.1	Network	Low	None
CVE-2022-21272	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	None
CVE-2022-21369	PeopleSoft Enterprise PeopleTools	Rich Text Editor	HTTP	Yes	6.1	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-37695	PeopleSoft Enterprise PeopleTools	Rich Text Editor (CKEditor)	HTTP	No	5.4	Network	Low	Low
CVE-2022-21364	PeopleSoft Enterprise PeopleTools	Weblogic	HTTP	Yes	5.3	Network	Low	None

Additional CVEs addressed are:

- The patch for CVE-2021-22931 also addresses CVE-2021-22939 and CVE-2021-22940.
- The patch for CVE-2021-22946 also addresses CVE-2021-22924, CVE-2021-22925, CVE-2021-22926 and CVE-2021-22947.
- The patch for CVE-2021-23337 also addresses CVE-2020-28500 and CVE-2020-8203.
- The patch for CVE-2021-3712 also addresses CVE-2021-3711.
- The patch for CVE-2021-37137 also addresses CVE-2021-37136.
- The patch for CVE-2021-37695 also addresses CVE-2021-32808 and CVE-2021-32809.

Oracle Policy Automation Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Policy Automation. 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Oracle Policy Automation	Determinations Engine (JDBC)	Oracle Net	Yes	8.3	Network	High	None

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 43 new security patches for Oracle Retail Applications. 34 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	I P
CVE-2020-13936	Oracle Retail Integration Bus	RIB Kernal (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	
CVE-2020-13936	Oracle Retail Order Broker	Order Broker Foundation (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	
CVE-2020-13936	Oracle Retail Service Backbone	RSB kernel (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	
CVE-2021-2351	Oracle Retail Analytics	Other (JDBC)	Oracle Net	Yes	8.3	Network	High	I
CVE-2021-2351	Oracle Retail Assortment Planning	Application Core (JDBC)	Oracle Net	Yes	8.3	Network	High	I
CVE-2021-2351	Oracle Retail Back Office	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	I
CVE-2021-2351	Oracle Retail Central Office	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	I
CVE-2021-2351	Oracle Retail Customer Insights	Other (JDBC)	Oracle Net	Yes	8.3	Network	High	I
CVE-2021-2351	Oracle Retail Extract Transform and Load	Mathematical Operators (JDBC)	Oracle Net	Yes	8.3	Network	High	I
CVE-2021-2351	Oracle Retail Financial Integration	PeopleSoft Integration Bugs (JDBC)	Oracle Net	Yes	8.3	Network	High	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-2351	Oracle Retail Integration Bus	RIB Kernal (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Merchandising System	Foundation (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Order Broker	System Administration (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Order Management System	Upgrade Install (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Point-of-Service	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Predictive Application Server	RPAS Server (OCCI)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Price Management	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Returns Management	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Service Backbone	RSB Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Oracle Retail Xstore Point of Service	Xenvironment (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-22118	Oracle Retail Customer Management and	Deal (Spring Framework)	None	No	7.8	Local	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Segmentation Foundation							
CVE-2021-4104	Oracle Retail Allocation	General (Apache Log4j)	HTTP	No	7.5	Network	High	
CVE-2021-23337	Oracle Retail Customer Management and Segmentation Foundation	Security (Lodash)	HTTP	No	7.2	Network	Low	
CVE-2021-44832	Oracle Retail Assortment Planning	Application Core (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-44832	Oracle Retail Fiscal Management	NF Issuing (Apache Log4j)	HTTP	No	6.6	Network	High	
CVE-2021-45105	Oracle Retail Back Office	Security (Apache Log4j)	HTTP	Yes	5.9	Network	High	I
CVE-2021-45105	Oracle Retail Central Office	Security (Apache Log4j)	HTTP	Yes	5.9	Network	High	I
CVE-2021-45105	Oracle Retail EFTLink	Installation (Apache Log4j)	HTTP	Yes	5.9	Network	High	I
CVE-2021-45105	Oracle Retail Integration Bus	RIB Kernal (Apache Log4j)	HTTP	Yes	5.9	Network	High	I
CVE-2021-45105	Oracle Retail Invoice Matching	Security (Apache Log4j)	HTTP	Yes	5.9	Network	High	I

