Oracle Critical Patch Update Advisory - October 2021

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third-party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to "Critical Patch Updates, Security Alerts and Bulletins" for information about Oracle Security advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update security patches without delay.

This Critical Patch Update contains 419 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 October 2021 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

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

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

Affected Products and Versions	Patch Availability Document
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0	Enterprise Manager
Enterprise Manager for Oracle Database, version 13.4.0.0	Enterprise Manager

Affected Products and Versions	Patch Availability Document
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
Essbase Administration Services, versions prior to 11.1.2.4.046, prior to 21.3,	Database
Hyperion Financial Management, versions 11.1.2.4, 11.2.6.0	Fusion Middleware
Hyperion Financial Reporting, versions 11.1.2.4, 11.2.6.0	Fusion Middleware
Hyperion Infrastructure Technology, version 11.2.6.0	Fusion Middleware
Hyperion Planning, versions 11.1.2.4, 11.2.6.0	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	Oracle Construction and Engineering Sui
JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.6.0	JD Edwards
JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.0	JD Edwards
JD Edwards World Security, version A9.4	JD Edwards
MySQL Client, versions 8.0.26 and prior	MySQL
MySQL Cluster, versions 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior, 8.0.26 and prior	MySQL
MySQL Connectors, versions 8.0.26 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.25 and prior	MySQL
MySQL Server, versions 5.7.35 and prior, 8.0.26 and prior	MySQL
MySQL Workbench, versions 8.0.26 and prior	MySQL
Oracle Agile PLM, versions 9.3.3, 9.3.6	Oracle Supply Chain Products
Oracle Application Express, versions prior to 21.1.0	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager
Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2	Oracle Supply Chain Products
Oracle Banking Cash Management, versions 14.2, 14.3, 14.5	Contact Support
Oracle Banking Corporate Lending Process Management, versions 14.2, 14.3, 14.5	Contact Support
Oracle Banking Credit Facilities Process Management, versions 14.2, 14.3, 14.5	Contact Support
Oracle Banking Enterprise Default Management, versions 2.10.0, 2.12.0	Oracle Banking Platform
Oracle Banking Extensibility Workbench, versions 14.2, 14.3, 14.5	Contact Support
Oracle Banking Platform, versions 2.6.2, 2.7.1, 2.9.0, 2.12.0	Oracle Banking Platform

Affected Products and Versions	Patch Availability Document
Oracle Banking Supply Chain Finance, versions 14.2, 14.3, 14.5	Contact Support
Oracle Banking Trade Finance Process Management, versions 14.2, 14.3, 14.5	Contact Support
Oracle Banking Virtual Account Management, versions 14.2, 14.3, 14.5	Contact Support
Oracle Business Activity Monitoring, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 5.9.0.0.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Commerce Guided Search, version 11.3.2	Oracle Commerce
Oracle Commerce Merchandising, version 11.3.2	Oracle Commerce
Oracle Communications Application Session Controller, version 3.9	Oracle Communications Application Sess Controller
Oracle Communications Billing and Revenue Management, versions 7.5.0.0.0, 12.0.0.3.0	Oracle Communications Billing and Reve Management
Oracle Communications BRM - Elastic Charging Engine, version 12.0.0.3	Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Calendar Server, version 8.0.0.6.0	Oracle Communications Calendar Server
Oracle Communications Cloud Native Core Network Repository Function, version 1.14.0	Oracle Communications Cloud Native Co Network Repository Function
Oracle Communications Cloud Native Core Policy, version 1.11.0	Communications Cloud Native Core Polic
Oracle Communications Control Plane Monitor, versions 3.4, 4.2, 4.3, 4.4	Oracle Communications Control Plane Monitor
Oracle Communications Converged Application Server - Service Controller, version 6.2	Oracle Communications Converged Application Server - Service Controller
Oracle Communications Design Studio, version 7.4.2	Oracle Communications Design Studio
Oracle Communications Diameter Signaling Router, versions 8.0.0.0-8.5.0.0	Oracle Communications Diameter Signal Router
Oracle Communications EAGLE	Oracle Communications EAGLE
Oracle Communications EAGLE FTP Table Base Retrieval, version 4.5	Oracle Communications EAGLE FTP Tabl Base Retrieval
Oracle Communications EAGLE LNP Application Processor, versions 46.7, 46.8, 46.9	Oracle Communications EAGLE LNP Application Processor
Oracle Communications Element Manager, versions 8.2.0.0-8.2.4.0	Oracle Communications Element Manag

Affected Products and Versions	Patch Availability Document
Oracle Communications Fraud Monitor, versions 3.4-4.4	Oracle Communications Fraud Monitor
Oracle Communications Interactive Session Recorder, version 6.4	Oracle Communications Interactive Sessi Recorder
Oracle Communications LSMS, versions 13.1-13.4	Oracle Communications LSMS
Oracle Communications Messaging Server, version 8.1	Oracle Communications Messaging Serv
Oracle Communications MetaSolv Solution, version 6.3.1	Oracle Communications MetaSolv Soluti
Oracle Communications Offline Mediation Controller, version 12.0.0.3.0	Oracle Communications Offline Mediatio Controller
Oracle Communications Operations Monitor, versions 3.4, 4.2, 4.3, 4.4	Oracle Communications Operations Mon
Oracle Communications Policy Management, version 12.5.0	Oracle Communications Policy Managem
Oracle Communications Pricing Design Center, version 12.0.0.3.0	Oracle Communications Pricing Design Center
Oracle Communications Services Gatekeeper, version 7.0	Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller, versions 8.4, 9.0	Oracle Communications Session Border Controller
Oracle Communications Session Report Manager, versions 8.0.0.0-8.2.5.0	Oracle Communications Session Report Manager
Oracle Communications Session Route Manager, versions 8.0.0.0-8.2.5.0	Oracle Communications Session Route Manager
Oracle Data Integrator, version 12.2.1.4.0	Fusion Middleware
Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 19c, 21c	Database
Oracle Documaker, versions 12.6.0-12.6.4	Oracle Insurance Applications
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10	Oracle E-Business Suite
Oracle Enterprise Communications Broker, versions 3.2, 3.3	Oracle Enterprise Communications Broke
Oracle Enterprise Repository, version 11.1.1.7.0	Fusion Middleware
Oracle Enterprise Telephony Fraud Monitor, versions 3.4, 4.2, 4.3, 4.4	Oracle Enterprise Telephony Fraud Monit
Oracle Ethernet Switch ES2-64, Oracle Ethernet Switch ES2-72, version 2.0.0.14	Systems
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.1	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Enterprise Case Management, versions 8.0.7.2.0, 8.0.8.1.0	Oracle Financial Services Enterprise Case Management

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Model Management and Governance, versions 8.0.8.0.0-8.1.0.0.0	Oracle Financial Services Model Management and Governance
Oracle FLEXCUBE Core Banking, versions 11.7, 11.8, 11.9, 11.10	Contact Support
Oracle Global Lifecycle Management OPatch	Global Lifecycle Management
Oracle GoldenGate, versions prior to 19.1.0.0.0.210420	Database
Oracle GoldenGate Application Adapters, version 19.1.0.0.0	Fusion Middleware
Oracle GraalVM Enterprise Edition, versions 20.3.3, 21.2.0	Java SE
Oracle Graph Server and Client, versions prior to 21.3.0	Database
Oracle Health Sciences Central Coding, versions 6.2.0, 6.3.0	Health Sciences
Oracle Health Sciences InForm, version 6.3.0	Health Sciences
Oracle Healthcare Data Repository, versions 7.0.2, 8.1.0	Health Sciences
Oracle Healthcare Foundation, versions 7.3, 8.0, 8.1	Health Sciences
Oracle Hospitality Cruise Shipboard Property Management System, version 20.1.0	Oracle Hospitality Cruise Shipboard Prop Management System
Oracle HTTP Server, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Insurance Calculation Engine, versions 11.0.0-11.3.1	Oracle Insurance Applications
Oracle Insurance Policy Administration, versions 11.0.0-11.3.1	Oracle Insurance Applications
Oracle Java SE, versions 7u311, 8u301, 11.0.12, 17	Java SE
Oracle NoSQL Database	NoSQL Database
Oracle Outside In Technology, version 8.5.5	Fusion Middleware
Oracle Real User Experience Insight, versions 13.4.1.0, 13.5.1.0	Enterprise Manager
Oracle Real-Time Decision Server, versions 3.2.0.0, 11.1.1.9.0	Fusion Middleware
Oracle REST Data Services, versions prior to 21.3	Database
Oracle Retail Advanced Inventory Planning, versions 14.1, 15.0, 16.0	Retail Applications
Oracle Retail Assortment Planning, version 16.0	Retail Applications
Oracle Retail Back Office, versions 14.0, 14.1	Retail Applications
Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Central Office, versions 14.0, 14.1	Retail Applications

Affected Products and Versions	Patch Availability Document
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0	Retail Applications
Oracle Retail Extract Transform and Load, version 13.2.8	Retail Applications
Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.4.0, 16.0.3.0	Retail Applications
Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.4.0, 16.0.3.0, 19.0.1.0	Retail Applications
Oracle Retail Merchandising System, versions 15.0.3, 19.0.1	Retail Applications
Oracle Retail Point-of-Service, versions 14.0, 14.1	Retail Applications
Oracle Retail Predictive Application Server, versions 14.1.3, 15.0.3, 16.0.3	Retail Applications
Oracle Retail Returns Management, versions 14.0, 14.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.4.0, 16.0.3.0, 19.0.1.0	Retail Applications
Oracle Retail Store Inventory Management, versions 14.1, 15.0, 16.0	Retail Applications
Oracle Secure Backup, versions prior to 18.1.0.1.0	Oracle Secure Backup
Oracle Secure Global Desktop, version 5.6	Virtualization
Oracle Solaris, version 11	Systems
Oracle Spatial Studio	Database
Oracle SQL Developer	Database
Oracle Transportation Management, version 6.4.3	Oracle Supply Chain Products
Oracle Utilities Framework, versions 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 6.1.28	Virtualization
Oracle WebCenter Portal, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
PeopleSoft Enterprise CC Common Application Objects, version 9.2	PeopleSoft
PeopleSoft Enterprise CS Academic Advisement, version 9.2	PeopleSoft
PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2	PeopleSoft

Affected Products and Versions	Patch Availability Document
PeopleSoft Enterprise CS SA Integration Pack, versions 9.0, 9.2	PeopleSoft
PeopleSoft Enterprise CS Student Records, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.59	PeopleSoft
PeopleSoft Enterprise SCM, version 9.2	PeopleSoft
Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.12, 19.12.0-19.12.11, 20.12.0-20.12.7	Oracle Construction and Engineering Sui
Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12	Oracle Construction and Engineering Sui
Siebel Applications, versions 21.9 and prior	Siebel
Tekelec Platform Distribution, versions 7.4.0-7.7.1	Tekelec Platform Distribution
Tekelec Virtual Operating Environment, versions 3.4.0-3.7.1	Tekelec Virtual Operating Environment

Note:

- Vulnerabilities affecting either Oracle Database or Oracle Fusion Middleware may affect Oracle Fusion Applications, so Oracle customers should refer to Oracle Fusion Applications Critical Patch Update Knowledge Document, My Oracle Support Note 1967316.1 for information on patches to be applied to Fusion Application environments.
- Vulnerabilities affecting Oracle Solaris may affect Oracle ZFSSA so Oracle customers should refer to the Oracle and Sun Systems Product Suite Critical Patch Update Knowledge Document, My Oracle Support Note 2160904.1 for information on minimum revisions of security patches required to resolve ZFSSA issues published in Critical Patch Updates and Solaris Third Party bulletins.
- Solaris Third Party Bulletins are used to announce security patches for third party software distributed with Oracle Solaris. Solaris 10 customers should refer to the latest patch-sets which contain critical security fixes and detailed in Systems Patch Availability Document. Please see Reference Index of CVE IDs and Solaris Patches (My Oracle Support Note 1448883.1) for more information.
- Users running Java SE with a browser can download the latest release from https://java.com. Users on the Windows and Mac OS X platforms can also use automatic updates to get the latest release.

Risk Matrix Content

Risk matrices list only security vulnerabilities that are newly addressed by the patches associated with this advisory. Risk matrices for previous security patches can be found in previous Critical Patch Update advisories and Alerts. An English text version of the risk matrices provided in this document is here.

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. Each vulnerability is identified by a CVE# which is its unique identifier. A vulnerability that affects multiple products will appear with the same CVE# in all risk matrices. A CVE# shown in *italics* indicates that this vulnerability impacts a different product, but also has impact on the product where the italicized CVE# is listed.

Security vulnerabilities are scored using CVSS version 3.1 (see Oracle CVSS Scoring for an explanation of how Oracle applies CVSS version 3.1).

Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update. Oracle does not disclose detailed information about this security analysis to customers, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see Oracle vulnerability disclosure policies.

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

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply Critical Patch Update security patches as soon as possible. Until you apply the Critical Patch Update patches, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

Oracle strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about

products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Critical Patch Update Supported Products and Versions

Patches released through the Critical Patch Update program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the Lifetime Support Policy. Oracle recommends that customers plan product upgrades to ensure that patches released through the Critical Patch Update program are available for the versions they are currently running.

Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, it is likely that earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

Database, Fusion Middleware, and Oracle Enterprise Manager products are patched in accordance with the Software Error Correction Support Policy explained in My Oracle Support Note 209768.1. Please review the Technical Support Policies for further guidelines regarding support policies and phases of support.

Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Critical Patch Update to Oracle:

- 0xfoxone: CVE-2021-35572, CVE-2021-35573, CVE-2021-35574, CVE-2021-35656, CVE-2021-35657, CVE-2021-35658, CVE-2021-35661, CVE-2021-35662
- Andrej Simko of Accenture: CVE-2021-35580, CVE-2021-35581, CVE-2021-35582
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2021-35590, CVE-2021-35592, CVE-2021-35593, CVE-2021-35594, CVE-2021-35598, CVE-2021-35621
- Artem Smotrakov: CVE-2021-35603
- Asaf Greenholts of Bank Hapoalim: CVE-2021-35550
- Aveek Biswas of Salesforce.com: CVE-2021-27290, CVE-2021-32804
- Black Lantern Security LLC: CVE-2021-35665
- Chuck Hunley of sas.com: CVE-2021-35567
- DoHyun Lee (l33d0hyun) of VirtualBoBs: CVE-2021-35540
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2021-2332
- Emad Al-Mousa: CVE-2021-35576

- Girlelecta: CVE-2021-35659, CVE-2021-35660
- Guillaume Jacques of synacktiv: CVE-2021-35651, CVE-2021-35652, CVE-2021-35653, CVE-2021-35654, CVE-2021-35655
- Hongkun Chen of Alibaba: CVE-2021-2471
- Jie Liang of WingTecher Lab of Tsinghua University: CVE-2021-35641, CVE-2021-35642, CVE-2021-35643, CVE-2021-35644, CVE-2021-35645
- Jingzhou Fu of WingTecher Lab of Tsinghua University: CVE-2021-35641, CVE-2021-35642, CVE-2021-35643, CVE-2021-35644, CVE-2021-35645
- John Simpson of Trend Micro Security Research working with the Zero Day Initiative: CVE-2021-35611
- Kosong: CVE-2021-2461
- Lai Han of NSFocus Security Team: CVE-2021-35620
- Liboheng of Tophant Starlight laboratory: CVE-2021-35617
- Markus Loewe: CVE-2021-35561
- Matthias Kaiser of Apple Information Security: CVE-2021-2137
- Ofir Hamam: CVE-2021-2476, CVE-2021-35616
- Paul Barbé of synacktiv: CVE-2021-35651, CVE-2021-35652, CVE-2021-35653, CVE-2021-35654, CVE-2021-35655
- Qiguang Zhu: CVE-2021-35551
- Qiuhao Li: CVE-2021-2475
- Ryan Emmons: CVE-2021-35538
- Sven Woynoski of it.sec GmbH: CVE-2021-2414, CVE-2021-2416
- Théo Louis-Tisserand of synacktiv: CVE-2021-35651, CVE-2021-35652, CVE-2021-35653, CVE-2021-35654, CVE-2021-35655
- Tristen Hayfield of Cisco: CVE-2021-35565
- Victor Rodriguez: CVE-2021-35595
- Xu Yuanzhen of Alibaba Cloud Security Team: CVE-2021-2471
- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2021-35557, CVE-2021-35558, CVE-2021-35634, CVE-2021-35641, CVE-2021-35642, CVE-2021-35643, CVE-2021-35644, CVE-2021-35645
- Yi Ren of Alibaba: CVE-2021-35542
- Zhiyong Wu of WingTecher Lab of Tsinghua University: CVE-2021-35641, CVE-2021-35642, CVE-2021-35643, CVE-2021-35644, CVE-2021-35645

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:

- Alexander Kornbrust of Red Database Security [2 reports]
- Andrej Simko of Accenture
- Emad Al-Mousa
- Fabian Meumertzheim of Code Intelligence
- Hinemos Development Team, NTT DATA INTELLILINK Corporation working with Red Hat
- Juho Nurminen of Mattermost
- Masafumi Miura of Red Hat
- Paul Fiterau Brostean of Uppsala University [3 reports]
- Yoshikazu Nojima of Red Hat

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:

- Adarsh VS Mannarakkal
- Ali Alzahrani
- Anil Bhatt
- Aravindha Hariharan
- Black Lantern Security LLC [8 reports]
- Brahim Ait Boufakri
- Dara Greaney
- Gaurang Maheta of gaurang maheta

- Gil Hoffer
- H01 from FPT Software Cybersecurity Assurance Service
- Jebarson Immanuel
- Khalid matar Alharthi
- Lidor Ben Shitrit from Orca Security
- Mahad Ali
- Maxime Bonillo
- Nic Palmer (Optimus Crime)
- Omri Litvak
- Osama Mohammed
- PhishLabs Security Operations
- Priyanshu Kumawat
- PwnWiki Administrator of PwnWiki
- Sergiy Kornienko
- Seth Duda of SquareWorks Consulting
- Shuvam Adhikari
- Vaishnav Pardhi
- Vismit Sudhir Rakhecha (Druk) [2 reports]

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:

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

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - October 2021 Documentation Map
- Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions
- Risk Matrix Definitions

- Use of Common Vulnerability Scoring System (CVSS) by Oracle
- English text version of the risk matrices
- CVRF XML version of the risk matrices
- Map of CVE to Advisory/Alert
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2022-January-18	Rev 3. Updated the essbase affected versions
2021-October-28	Rev 2. Changed the product of CVE-2018-20843 from Oracle WebLogic Server Proxy Plu In to Oracle HTTP Server and added 5.9.0.0.0 to affected versions of Oracle Business Intelligence Enterprise Edition.
2021-October-19	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

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

- 9 new security patches for Oracle Database Products
- 5 new security patches for Oracle Essbase
- No new security patches for Oracle Global Lifecycle Management, but third party patches are provided
- 1 new security patch for Oracle GoldenGate
- 1 new security patch for Oracle Graph Server and Client
- No new security patches for Oracle NoSQL Database, but third party patches are provided
- 1 new security patch for Oracle REST Data Services
- 1 new security patch for Oracle Secure Backup
- No new security patches for Oracle Spatial Studio, but third party patches are provided
- No new security patches for Oracle SQL Developer, but third party patches are provided

Oracle Database Server Risk Matrix

This Critical Patch Update contains 9 new security patches plus additional third party patches noted below for Oracle Database Products. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-35599	Zero Downtime DB Migration to Cloud	Local Logon	Local Logon	No	8.2	Local	Low	High	
CVE-2021-25122	Oracle Database Enterprise Edition (Apache Tomcat)	None	HTTP	Yes	7.5	Network	Low	None	
CVE-2021-35619	Java VM	Create Procedure	Oracle Net	No	7.1	Network	High	Low	F
CVE-2021-2332	Oracle LogMiner	DBA	Oracle Net	No	6.7	Network	Low	High	
CVE-2021-35551	RDBMS Security	DBA	Oracle Net	No	5.5	Network	Low	High	
CVE-2021-35557	Core RDBMS	Create Table	Oracle Net	No	4.3	Network	Low	Low	
CVE-2021-35558	Core RDBMS	Create Table	Oracle Net	No	4.3	Network	Low	Low	
CVE-2021-26272	Oracle Application Express (CKEditor)	None	HTTP	Yes	4.3	Network	Low	None	F
CVE-2021-35576	Oracle Database Enterprise Edition	Local Logon	Oracle Net	No	2.7	Network	Low	High	

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	
	Unified Audit								

Additional CVEs addressed are:

- The patch for CVE-2021-25122 also addresses CVE-2020-9484 and CVE-2021-25329.
- The patch for CVE-2021-26272 also addresses CVE-2021-26271.