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-45105	Oracle Retail Order Broker	System Administration (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-45105	Oracle Retail Order Management System	Upgrade Install (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-45105	Oracle Retail Point-of-Service	Administration (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-45105	Oracle Retail Predictive Application Server	RPAS Server (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-45105	Oracle Retail Price Management	Security (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-45105	Oracle Retail Returns Management	Security (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-45105	Oracle Retail Service Backbone	RSB Installation (Apache Log4j)	HTTP	Yes	5.9	Network	High	
CVE-2021-31812	Oracle Retail Customer Management and Segmentation Foundation	Security (Apache PDFbox)	None	No	5.5	Local	Low	
CVE-2021-29425	Oracle Retail Assortment Planning	Application Core (Apache Commons IO)	HTTP	Yes	4.8	Network	High	
CVE-2021-29425	Oracle Retail Integration	RIB Kernal (Apache	HTTP	Yes	4.8	Network	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Bus	Commons IO)						
CVE-2021-29425	Oracle Retail Order Broker	System Administration (Apache Commons IO)	HTTP	Yes	4.8	Network	High	
CVE-2021-29425	Oracle Retail Service Backbone	RSB Installation (Apache Commons IO)	HTTP	Yes	4.8	Network	High	
CVE-2021-29425	Oracle Retail Size Profile Optimization	Application Core (Apache Commons IO)	HTTP	Yes	4.8	Network	High	

Notes:

1. This patch also addresses vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers need not apply the patches/mitigations of Security Alert CVE-2021-44228 and CVE-2021-45046 for this product.

Additional CVEs addressed are:

- The patch for CVE-2021-23337 also addresses CVE-2020-28500.
- The patch for CVE-2021-31812 also addresses CVE-2021-31811.

Oracle Siebel CRM Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-2351	Siebel UI Framework	EAI (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-44832	Siebel UI Framework	Enterprise Cache (Apache Log4j)	HTTP	No	6.6	Network	High	High

Notes:

1. This patch also addresses vulnerabilities CVE-2021-44228 and CVE-2021-45046. Customers need not apply the patches/mitigations of Security Alert CVE-2021-44228 and CVE-2021-45046 for this product.

Additional CVEs addressed are:

- The patch for CVE-2021-44832 also addresses CVE-2021-45105.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 10 new security patches for Oracle Supply Chain. 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-2021-2351	Oracle Agile Engineering Data Management	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Agile PLM	Security (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Demantra Demand Management	Security (JDBC, OCCI)	Oracle Net	Yes	8.3	Network	High	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2021-2351	Oracle Product Lifecycle Analytics	Installation (JDBC)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2021-2351	Oracle Rapid Planning	Middle Tier (JDBC, OCCI)	Oracle Net	Yes	8.3	Network	High	Non
CVE-2020-25649	Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite	Installation Issues (jackson-databind)	HTTP	Yes	7.5	Network	Low	Non
CVE-2021-35043	Oracle Agile PLM	Security (AntiSamy)	HTTP	Yes	6.1	Network	Low	Non
CVE-2021-36374	Oracle Agile PLM	Security (Apache Ant)	None	No	5.5	Local	Low	Non
CVE-2020-17521	Oracle Agile PLM MCAD Connector	CAX Client (Apache Groovy)	None	No	5.5	Local	Low	Low
CVE-2021-33037	Oracle Agile PLM	Security (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	Non

Additional CVEs addressed are:

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

Oracle Support Tools Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-27568	OSS Support Tools	Diagnostic Assistant (json-smart)	HTTP	Yes	9.1	Network	Low	None	N
CVE-2021-2351	OSS Support Tools	Diagnostic Assistant (JDBC)	Oracle Net	Yes	8.3	Network	High	None	Re
CVE-2016-7103	OSS Support Tools	Diagnostic Assistant (jQuery UI)	HTTP	Yes	6.1	Network	Low	None	Re
CVE-2021-29425	OSS Support Tools	Diagnostic Assistant (Apache Commons IO)	HTTP	Yes	4.8	Network	High	None	N

Oracle Systems Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle Systems. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2021-3517	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	8.6	Network	Low	None
CVE-2021-2351	Oracle ZFS Storage Application Integration Engineering Software	Snap Management Utility (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2020-8285	Fujitsu M10-1, M10-	XCP Firmware	HTTP	Yes	7.5	Network	Low	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	4, M10-4S, M12-1, M12-2, M12-2S Servers	(cURL)						
CVE-2021-3326	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (glibc)	Multiple	Yes	7.5	Network	Low	None
CVE-2021-23840	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (OpenSSL)	TLS	Yes	7.5	Network	Low	None
CVE-2020-13817	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers	XCP Firmware (NTP)	NTP	Yes	7.4	Network	High	None
CVE-2021-43395	Oracle Solaris	Filesystem	None	No	6.5	Local	Low	Low
CVE-2022-21375	Oracle Solaris	Kernel	None	No	5.5	Local	Low	Low
CVE-2022-21271	Oracle Solaris	Libraries	Multiple	Yes	5.3	Network	Low	None
CVE-2022-21263	Oracle Solaris	Fault Management Architecture	None	No	4.8	Local	Low	Low
CVE-2022-21298	Oracle Solaris	Install	None	No	3.9	Local	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2020-8285 also addresses CVE-2020-8177 and CVE-2020-8284.
- The patch for CVE-2021-3517 also addresses CVE-2021-3516, CVE-2021-3541 and CVE-2021-36690.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 13 new security patches for Oracle Utilities Applications. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-14756	Oracle Utilities Framework	General (Oracle Coherence)	HTTP	Yes	9.8	Network	Low	None
CVE-2021-27568	Oracle Utilities Framework	Common (json-smart)	HTTP	Yes	9.1	Network	Low	None
CVE-2021-39139	Oracle Utilities Framework	General (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2020-13936	Oracle Utilities Testing Accelerator	Tools (Apache Velocity Engine)	HTTP	No	8.8	Network	Low	Low
CVE-2021-39139	Oracle Utilities Testing Accelerator	Tools (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2021-2351	Oracle Utilities Framework	General (JDBC)	HTTP	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 Utilities Testing Accelerator	Tools (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2021-22118	Oracle Utilities Testing Accelerator	Tools (Spring Framework)	None	No	7.8	Local	Low	Low
CVE-2021-36090	Oracle Utilities Testing Accelerator	Tools (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-4104	Oracle Utilities Testing Accelerator	Tools (Apache Log4j)	HTTP	No	7.5	Network	High	Low
CVE-2021-36374	Oracle Utilities Testing Accelerator	Tools (Apache Ant)	None	No	5.5	Local	Low	None
CVE-2021-33037	Oracle Utilities Testing Accelerator	Tools (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	None
CVE-2021-29425	Oracle Utilities Testing Accelerator	Tools (Apache Commons IO)	HTTP	Yes	4.8	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2020-14756 also addresses CVE-2020-14642, CVE-2021-2277, CVE-2021-2344, CVE-2021-2371 and CVE-2021-2428.
- The patch for CVE-2021-27568 also addresses CVE-2021-31684.
- 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-2021-39139 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.

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Virtualization. Neither of these vulnerabilities may be remotely exploitable without authentication, i.e., neither may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2022-21394	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	N
CVE-2022-21295	Oracle VM VirtualBox	Core	None	No	3.8	Local	Low	Low	N

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