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

- Autonomous Health Framework (Apache Commons IO): CVE-2021-29425.
- GraalVM Multilingual Engine: CVE-2021-29921, CVE-2020-28928, CVE-2021-2341, CVE-2021-2369, CVE-2021-2388 and CVE-2021-2432.
- Oracle Spatial and Graph - GeoRaster (OpenJPEG): CVE-2020-27824.

Oracle Essbase Risk Matrix

This Critical Patch Update contains 5 new security patches 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 VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2021-35652	Essbase Administration Services	EAS Console	HTTP	Yes	10.0	Network	Low	No
CVE-2021-35651	Essbase Administration Services	EAS Console	HTTP	No	8.5	Network	Low	Lo
CVE-2021-35653	Essbase Administration	EAS Console	HTTP	No	7.7	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
	Services							
CVE-2021-35654	Essbase Administration Services	EAS Console	HTTP	Yes	7.5	Network	Low	No
CVE-2021-35655	Essbase Administration Services	EAS Console	HTTP	Yes	5.3	Network	Low	No

Oracle Global Lifecycle Management Risk Matrix

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

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

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

- Oracle Global Lifecycle Management OPatch
  - Patch Installer (Apache Commons Compress): CVE-2021-36090, CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.
  - Patch Installer (jackson-databind): CVE-2020-25649.

Oracle GoldenGate Risk Matrix

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

Additional CVEs addressed are:

- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739.

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

- Oracle GoldenGate
  - General (Apache Batik): CVE-2020-11987 and CVE-2019-17566.
  - Install (jQuery): CVE-2020-11023, CVE-2019-11358 and CVE-2020-11022.
  - Internal Framework (Google Guava): CVE-2018-10237 and CVE-2020-8908.

Oracle Graph Server and Client Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle Graph Server and Client. This vulnerability is 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-2021-25122	Oracle Graph Server	Packaging/install (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None

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

Additional CVEs addressed are:

- The patch for CVE-2021-25122 also addresses CVE-2021-25329.

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 (Guava): CVE-2020-8908.
  - Packaging/Install (Lodash): CVE-2021-23337 and CVE-2020-28500.
  - Packaging/Install (jackson-databind): CVE-2020-25649.

Oracle NoSQL Database Risk Matrix

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

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

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

- Oracle NoSQL Database
  - Administration (Go): CVE-2021-34558.
  - Administration (Netty): CVE-2021-21409.

Oracle REST Data Services Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2021-28165	Oracle REST Data Services	General (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low	None	N

Additional CVEs addressed are:

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

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

- Oracle REST Data Services
  - Infrastructure (Apache Batik): CVE-2020-11988, CVE-2019-17566 and CVE-2020-11987.

Oracle Secure Backup Risk Matrix

This Critical Patch Update contains 1 new security patch plus additional third party patches noted below for Oracle Secure Backup. 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	Us Inte
CVE-2021-3450	Oracle Secure	Oracle Secure	TLS	Yes	7.4	Network	High	None	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
	Backup	Backup (OpenSSL)							

Additional CVEs addressed are:

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

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

- Oracle Secure Backup
  - Generic (PHP): CVE-2021-21702, CVE-2020-7065 and CVE-2020-7071.

Oracle Spatial Studio Risk Matrix

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

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

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

- Oracle Spatial Studio
  - Install (Apache Commons IO): CVE-2021-29425.
  - Install (Apache Commons BeanUtils): CVE-2019-10086.

Oracle SQL Developer Risk Matrix

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

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

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

- SQL Developer Data Modeler
  - Infrastructure (Apache PDFBox): CVE-2021-27807.

Oracle Commerce Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Commerce. 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			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-37695	Oracle Commerce Guided Search	Content Acquisition System (CKEditor)	HTTP	No	5.4	Network	Low	
CVE-2021-37695	Oracle Commerce Merchandising	Merchandising (CKEditor)	HTTP	No	5.4	Network	Low	

Additional CVEs addressed are:

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

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 19 new security patches for Oracle Communications Applications. 14 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2021-3177	Oracle Communications Pricing Design Center	Pricing (Python)	HTTP	Yes	9.8	Network	Low
CVE-2021-2351	Oracle Communications MetaSolv Solution	Reports (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-22118	Oracle Communications BRM - Elastic Charging Engine	Controller (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-36090	Oracle Communications Messaging Server	Message Store (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2021-30468	Oracle Communications Messaging Server	Security (Apache CXF)	HTTP	Yes	7.5	Network	Low
CVE-2020-25648	Oracle Communications Offline Mediation Controller	Storage & Reporting (NSS)	HTTPS	Yes	7.5	Network	Low
CVE-2019-10086	Oracle Communications	Billing Care (Apache	HTTP	Yes	7.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
	Billing and Revenue Management	Commons BeanUtils)					
CVE-2021-23337	Oracle Communications Design Studio	PSR Designer (Lodash)	HTTP	No	7.2	Network	Low
CVE-2020-6950	Oracle Communications Pricing Design Center	Services Manager (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low
CVE-2021-21409	Oracle Communications BRM - Elastic Charging Engine	OUI Installer (Netty)	HTTP	Yes	5.9	Network	High
CVE-2021-21409	Oracle Communications Design Studio	PSR Designer (Netty)	HTTP	Yes	5.9	Network	High
CVE-2021-21409	Oracle Communications Messaging Server	Multiplexor (Netty)	HTTP	Yes	5.9	Network	High
CVE-2020-17521	Oracle Communications BRM - Elastic Charging Engine	Orchestration (Apache Groovy)	None	No	5.5	Local	Low
CVE-2021-31812	Oracle Communications Messaging Server	Monitoring (Apache PDFBox)	None	No	5.5	Local	Low
CVE-2021-28657	Oracle Communications Messaging Server	Monitoring (Apache Tika)	None	No	5.5	Local	Low
CVE-2021-29425	Oracle Communications Calendar Server	Administration (Apache Commons IO)	HTTP	Yes	5.3	Network	Low
CVE-2021-29425	Oracle Communications Messaging Server	Message Store (Apache Commons IO)	HTTP	Yes	5.3	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2021-29425	Oracle Communications MetaSolv Solution	Reports (Apache Commons IO)	HTTP	Yes	5.3	Network	Low
CVE-2021-33037	Oracle Communications Pricing Design Center	Pricing (Apache Tomcat)	HTTP	Yes	5.3	Network	Low

Additional CVEs addressed are:

- The patch for CVE-2021-21409 also addresses CVE-2021-21290.
- The patch for CVE-2021-23337 also addresses CVE-2020-28500.
- The patch for CVE-2021-30468 also addresses CVE-2021-21290.
- The patch for CVE-2021-3177 also addresses CVE-2021-23336.
- The patch for CVE-2021-31812 also addresses CVE-2021-27807 and CVE-2021-27906.
- The patch for CVE-2021-33037 also addresses CVE-2021-30369 and CVE-2021-30640.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.

Oracle Communications Risk Matrix

This Critical Patch Update contains 71 new security patches plus additional third party patches noted below for Oracle Communications. 56 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 VERS		
					Base Score	Attack Vector	Attacl Compl
CVE-2021-21345	Oracle Communications Policy Management	Policy (XStream)	HTTP	No	9.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attack Comple
CVE-2021-21783	Oracle Communications Diameter Signaling Router	Platform (gSOAP)	HTTP	Yes	9.8	Network	Low
CVE-2017-9841	Oracle Communications Diameter Signaling Router	Signaling (PHP)	HTTP	Yes	9.8	Network	Low
CVE-2021-21783	Oracle Communications EAGLE LNP Application Processor	Patches (gSOAP)	HTTP	Yes	9.8	Network	Low
CVE-2020-11998	Oracle Communications Element Manager	Work orders (Apache ActiveMQ)	HTTP	Yes	9.8	Network	Low
CVE-2021-21783	Oracle Communications LSMS	Platform (gSOAP)	HTTP	Yes	9.8	Network	Low
CVE-2020-17530	Oracle Communications Policy Management	Enterprise Policy (Apache Struts2)	HTTP	Yes	9.8	Network	Low
CVE-2020-11998	Oracle Communications Session Report Manager	Reports (Apache ActiveMQ)	HTTP	Yes	9.8	Network	Low
CVE-2020-11998	Oracle Communications Session Route Manager	Route Manager (Apache ActiveMQ)	HTTP	Yes	9.8	Network	Low
CVE-2021-21783	Tekelec Virtual Operating Environment	Syscheck (gSOAP)	HTTP	Yes	9.8	Network	Low
CVE-2021-23017	Oracle Communications Control Plane Monitor	Infrastructure (nginx)	HTTP	Yes	9.4	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attacl Comple
CVE-2021-23017	Oracle Communications Fraud Monitor	Infrastructure (nginx)	HTTP	Yes	9.4	Network	Low
CVE-2021-23017	Oracle Communications Operations Monitor	Developer Infrastructure (nginx)	HTTP	Yes	9.4	Network	Low
CVE-2021-23017	Oracle Enterprise Telephony Fraud Monitor	Policies (nginx)	HTTP	Yes	9.4	Network	Low
CVE-2021-22112	Oracle Communications Element Manager	Work Orders (Spring Security)	HTTP	No	8.8	Network	Low
CVE-2020-10878	Oracle Communications Diameter Signaling Router	Platform (Perl)	HTTP	Yes	8.6	Network	Low
CVE-2020-10878	Oracle Communications LSMS	Platform (Perl)	HTTP	Yes	8.6	Network	Low
CVE-2020-10878	Tekelec Platform Distribution	Platform (Perl)	HTTP	Yes	8.6	Network	Low
CVE-2021-2351	Oracle Communications Application Session Controller	Signaling (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2461	Oracle Communications Interactive Session Recorder	Provision API	HTTP	Yes	8.3	Network	Low
CVE-2021-2351	Oracle Communications Session Report Manager	Reports (JDBC)	Oracle Net	Yes	8.3	Network	High
CVE-2021-2351	Oracle Communications	Route Manager (JDBC)	Oracle Net	Yes	8.3	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attack Comple
	Session Route Manager						
CVE-2020-10543	Oracle Communications EAGLE LNP Application Processor	Realtime db (Perl)	HTTP	Yes	8.2	Network	Low
CVE-2020-24750	Oracle Communications Element Manager	Security (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-24750	Oracle Communications Policy Management	Policy (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-24750	Oracle Communications Session Report Manager	Reports (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-28052	Oracle Communications Session Report Manager	Reports (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High
CVE-2020-24750	Oracle Communications Session Route Manager	Reports (jackson-databind)	HTTP	Yes	8.1	Network	High
CVE-2020-28052	Oracle Communications Session Route Manager	Route Manager (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High
CVE-2021-22118	Oracle Communications Element Manager	Work Orders (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22118	Oracle Communications Interactive Session Recorder	Monitor (Spring Framework)	None	No	7.8	Local	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attack Comple
CVE-2021-22118	Oracle Communications Session Report Manager	Reports (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22118	Oracle Communications Session Route Manager	Route Manager (Spring Framework)	None	No	7.8	Local	Low
CVE-2020-29661	Tekelec Platform Distribution	Storage Management (Kernel)	None	No	7.8	Local	Low
CVE-2021-3156	Tekelec Platform Distribution	Storage Management (Sudo)	None	No	7.8	Local	Low
CVE-2021-33560	Oracle Communications Cloud Native Core Network Repository Function	Measurements (libgcrypt)	HTTP	Yes	7.5	Network	Low
CVE-2020-11994	Oracle Communications Diameter Signaling Router	IDIH - Visualization (Apache Camel)	HTTP	Yes	7.5	Network	Low
CVE-2020-25649	Oracle Communications Diameter Signaling Router	IDIH - Visualization (jackson-databind)	HTTP	Yes	7.5	Network	Low
CVE-2021-36090	Oracle Communications Element Manager	Fault Management (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2021-30468	Oracle Communications Element Manager	Work Orders (Apache CXF)	HTTP	Yes	7.5	Network	Low
CVE-2021-28165	Oracle Communications	Work Orders (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attack Comple
	Element Manager						
CVE-2018-20034	Oracle Communications LSMS	NPA Agent (Flexnet)	HTTP	Yes	7.5	Network	Low
CVE-2020-5258	Oracle Communications Policy Management	Policy (dojo)	HTTP	Yes	7.5	Network	Low
CVE-2020-5398	Oracle Communications Policy Management	VNF Manager (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2021-28165	Oracle Communications Services Gatekeeper	Messaging Service (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2020-7226	Oracle Communications Services Gatekeeper	Payment (Cryptacular)	HTTP	Yes	7.5	Network	Low
CVE-2021-22696	Oracle Communications Session Report Manager	Reports (Apache CXF)	HTTP	Yes	7.5	Network	Low
CVE-2021-36090	Oracle Communications Session Report Manager	Reports (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low
CVE-2021-28165	Oracle Communications Session Report Manager	Reports (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2021-22696	Oracle Communications Session Route Manager	Route Manager (Apache CXF)	HTTP	Yes	7.5	Network	Low
CVE-2021-36090	Oracle Communications	Route Manager (Apache	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attack Comple
	Session Route Manager	Commons Compress)					
CVE-2021-28165	Oracle Communications Session Route Manager	Route Manager (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2021-25215	Tekelec Platform Distribution	Storage Management (BIND)	HTTP	Yes	7.5	Network	Low
CVE-2019-10086	Oracle Communications Policy Management	Policy (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low
CVE-2021-23337	Oracle Communications Cloud Native Core Policy	Signaling (Lodash)	HTTP	No	7.2	Network	Low
CVE-2021-23337	Oracle Communications Session Border Controller	Routing (Lodash)	HTTP	No	7.2	Network	Low
CVE-2021-23337	Oracle Enterprise Communications Broker	Routing (Lodash)	HTTP	No	7.2	Network	Low
CVE-2021-2414	Oracle Communications Session Border Controller	Routing	HTTP	No	6.8	Network	Low
CVE-2020-8622	Oracle Communications Diameter Signaling Router	Provisioning (BIND)	HTTP	No	6.5	Network	Low
CVE-2021-30640	Tekelec Platform Distribution	Console (Apache Tomcat)	HTTP	Yes	6.5	Network	High
CVE-2021-27906	Oracle Communications Session Report Manager	Reports (Apache PDFBox)	None	No	5.5	Local	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attacl Comple
CVE-2021-29425	Oracle Communications Application Session Controller	Signaling (Apache Commons IO)	HTTP	Yes	5.3	Network	Low
CVE-2021-29425	Oracle Communications Converged Application Server - Service Controller	Charging (Apache Commons IO)	HTTP	Yes	5.3	Network	Low
CVE-2021-33037	Oracle Communications Diameter Signaling Router	Platform (Apache Tomcat)	HTTP	Yes	5.3	Network	Low
CVE-2021-33037	Oracle Communications Policy Management	MediationServer (Apache Tomcat)	HTTP	Yes	5.3	Network	Low
CVE-2021-29425	Oracle Communications Session Report Manager	Reports (Apache Commons IO)	HTTP	Yes	5.3	Network	Low
CVE-2021-33037	Oracle Communications Session Report Manager	Reports (Apache Tomcat)	HTTP	Yes	5.3	Network	Low
CVE-2021-29425	Oracle Communications Session Route Manager	Route Manager (Apache Commons IO)	HTTP	Yes	5.3	Network	Low
CVE-2021-33037	Oracle Communications Session Route Manager	Route Manager (Apache Tomcat)	HTTP	Yes	5.3	Network	Low
CVE-2021-2416	Oracle Communications Session Border Controller	Routing	HTTP	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attack Comple
CVE-2020-9488	Oracle Communications EAGLE FTP Table Base Retrieval	Logging (Apache Log4j)	HTTP	Yes	3.7	Network	High

Additional CVEs addressed are:

- The patch for CVE-2017-9841 also addresses CVE-2020-7069 and CVE-2021-21702.
- The patch for CVE-2018-20034 also addresses CVE-2018-20031, CVE-2018-20032 and CVE-2018-20033.
- The patch for CVE-2020-10543 also addresses CVE-2020-10878.
- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723.
- The patch for CVE-2020-11998 also addresses CVE-2020-13947 and CVE-2021-26117.
- The patch for CVE-2020-17530 also addresses CVE-2019-0230 and CVE-2019-0233.
- The patch for CVE-2020-24750 also addresses CVE-2020-24616, CVE-2020-25649 and CVE-2020-36189.
- The patch for CVE-2020-25649 also addresses CVE-2020-14195, CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188 and CVE-2020-36189.
- The patch for CVE-2020-29661 also addresses CVE-2021-20265, CVE-2021-27364 and CVE-2021-27365.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.
- The patch for CVE-2020-9488 also addresses CVE-2017-5645.
- The patch for CVE-2021-21345 also addresses CVE-2020-26217, CVE-2021-21341, CVE-2021-21342, CVE-2021-21343, CVE-2021-21344, CVE-2021-21346, CVE-2021-21347, CVE-2021-21348, CVE-2021-21349, CVE-2021-21350, CVE-2021-21351 and CVE-2021-29505.
- The patch for CVE-2021-23337 also addresses CVE-2020-28500 and CVE-2020-8203.
- The patch for CVE-2021-27906 also addresses CVE-2021-27807.
- The patch for CVE-2021-28165 also addresses CVE-2020-27218, CVE-2021-28163 and CVE-2021-28164.
- The patch for CVE-2021-30468 also addresses CVE-2021-22696.
- The patch for CVE-2021-30640 also addresses CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797 and CVE-2021-33037.

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

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

- Oracle Communications EAGLE
  - Health Check (Perl): CVE-2020-10878, CVE-2020-10543 and CVE-2020-12723.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Construction and Engineering. 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			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-26691	Instantis EnterpriseTrack	Core (Apache HTTP Server)	HTTP	Yes	9.8	Network	Low	
CVE-2021-2351	Instantis EnterpriseTrack	Core (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-2351	Primavera Gateway	Admin (JDBC)	Oracle Net	Yes	8.3	Network	High	
CVE-2021-36090	Primavera Gateway	Admin (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-36090	Primavera Unifier	File Management (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	
CVE-2021-23337	Primavera Gateway	Admin (Lodash)	HTTP	No	7.2	Network	Low	
CVE-2021-23337	Primavera Unifier	Platform, UI (Lodash)	HTTP	No	7.2	Network	Low	
CVE-2021-36374	Primavera Gateway	Admin (Apache Ant)	None	No	5.5	Local	Low	
CVE-2021-28657	Primavera Unifier	Platform (Apache Tika)	None	No	5.5	Local	Low	
CVE-2021-36374	Primavera Unifier	System Configuration (Apache Ant)	None	No	5.5	Local	Low	
CVE-2021-33037	Instantis EnterpriseTrack	Core (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	
CVE-2021-29425	Primavera Gateway	Admin (Apache Commons IO)	HTTP	Yes	5.3	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2021-23337 also addresses CVE-2020-28500 and CVE-2020-8203.
- The patch for CVE-2021-26691 also addresses CVE-2019-17567, CVE-2020-13950, CVE-2020-35452, CVE-2021-26690, CVE-2021-30641 and CVE-2021-31618.
- 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.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 18 new security patches for Oracle E-Business Suite. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

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 October 2021 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Oracle E-Business Suite. For information on what patches need to be applied to your environments, refer to Oracle E-Business Suite Release 12 Critical Patch Update Knowledge Document (October 2021), My Oracle Support Note 2484000.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-35566	Oracle Applications Manager	Diagnostics	HTTP	No	8.1	Network	Low	
CVE-2021-2483	Oracle Content Manager	Content Item Manager	HTTP	No	8.1	Network	Low	
CVE-2021-35536	Oracle Deal Management	Miscellaneous	HTTP	No	8.1	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-35585	Oracle Incentive Compensation	User Interface	HTTP	No	8.1	Network	Low	
CVE-2021-35570	Oracle Mobile Field Service	Admin UI	HTTP	No	8.1	Network	Low	
CVE-2021-2484	Oracle Operations Intelligence	BIS Operations Intelligence	HTTP	No	8.1	Network	Low	
CVE-2021-2482	Oracle Payables	Invoice Approvals	HTTP	No	8.1	Network	Low	
CVE-2021-35563	Oracle Shipping Execution	Workflow Events	HTTP	No	8.1	Network	Low	
CVE-2021-2485	Oracle Trade Management	Quotes	HTTP	No	8.1	Network	Low	
CVE-2021-35562	Oracle Universal Work Queue	Work Provider Site Level Administration	HTTP	No	8.1	Network	Low	
CVE-2021-2474	Oracle Web Analytics	Admin	HTTP	No	8.1	Network	Low	
CVE-2021-35582	Oracle Applications Manager	View Reports	HTTP	No	6.5	Network	Low	
CVE-2021-35580	Oracle Applications Manager	View Reports	HTTP	Yes	6.1	Network	Low	N
CVE-2021-2477	Oracle Applications Framework	Session Management	HTTP	Yes	5.3	Network	Low	N
CVE-2021-35554	Oracle Trade Management	Quotes	HTTP	Yes	5.3	Network	Low	N
CVE-2021-35569	Oracle Applications Manager	Diagnostics	HTTP	No	4.9	Network	Low	I
CVE-2021-35581	Oracle Applications	View Reports	HTTP	Yes	4.7	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Manager							
CVE-2021-35611	Oracle Sales Offline	Offline Template	HTTP	No	4.3	Network	Low	

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Enterprise Manager. 5 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 October 2021 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Enterprise Manager. For information on what patches need to be applied to your environments, refer to Critical Patch Update October 2021 Patch Availability Document for Oracle Products, My Oracle Support Note 2796575.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-26691	Enterprise Manager Ops Center	Networking (Apache HTTP Server)	HTTP	Yes	9.8	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-2021-2137	Enterprise Manager Base Platform	Policy Framework	HTTP	No	8.8	Network	Low	Low
CVE-2021-29505	Enterprise Manager Ops Center	Guest Management (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2021-3518	Enterprise Manager Ops Center	Guest Management (libxml2)	HTTP	Yes	8.8	Network	Low	None
CVE-2021-3518	Oracle Real User Experience Insight	End User Experience Management (libxml2)	HTTP	Yes	8.8	Network	Low	None
CVE-2021-2351	Oracle Real User Experience Insight	End User Experience Management (JDBC)	Oracle Net	Yes	8.3	Network	High	None
CVE-2020-25649	Oracle Application Testing Suite	Load Testing for Web Apps (jackson-databind)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-20227	Enterprise Manager for Oracle Database	Provisioning (SQLite)	None	No	5.5	Local	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2020-25649 also addresses CVE-2020-24616, CVE-2020-24750, CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188 and CVE-2020-36189.
- The patch for CVE-2021-26691 also addresses CVE-2019-17567, CVE-2020-13950, CVE-2020-35452, CVE-2021-26690, CVE-2021-30641 and CVE-2021-31618.
- The patch for CVE-2021-3518 also addresses CVE-2019-20388, CVE-2020-24977, CVE-2020-7595, CVE-2021-3517 and CVE-2021-3537.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 44 new security patches for Oracle Financial Services Applications. 26 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-21345	Oracle Banking Virtual Account Management	Common Core (XStream)	HTTP	No	9.9	Network	Low	Lo
CVE-2020-5413	Oracle Banking Corporate Lending Process Management	Loans (Spring Integration)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-5413	Oracle Banking Credit Facilities Process Management	Credit Appraisal (Spring Integration)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-5413	Oracle Banking Supply Chain Finance	Account-Maintenance (Spring Integration)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-5413	Oracle Banking Virtual Account Management	Common Core (Spring Integration)	HTTP	Yes	9.8	Network	Low	No
CVE-2020-10683	Oracle FLEXCUBE Core Banking	Bills And Collections (dom4j)	HTTP	Yes	9.8	Network	Low	No
CVE-2021-29505	Oracle Banking	Accessibility (XStream)	HTTP	No	8.8	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Cash Management							
CVE-2021-29505	Oracle Banking Corporate Lending Process Management	Lending (XStream)	HTTP	No	8.8	Network	Low	Lo
CVE-2021-29505	Oracle Banking Credit Facilities Process Management	Credit Appraisal (XStream)	HTTP	No	8.8	Network	Low	Lo
CVE-2020-15824	Oracle Banking Extensibility Workbench	Web UI (Kotlin)	HTTP	No	8.8	Network	Low	Lo
CVE-2021-29505	Oracle Banking Supply Chain Finance	Account-Maintenance (XStream)	HTTP	No	8.8	Network	Low	Lo
CVE-2021-29505	Oracle Banking Trade Finance Process Management	Dashboard (XStream)	HTTP	No	8.8	Network	Low	Lo
CVE-2020-24750	Oracle Banking Corporate Lending Process Management	Lending (jackson-databind)	HTTP	Yes	8.1	Network	High	No
CVE-2020-28052	Oracle Banking Corporate Lending Process Management	Loans (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2020-24750	Oracle Banking Credit Facilities Process Management	Credit Appraisal (jackson-databind)	HTTP	Yes	8.1	Network	High	Nc
CVE-2020-28052	Oracle Banking Credit Facilities Process Management	Credit Appraisal (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	Nc
CVE-2020-28052	Oracle Banking Extensibility Workbench	Web UI (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	Nc
CVE-2020-24750	Oracle Banking Supply Chain Finance	Invoice (jackson-databind)	HTTP	Yes	8.1	Network	High	Nc
CVE-2020-28052	Oracle Banking Supply Chain Finance	Security (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	Nc
CVE-2020-28052	Oracle Banking Virtual Account Management	Common Core (Bouncy Castle Java Library)	HTTPS	Yes	8.1	Network	High	Nc
CVE-2020-25649	Oracle Banking Extensibility Workbench	Web UI (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-36090	Oracle Banking Platform	Product Accounting (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2020-25649	Oracle Banking Virtual	Account (jackson-databind)	HTTP	Yes	7.5	Network	Low	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Account Management							
CVE-2021-36090	Oracle Financial Services Analytical Applications Infrastructure	Rate Management (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2021-36090	Oracle Financial Services Enterprise Case Management	Web UI (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2019-0227	Oracle FLEXCUBE Core Banking	Bills And Collections (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Nc
CVE-2020-8203	Oracle Banking Virtual Account Management	Account (Lodash)	HTTP	Yes	7.4	Network	High	Nc
CVE-2021-23337	Oracle Banking Corporate Lending Process Management	Lending (Lodash)	HTTP	No	7.2	Network	Low	Hi
CVE-2021-23337	Oracle Banking Credit Facilities Process Management	Collateral Review (Lodash)	HTTP	No	7.2	Network	Low	Hi
CVE-2021-23337	Oracle Banking Extensibility Workbench	Banking (Lodash)	HTTP	No	7.2	Network	Low	Hi
CVE-2021-23337	Oracle Banking	Invoice (Lodash)	HTTP	No	7.2	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Supply Chain Finance							
CVE-2021-23337	Oracle Banking Trade Finance Process Management	Dashboard (Lodash)	HTTP	No	7.2	Network	Low	Hi
CVE-2020-6950	Oracle Banking Enterprise Default Management	Collections (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low	Nc
CVE-2020-6950	Oracle Banking Platform	Investment Account (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low	Nc
CVE-2021-26272	Oracle Financial Services Model Management and Governance	Model Governance (CKEditor)	HTTP	Yes	6.5	Network	Low	Nc
CVE-2021-21409	Oracle Banking Corporate Lending Process Management	Lending (Netty)	HTTP	Yes	5.9	Network	High	Nc
CVE-2021-21409	Oracle Banking Credit Facilities Process Management	Collateral Review (Netty)	HTTP	Yes	5.9	Network	High	Nc

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-21409	Oracle Banking Trade Finance Process Management	Dashboard (Netty)	HTTP	Yes	5.9	Network	High	Nc
CVE-2021-31812	Oracle Banking Corporate Lending Process Management	Lending (Apache PDFBox)	None	No	5.5	Local	Low	Nc
CVE-2021-31812	Oracle Banking Credit Facilities Process Management	Collateral Review (Apache PDFBox)	None	No	5.5	Local	Low	Nc
CVE-2021-31812	Oracle Banking Supply Chain Finance	Security (Apache PDFBox)	None	No	5.5	Local	Low	Nc
CVE-2021-27906	Oracle Banking Trade Finance Process Management	Dashboard (Apache PDFBox)	None	No	5.5	Local	Low	Nc
CVE-2021-27906	Oracle Banking Virtual Account Management	Common Core (Apache PDFBox)	None	No	5.5	Local	Low	Nc
CVE-2021-36374	Oracle Financial Services Analytical Applications Infrastructure	Publish Catalog (Apache Ant)	None	No	5.5	Local	Low	Nc

Additional CVEs addressed are:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2020-24750 also addresses CVE-2020-24616.
- The patch for CVE-2020-25649 also addresses CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188 and CVE-2020-36189.
- The patch for CVE-2020-28052 also addresses CVE-2020-26217.
- The patch for CVE-2021-21345 also addresses CVE-2021-21341, CVE-2021-21342, CVE-2021-21343, CVE-2021-21344, CVE-2021-21346, CVE-2021-21347, CVE-2021-21348, CVE-2021-21349, CVE-2021-21350 and CVE-2021-21351.
- The patch for CVE-2021-21409 also addresses CVE-2021-21290.
- The patch for CVE-2021-23337 also addresses CVE-2020-28500 and CVE-2020-8203.
- The patch for CVE-2021-26272 also addresses CVE-2021-26271 and CVE-2021-37695.
- The patch for CVE-2021-27906 also addresses CVE-2019-0228 and CVE-2021-27807.
- The patch for CVE-2021-29505 also addresses CVE-2020-26217 and CVE-2021-21345.
- The patch for CVE-2021-31812 also addresses CVE-2021-27906 and CVE-2021-31811.
- The patch for CVE-2021-36090 also addresses CVE-2021-35515, CVE-2021-35516 and CVE-2021-35517.
- The patch for CVE-2021-36374 also addresses CVE-2021-36373.

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 38 new security patches for Oracle Fusion Middleware. 30 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 October 2021 to the Oracle Database components of Oracle Fusion Middleware products. For information on what patches need to be applied to your environments, refer to Critical Patch Update October 2021 Patch Availability Document for Oracle Products, My Oracle Support Note 2796575.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-13990	Oracle WebCenter Sites	WebCenter Sites (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	None
CVE-2018-8088	Oracle WebLogic Server	Web Services (slf4j-ext)	HTTP	Yes	9.8	Network	Low	None
CVE-2021-35617	Oracle WebLogic Server	Coherence Container	IIOP	Yes	9.8	Network	Low	None
CVE-2021-29505	Oracle Business Activity Monitoring	General (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2021-29505	Oracle WebCenter Portal	Discussion Forums (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2021-29505	Oracle WebCenter Sites	WebCenter Sites (XStream)	HTTP	No	8.8	Network	Low	Low
CVE-2021-30468	Oracle Business Intelligence Enterprise Edition	Analytics Server (Apache CXF)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-25649	Oracle Data Integrator	Install, config, upgrade (jackson-databind)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35572	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35573	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35662	Oracle Outside In	Outside In Filters	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
	Technology							
CVE-2021-35661	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35574	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35660	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35659	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35658	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35657	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2021-35656	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.5	Network	Low	None
CVE-2020-5258	Oracle WebCenter Sites	WebCenter Sites (dojo)	HTTP	Yes	7.5	Network	Low	None
CVE-2020-7226	Oracle WebLogic Server	Core (Cryptacular)	SAML	Yes	7.5	Network	Low	None
CVE-2021-35620	Oracle WebLogic Server	Core	T3	Yes	7.5	Network	Low	None
CVE-2018-20843	Oracle HTTP Server	SSL Module (LibExpat)	HTTP	Yes	7.5	Network	Low	None
CVE-2021-26272	Oracle WebCenter Sites	WebCenter Sites (CKEditor)	HTTP	Yes	6.5	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
CVE-2020-11022	Oracle WebLogic Server	Web Services (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2021-23841	Oracle Business Intelligence Enterprise Edition	Analytics Server (OpenSSL)	HTTPS	Yes	5.9	Network	High	None
CVE-2021-35666	Oracle HTTP Server	OSSL Module	HTTPS	Yes	5.9	Network	High	None
CVE-2020-1971	Oracle HTTP Server	SSL Module (OpenSSL)	HTTPS	Yes	5.9	Network	High	None
CVE-2018-10237	Oracle WebLogic Server	Web Services (Google Guava)	HTTP	Yes	5.9	Network	High	None
CVE-2021-36374	Oracle Enterprise Repository	Security Subsystem - 12c (Apache Ant)	None	No	5.5	Local	Low	None
CVE-2021-36374	Oracle Real-Time Decision Server	Platform Installation (Apache Ant)	None	No	5.5	Local	Low	None
CVE-2021-27906	Oracle WebCenter Sites	WebCenter Sites (Apache PDFbox)	None	No	5.5	Local	Low	None
CVE-2019-12415	Oracle WebCenter Sites	WebCenter Sites (Apache POI)	None	No	5.5	Local	Low	Low
CVE-2019-12400	Oracle WebLogic Server	Web Services (Apache Santuario	None	No	5.5	Local	Low	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
		XML Security For Java)						
CVE-2021-29425	Oracle GoldenGate Application Adapters	Application Adapters (Apache Commons IO)	HTTP	Yes	5.3	Network	Low	None
CVE-2021-29425	Oracle Real-Time Decision Server	Decision Server (Apache Commons IO)	HTTP	Yes	5.3	Network	Low	None
CVE-2021-29425	Oracle WebLogic Server	Console (Apache Commons IO)	HTTP	Yes	5.3	Network	Low	None
CVE-2021-35552	Oracle WebLogic Server	Diagnostics	HTTP	Yes	5.3	Network	Low	None
CVE-2021-2480	Oracle HTTP Server	Web Listener	HTTP	Yes	3.7	Network	High	None

Notes:

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

Additional CVEs addressed are:

- The patch for CVE-2018-20843 also addresses CVE-2019-10082.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2020-11022 also addresses CVE-2019-11358 and CVE-2020-11023.
- The patch for CVE-2021-23841 also addresses CVE-2020-1971, CVE-2021-23839 and CVE-2021-23840.
- The patch for CVE-2021-26272 also addresses CVE-2021-26271.

- The patch for CVE-2021-27906 also addresses CVE-2021-27807.
- The patch for CVE-2021-30468 also addresses CVE-2020-13954 and CVE-2021-22696.
- The patch for CVE-2021-36374 also addresses CVE-2017-5645, CVE-2020-11979 and CVE-2021-36373.

Oracle Health Sciences Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-17195	Oracle Healthcare Data Repository	Install Utility (Nimbus JOSE+JWT)	HTTP	Yes	9.8	Network	Low	None
CVE-2021-22118	Oracle Healthcare Data Repository	Service Framework (Spring Framework)	None	No	7.8	Local	Low	Low
CVE-2020-11022	Oracle Health Sciences Central Coding	UI (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-11023	Oracle Health Sciences InForm	UI (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-17521	Oracle Healthcare Data Repository	Install Utility (Apache Groovy)	None	No	5.5	Local	Low	Low
CVE-2021-28657	Oracle Healthcare Foundation	Security (Apache Tika)	None	No	5.5	Local	Low	None

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Hospitality 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 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-11022	Oracle Hospitality Cruise Shipboard Property Management System	Next-Gen SPMS (jQuery)	HTTP	Yes	6.1	Network	Low	None

Oracle Hyperion Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-35665	Hyperion Financial Reporting	Repository	HTTP	Yes	6.1	Network	Low	No
CVE-2019-11358	Hyperion Planning	Hyperion Planning (jQuery)	HTTP	Yes	6.1	Network	Low	No
CVE-2021-27906	Hyperion Financial Reporting	Server Components (Apache PDFBox)	None	No	5.5	Local	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-29425	Hyperion Financial Management	Security (Apache Commons IO)	Multiple	Yes	5.3	Network	Low	No
CVE-2019-7317	Hyperion Infrastructure Technology	Installation and Configuration (libpng)	HTTP	Yes	5.3	Network	High	No
CVE-2020-27218	Hyperion Infrastructure Technology	Installation and Configuration (Eclipse Jetty)	HTTP	Yes	4.8	Network	High	No

Additional CVEs addressed are:

- The patch for CVE-2019-7317 also addresses CVE-2018-14550.
- The patch for CVE-2021-27906 also addresses CVE-2021-27807.

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 16 new security patches for Oracle Insurance Applications. 11 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2016-1000031	Oracle Documaker	Development tools (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2019-13990	Oracle Documaker	Development tools (Terracotta Quartz Scheduler)	HTTP	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-10683	Oracle Documaker	Development tools (dom4j)	HTTP	Yes	9.8	Network	Low	
CVE-2019-17195	Oracle Insurance Policy Administration	Architecture (Nimbus JOSE+JWT)	HTTP	Yes	9.8	Network	Low	
CVE-2020-11987	Oracle Insurance Policy Administration	Architecture (Apache Batik)	HTTP	Yes	8.2	Network	Low	
CVE-2020-36189	Oracle Documaker	Development tools (jackson-databind)	HTTP	Yes	8.1	Network	High	
CVE-2021-22118	Oracle Documaker	Development tools (Spring Framework)	None	No	7.8	Local	Low	
CVE-2021-22118	Oracle Insurance Policy Administration	Architecture (Spring Framework)	None	No	7.8	Local	Low	
CVE-2020-5258	Oracle Documaker	Development tools (dojo)	HTTP	Yes	7.5	Network	Low	
CVE-2020-5398	Oracle Insurance Calculation Engine	Architecture (Spring Framework)	HTTP	Yes	7.5	Network	High	
CVE-2019-10086	Oracle Documaker	Development tools (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2019-10086	Oracle Insurance Policy Administration	Architecture (Apache Commons BeanUtils)	HTTP	Yes	7.3	Network	Low	
CVE-2021-36374	Oracle Insurance Policy Administration	Architecture (Apache Ant)	None	No	5.5	Local	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2020-17521	Oracle Insurance Policy Administration	Architecture (Apache Groovy)	None	No	5.5	Local	Low
CVE-2021-37695	Oracle Documaker	Development tools (CKEditor)	HTTP	No	5.4	Network	Low
CVE-2021-29425	Oracle Documaker	Development tools (Apache Commons IO)	HTTP	Yes	5.3	Network	Low

Additional CVEs addressed are:

- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2020-36189 also addresses CVE-2020-25649, CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187 and CVE-2020-36188.
- The patch for CVE-2020-5398 also addresses CVE-2018-11039, CVE-2018-11040, CVE-2018-1257, CVE-2018-1258, CVE-2018-1270, CVE-2018-1271, CVE-2018-1272, CVE-2018-1275, CVE-2018-15756 and CVE-2020-5397.
- The patch for CVE-2021-36374 also addresses CVE-2021-36373.
- The patch for CVE-2021-37695 also addresses CVE-2021-32808 and CVE-2021-32809.

Oracle Java SE Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle Java SE. 13 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-3517	Java SE	JavaFX (libxml)	Multiple	Yes	8.6	Network	Low	None	
CVE-2021-35560	Java SE	Deployment	Multiple	Yes	7.5	Network	High	None	F
CVE-2021-27290	Oracle GraalVM Enterprise Edition	Node (Node.js)	Multiple	Yes	7.5	Network	Low	None	
CVE-2021-35567	Java SE, Oracle GraalVM Enterprise Edition	Libraries	Kerberos	No	6.8	Network	Low	Low	F
CVE-2021-35550	Java SE, Oracle GraalVM Enterprise Edition	JSSE	TLS	Yes	5.9	Network	High	None	
CVE-2021-3522	Java SE	JavaFX (GStreamer)	None	No	5.5	Local	Low	None	F
CVE-2021-35586	Java SE, Oracle GraalVM Enterprise Edition	ImageIO	Multiple	Yes	5.3	Network	Low	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-35564	Java SE, Oracle GraalVM Enterprise Edition	Keytool	Multiple	Yes	5.3	Network	Low	None	
CVE-2021-35556	Java SE, Oracle GraalVM Enterprise Edition	Swing	Multiple	Yes	5.3	Network	Low	None	
CVE-2021-35559	Java SE, Oracle GraalVM Enterprise Edition	Swing	Multiple	Yes	5.3	Network	Low	None	
CVE-2021-35561	Java SE, Oracle GraalVM Enterprise Edition	Utility	Multiple	Yes	5.3	Network	Low	None	
CVE-2021-35565	Java SE, Oracle GraalVM	JSSE	TLS	Yes	5.3	Network	Low	None	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
	Enterprise Edition								
CVE-2021-35578	Java SE, Oracle GraalVM Enterprise Edition	JSSE	TLS	Yes	5.3	Network	Low	None	
CVE-2021-35603	Java SE, Oracle GraalVM Enterprise Edition	JSSE	TLS	Yes	3.7	Network	High	None	
CVE-2021-35588	Java SE, Oracle GraalVM Enterprise Edition	Hotspot	Multiple	Yes	3.1	Network	High	None	F

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 does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

2. 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.

3. This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.

Additional CVEs addressed are:

- The patch for CVE-2021-27290 also addresses CVE-2019-16775, CVE-2021-22931, CVE-2021-22939, CVE-2021-22940, CVE-2021-32803, CVE-2021-32804, CVE-2021-37701, CVE-2021-37712, CVE-2021-37713, CVE-2021-39134 and CVE-2021-39135.
- The patch for CVE-2021-3517 also addresses CVE-2021-3537.

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle JD Edwards. 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			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-22884	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech (Node.js)	HTTP	Yes	7.5	Network	High	N
CVE-2020-25648	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure (NSS)	TLS	Yes	7.5	Network	Low	N
CVE-2020-8203	JD Edwards EnterpriseOne Tools	E1 Dev Platform Tech (Lodash)	HTTP	Yes	7.4	Network	High	N
CVE-2021-3450	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure (OpenSSL)	TLS	Yes	7.4	Network	High	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2021-3450	JD Edwards World Security	World Software Security (OpenSSL)	TLS	Yes	7.4	Network	High	N
CVE-2020-27216	JD Edwards EnterpriseOne Tools	Installation (Eclipse Jetty)	None	No	7.0	Local	High	L
CVE-2021-26272	JD Edwards EnterpriseOne Tools	Web Runtime (CKEditor)	HTTP	Yes	6.5	Network	Low	N
CVE-2020-17521	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator (Apache Groovy)	None	No	5.5	Local	Low	L
CVE-2021-20227	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure (SQLite)	None	No	5.5	Local	Low	L
CVE-2020-13956	JD Edwards EnterpriseOne Orchestrator	E1 IOT Orchestrator (Apache HttpClient)	HTTP	Yes	5.3	Network	Low	N
CVE-2020-13956	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics (Apache HttpClient)	HTTP	Yes	5.3	Network	Low	N

Additional CVEs addressed are:

- The patch for CVE-2021-22884 also addresses CVE-2020-8277, CVE-2021-22883 and CVE-2021-23840.
- The patch for CVE-2021-26272 also addresses CVE-2020-27193, CVE-2021-26271, CVE-2021-32808, CVE-2021-32809 and CVE-2021-37695.
- The patch for CVE-2021-3450 also addresses CVE-2021-23839, CVE-2021-23840, CVE-2021-23841 and CVE-2021-3449.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 66 new security patches for Oracle MySQL. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-22931	MySQL Cluster	Cluster: General (Node.js)	Multiple	Yes	9.8	Network	Low
CVE-2021-3711	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	Yes	9.8	Network	Low
CVE-2021-22112	MySQL Enterprise Monitor	Monitoring: General (Spring Security)	HTTPS	No	8.8	Network	Low
CVE-2021-3518	MySQL Workbench	MySQL Workbench (libxml2)	MySQL Workbench	Yes	8.8	Network	Low
CVE-2021-22118	MySQL Enterprise Monitor	Monitoring: General (Spring Framework)	None	No	7.8	Local	Low
CVE-2021-22926	MySQL Server	Server: Compiling (cURL)	Multiple	Yes	7.5	Network	Low
CVE-2021-36222	MySQL Server	Server: Compiling (Kerberos)	MySQL Protocol	Yes	7.5	Network	Low
CVE-2021-35583	MySQL Server	Server: Windows	MySQL Protocol	Yes	7.5	Network	Low
CVE-2021-3712	MySQL Workbench	MySQL Workbench (OpenSSL)	MySQL Workbench	Yes	7.4	Network	High
CVE-2021-35610	MySQL Server	Server: Optimizer	MySQL Protocol	No	7.1	Network	Low
CVE-2021-3712	MySQL Enterprise Monitor	Monitoring: General (OpenSSL)	None	No	6.7	Local	High
CVE-2021-35597	MySQL Client	C API	MySQL Protocol	No	6.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-35607	MySQL Server	Server: DML	MYSQL Protocol	No	6.5	Network	Low
CVE-2021-2481	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low
CVE-2021-35590	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2021-35592	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2021-35593	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2021-35594	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2021-35598	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High
CVE-2021-35621	MySQL Cluster	Cluster: General	Multiple	No	6.3	Adjacent Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-2471	MySQL Connectors	Connector/J	MySQL Protocol	No	5.9	Network	High
CVE-2021-35604	MySQL Server	InnoDB	MySQL Protocol	No	5.5	Network	Low
CVE-2021-35612	MySQL Server	Server: Optimizer	MySQL Protocol	No	5.5	Network	Low
CVE-2021-20227	MySQL Workbench	MySQL Workbench (SQLite)	None	No	5.5	Local	Low
CVE-2021-33037	MySQL Enterprise Monitor	Monitoring: General (Apache Tomcat)	Apache JServ Protocol (AJP)	Yes	5.3	Network	Low
CVE-2021-29425	MySQL Enterprise Monitor	Monitoring: General (Apache Commons IO)	HTTPS	Yes	5.3	Network	Low
CVE-2021-35608	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	5.3	Network	High
CVE-2021-35602	MySQL Server	Server: Options	MySQL Protocol	No	5.0	Network	High
CVE-2021-35577	MySQL Server	Server: Optimizer	MySQL Protcol	No	4.9	Network	Low
CVE-2021-2478	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2021-2479	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35537	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35591	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35596	MySQL Server	Server: Error Handling	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-35648	MySQL Server	Server: FTS	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35631	MySQL Server	Server: GIS	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35626	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35627	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35628	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35629	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35575	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35634	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35635	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35636	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35638	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35641	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35642	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35643	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35644	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35645	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35646	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35647	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2021-35630	MySQL Server	Server: Options	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35637	MySQL Server	Server: PS	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35546	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35622	MySQL Server	Server: Security: Encryption	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35624	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35639	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low
CVE-2021-35632	MySQL Server	Server: Data Dictionary	None	No	4.4	Local	Low
CVE-2021-35584	MySQL Cluster	Cluster: ndbcluster/plugin DDL	Multiple	No	4.3	Network	Low
CVE-2021-35613	MySQL Cluster	Cluster: General	Multiple	Yes	3.7	Network	High
CVE-2021-35640	MySQL Server	Server: DDL	MySQL Protocol	No	2.7	Network	Low
CVE-2021-35633	MySQL Server	Server: Logging	MySQL Protocol	No	2.7	Network	Low
CVE-2021-35625	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	2.7	Network	Low
CVE-2021-35623	MySQL Server	Server: Security: Roles	MySQL Protocol	No	2.7	Network	Low
CVE-2021-35618	MySQL Cluster	Cluster: General	Multiple	No	1.8	Adjacent Network	High

Additional CVEs addressed are:

- The patch for CVE-2021-22926 also addresses CVE-2021-22922, CVE-2021-22923, CVE-2021-22924, CVE-2021-22925, CVE-2021-22945, CVE-2021-22946 and CVE-2021-22947.
- The patch for CVE-2021-22931 also addresses CVE-2021-22939 and CVE-2021-22940.

- The patch for CVE-2021-3518 also addresses CVE-2019-20388, CVE-2020-24977, CVE-2020-7595, CVE-2021-3517 and CVE-2021-3537.
- The patch for CVE-2021-3711 also addresses CVE-2021-3712.
- The patch for CVE-2021-3712 also addresses CVE-2021-3711.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 17 new security patches for Oracle PeopleSoft. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2021-23926	PeopleSoft Enterprise PeopleTools	nVision (XMLBeans)	HTTP	Yes	9.1	Network	Low	No
CVE-2021-35543	PeopleSoft Enterprise CC Common Application Objects	Activity Guide Composer	HTTP	No	8.1	Network	Low	Lo
CVE-2021-36090	PeopleSoft Enterprise PeopleTools	Cloud Manager (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	No
CVE-2020-1967	PeopleSoft Enterprise PeopleTools	DPK (OpenSSL)	TLS	Yes	7.5	Network	Low	No
CVE-2021-35609	PeopleSoft Enterprise PeopleTools	SQR	HTTP	No	6.5	Network	Low	Lo
CVE-2021-28363	PeopleSoft Enterprise PeopleTools	Porting (urllib3)	HTTPS	Yes	6.5	Network	Low	No
CVE-2021-35595	PeopleSoft Enterprise	Business Interlink	HTTP	Yes	6.1	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
	PeopleTools							
CVE-2021-35568	PeopleSoft Enterprise PeopleTools	Rich Text Editor	HTTP	Yes	6.1	Network	Low	No
CVE-2021-35606	PeopleSoft Enterprise CS Campus Community	Notification Framework	HTTP	No	5.7	Adjacent Network	Low	Lo
CVE-2021-35601	PeopleSoft Enterprise CS SA Integration Pack	Students Administration	HTTP	No	5.7	Adjacent Network	Low	Lo
CVE-2021-27906	PeopleSoft Enterprise PeopleTools	Elastic Search (Apache PDFBox)	None	No	5.5	Local	Low	No
CVE-2019-12415	PeopleSoft Enterprise PeopleTools	nVision (Apache POI)	None	No	5.5	Local	Low	Lo
CVE-2021-35571	PeopleSoft Enterprise CS Academic Advisement	Advising Notes	HTTP	No	5.4	Network	Low	Lo
CVE-2021-35553	PeopleSoft Enterprise CS Student Records	Class Search	HTTP	No	5.4	Network	Low	Lo
CVE-2021-35541	PeopleSoft Enterprise SCM	Supplier Portal	HTTP	No	5.4	Network	Low	Lo
CVE-2021-29425	PeopleSoft Enterprise PeopleTools	Updates Change Assistant (Apache Commons IO)	HTTP	Yes	5.3	Network	Low	No
CVE-2020-13956	PeopleSoft Enterprise PeopleTools	Updates Change Assistant	HTTP	Yes	5.3	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Re
		(Apache HttpClient)						

Additional CVEs addressed are:

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

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 26 new security patches for Oracle Retail Applications. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-2351	Oracle Retail Store Inventory Management	SIM Integration (JDBC)	Oracle Net	Yes	8.3	Network	High	N
CVE-2021-22118	Oracle Retail Assortment Planning	Plan (Spring Framework)	None	No	7.8	Local	Low	L
CVE-2021-22118	Oracle Retail Merchandising System	Foundation (Spring Framework)	None	No	7.8	Local	Low	L
CVE-2021-22118	Oracle Retail Predictive Application Server	RPAS Fusion Client (Spring Framework)	None	No	7.8	Local	Low	L
CVE-2020-25649	Oracle Retail Customer Management and	Segment (jackson-databind)	HTTP	Yes	7.5	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	Segmentation Foundation							
CVE-2020-25649	Oracle Retail Merchandising System	Foundation (jackson-databind)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-6950	Oracle Retail Merchandising System	Foundation (Eclipse Mojarra)	HTTP	Yes	6.5	Network	Low	N
CVE-2020-1945	Oracle Retail Returns Management	Return Tickets (Apache Ant)	None	No	6.3	Local	High	L
CVE-2021-35043	Oracle Retail Back Office	Employee (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2021-35043	Oracle Retail Central Office	Transaction Tracker (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2021-35043	Oracle Retail Returns Management	Policy Evaluation (AntiSamy)	HTTP	Yes	6.1	Network	Low	N
CVE-2021-36374	Oracle Retail Advanced Inventory Planning	Operations & Maintenance (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Back Office	Employee (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Central Office	Transaction Tracker (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Extract Transform and Load	Mathematical Operators (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Financial Integration	EBS Integration Bugs (Apache Ant)	None	No	5.5	Local	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2021-36374	Oracle Retail Integration Bus	RIB Kernal (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Merchandising System	Foundation (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Point-of-Service	Pricing (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Predictive Application Server	RPAS Server (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Service Backbone	RSB Installation (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-36374	Oracle Retail Store Inventory Management	SIM Integration (Apache Ant)	None	No	5.5	Local	Low	N
CVE-2021-29425	Oracle Retail Customer Management and Segmentation Foundation	Segment (Apache Commons IO)	HTTP	Yes	5.3	Network	Low	N
CVE-2020-13956	Oracle Retail Customer Management and Segmentation Foundation	Segment (Apache HTTPClient)	HTTP	Yes	5.3	Network	Low	N
CVE-2020-8908	Oracle Retail Customer Management and Segmentation Foundation	Segment (Google Guava)	None	No	3.3	Local	Low	L

Additional CVEs addressed are:

- The patch for CVE-2020-25649 also addresses CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188 and CVE-2020-36189.
- The patch for CVE-2021-36374 also addresses CVE-2020-1945 and CVE-2021-36373.

Oracle Siebel CRM Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2021-28165	Siebel Core - Automation	Test Automation (Eclipse Jetty)	TLS	Yes	7.5	Network	Low	None
CVE-2021-25122	Siebel UI Framework	EAI (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None
CVE-2016-2183	Siebel UI Framework	EAI, SWSE (OpenSSL)	TLS	Yes	7.5	Network	Low	None
CVE-2020-9484	Siebel Apps - Marketing	Marketing (Apache Tomcat)	None	No	7.0	Local	High	Low
CVE-2021-26272	Siebel UI Framework	Open UI (CKEditor)	HTTP	Yes	6.5	Network	Low	None
CVE-2020-9488	Siebel Apps - Marketing	Marketing (Apache Log4j)	HTTP	Yes	3.7	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2021-26272 also addresses CVE-2021-26271.
- The patch for CVE-2021-28165 also addresses CVE-2021-28163 and CVE-2021-28164.

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle Supply Chain. 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			
					Base Score	Attack Vector	Attack Complex	
CVE-2021-28165	Oracle Autovue for Agile Product Lifecycle Management	Autovue Viewer Integration (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low	
CVE-2020-25649	Oracle Autovue for Agile Product Lifecycle Management	Autovue Viewer Integration (jackson-databind)	HTTP	Yes	7.5	Network	Low	
CVE-2020-17521	Oracle Agile PLM	Security (Apache Groovy)	None	No	5.5	Local	Low	
CVE-2021-35616	Oracle Transportation Management	UI Infrastructure	HTTP	No	5.4	Network	Low	
CVE-2021-2476	Oracle Transportation Management	Authentication	HTTP	Yes	5.3	Network	Low	

Additional CVEs addressed are:

- The patch for CVE-2020-25649 also addresses CVE-2020-10672, CVE-2020-10673, CVE-2020-10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-14060, CVE-2020-14061, CVE-2020-14062, CVE-2020-14195, CVE-2020-24616, CVE-2020-24750, CVE-2020-35490, CVE-2020-35491, CVE-2020-35728, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188, CVE-2020-36189, CVE-2020-9546, CVE-2020-9547 and CVE-2020-9548.
- The patch for CVE-2021-28165 also addresses CVE-2021-28163 and CVE-2021-28164.

Oracle Systems Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle Systems. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2021-26691	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	Yes	9.8	Network	Low	None	
CVE-2021-35539	Oracle Solaris	Filesystem	None	No	6.5	Local	Low	Low	
CVE-2021-35589	Oracle Solaris	Device drivers	None	No	6.0	Local	Low	High	
CVE-2021-35549	Oracle Solaris	Utility	None	No	3.9	Local	Low	Low	R
CVE-2020-1968	Oracle Ethernet Switch ES2-64, Oracle Ethernet Switch ES2-72	Firmware (OpenSSL)	HTTPS	Yes	3.7	Network	High	None	

Additional CVEs addressed are:

- The patch for CVE-2021-26691 also addresses CVE-2019-17567, CVE-2020-13950, CVE-2020-26116, CVE-2020-26137, CVE-2020-35452, CVE-2021-20227, CVE-2021-22207, CVE-2021-22222, CVE-2021-26690, CVE-2021-28957, CVE-2021-29921, CVE-2021-30641, CVE-2021-31618, CVE-2021-33503, CVE-2021-3426, CVE-2021-3520, CVE-2021-36222, CVE-2021-3711 and CVE-2021-3712.

Oracle Utilities Applications Risk Matrix

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

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2021-36374	Oracle Utilities Framework	General (Apache Ant)	None	No	5.5	Local	Low	None	R

Additional CVEs addressed are:

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

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Virtualization. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-35538	Oracle VM VirtualBox	Core	None	No	7.8	Local	Low	Low	
CVE-2021-35545	Oracle VM VirtualBox	Core	None	No	6.7	Local	Low	High	
CVE-2021-35540	Oracle VM VirtualBox	Core	None	No	5.5	Local	Low	Low	
CVE-2021-35649	Oracle Secure Global Desktop	Server	Multiple	No	5.4	Network	Low	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2021-33037	Oracle Secure Global Desktop	Core (Apache Tomcat)	HTTP	Yes	5.3	Network	Low	None	
CVE-2021-35650	Oracle Secure Global Desktop	Client	Multiple	No	4.6	Network	Low	Low	I
CVE-2021-35542	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	
CVE-2021-2475	Oracle VM VirtualBox	Core	None	No	4.4	Local	Low	High	

Notes:

1. This vulnerability does not apply to Windows systems.