

# Oracle Critical Patch Update Advisory - July 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 342 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at [July 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        |
|--|------------------------------------|
| <a href="#">Big Data Spatial and Graph, versions prior to 2.0, prior to 23.1</a> | <a href="#">Database</a>           |
| <a href="#">Enterprise Manager Base Platform, version 13.4.0.0</a>               | <a href="#">Enterprise Manager</a> |

| Affected Products and Versions  | Patch Availability Document             |
|---|---|
| Essbase, version 21.2   | Database                                |
| Essbase Analytic Provider Services, versions 11.1.2.4, 21.2   | Database                                |
| Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2400, prior to XCP3100 | Systems                                 |
| Hyperion Essbase Administration Services, versions 11.1.2.4, 21.2                                       | Database                                |
| Hyperion Financial Reporting, versions 11.1.2.4, 11.2.5.0   | Fusion Middleware                       |
| Hyperion Infrastructure Technology, versions 11.1.2.4, 11.2.5.0   | Fusion Middleware                       |
| Identity Manager, versions 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0                               | Fusion Middleware                       |
| Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3  | Oracle Construction and Engineering Sui |
| JD Edwards EnterpriseOne Orchestrator, versions 9.2.5.3 and prior                                       | JD Edwards                              |
| JD Edwards EnterpriseOne Tools, versions 9.2.5.3 and prior  | JD Edwards                              |
| MICROS Compact Workstation 3, version 310   | MICROS Compact Workstation              |
| MICROS ES400 Series, versions 400-410   | MICROS ES400 Series                     |
| MICROS Kitchen Display System Hardware, version 210   | MICROS Kitchen Display System Hardwa    |
| MICROS Workstation 5A, version 5A   | MICROS Workstation 5A                   |
| MICROS Workstation 6, versions 610-655  | MICROS Workstation                      |
| MySQL Cluster, versions 8.0.25 and prior  | MySQL                                   |
| MySQL Connectors, versions 8.0.23 and prior   | MySQL                                   |
| MySQL Enterprise Monitor, versions 8.0.23 and prior   | MySQL                                   |
| MySQL Server, versions 5.7.34 and prior, 8.0.25 and prior   | MySQL                                   |
| Oracle Access Manager, version 11.1.2.3.0   | Fusion Middleware                       |
| Oracle Agile Engineering Data Management, version 6.2.1.0   | Oracle Supply Chain Products            |
| Oracle Agile PLM, versions 9.3.3, 9.3.5, 9.3.6  | Oracle Supply Chain Products            |
| Oracle Application Express, versions prior to 21.1.0.0.4  | Database                                |
| Oracle Application Express (CKEditor), versions prior to 21.1.0.0.1                                     | Database                                |
| Oracle Application Express Application Builder (DOMPurify), versions prior to 21.1.0.0.1                | Database                                |
| Oracle Application Testing Suite, version 13.3.0.1  | Enterprise Manager                      |

| Affected Products and Versions   | Patch Availability Document   |
|--|---|
| Oracle BAM (Business Activity Monitoring), versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0                   | Fusion Middleware   |
| Oracle Banking Enterprise Default Management, versions 2.10.0, 2.12.0                                    | Oracle Banking Platform   |
| Oracle Banking Liquidity Management, versions 14.2, 14.3, 14.5   | Contact Support   |
| Oracle Banking Party Management, version 2.7.0   | Oracle Banking Platform   |
| Oracle Banking Platform, versions 2.4.0, 2.7.1, 2.9.0, 2.12.0  | Oracle Banking Platform   |
| Oracle Banking Treasury Management, version 14.4   | Contact Support   |
| Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0                              | Fusion Middleware   |
| Oracle Business Intelligence Enterprise Edition, version 12.2.1.4.0                                      | Fusion Middleware   |
| Oracle Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0                       | Fusion Middleware   |
| Oracle Commerce Guided Search, version 11.3.2  | Oracle Commerce   |
| Oracle Commerce Guided Search / Oracle Commerce Experience Manager, versions 11.3.1.5, 11.3.2            | Oracle Commerce   |
| Oracle Commerce Merchandising, versions 11.1.0, 11.2.0, 11.3.0-11.3.2                                    | Oracle Commerce   |
| Oracle Commerce Platform, versions 11.0.0, 11.1.0, 11.2.0, 11.3.0-11.3.2                                 | Oracle Commerce   |
| Oracle Commerce Service Center, versions 11.0.0, 11.1.0, 11.2.0, 11.3.0-11.3.2                           | Oracle Commerce   |
| Oracle Communications Application Session Controller, version 3.9  | Oracle Communications Application Session Controller                              |
| Oracle Communications Billing and Revenue Management, versions 7.5.0.23.0, 12.0.0.3.0                    | Oracle Communications Billing and Revenue Management                              |
| Oracle Communications BRM - Elastic Charging Engine, versions 11.3.0.9.0, 12.0.0.3.0                     | Oracle Communications BRM - Elastic Charging Engine                               |
| Oracle Communications Cloud Native Core Console, version 1.4.0   | Communications Cloud Native Core Console  |
| Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.4.0, 1.7.0 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment |
| Oracle Communications Cloud Native Core Network Slice Selection Function, version 1.2.1                  | Communications Cloud Native Core Network Slice Selection Function                 |

| Affected Products and Versions   | Patch Availability Document                                      |
|--|--|
| Oracle Communications Cloud Native Core Policy, versions 1.5.0, 1.9.0                                | Communications Cloud Native Core Policy                          |
| Oracle Communications Cloud Native Core Security Edge Protection Proxy, version 1.7.0                | Communications Cloud Native Core Security Edge Protection Proxy  |
| Oracle Communications Cloud Native Core Service Communication Proxy, version 1.5.2                   | Communications Cloud Native Core Service Communication Proxy     |
| Oracle Communications Cloud Native Core Unified Data Repository, versions 1.4.0, 1.6.0               | Communications Cloud Native Core Unified Data Repository         |
| Oracle Communications Convergent Charging Controller, version 12.0.4.0.0                             | Oracle Communications Convergent Charging Controller             |
| Oracle Communications Design Studio, version 7.4.2   | Oracle Communications Design Studio                              |
| Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0-8.5.0                          | Oracle Communications Diameter Signaling Router                  |
| Oracle Communications EAGLE Software, versions 46.6.0-46.8.2   | Oracle Communications EAGLE                                      |
| Oracle Communications Evolved Communications Application Server, version 7.1                         | Oracle Communications Evolved Communications Application Server  |
| Oracle Communications Instant Messaging Server, version 10.0.1.4.0                                   | Oracle Communications Instant Messaging Server                   |
| Oracle Communications Network Charging and Control, versions 6.0.1.0, 12.0.1.0-12.0.4.0, 12.0.4.0.0  | Oracle Communications Network Charging and Control               |
| Oracle Communications Offline Mediation Controller, version 12.0.0.3.0                               | Oracle Communications Offline Mediation Controller               |
| Oracle Communications Pricing Design Center, version 12.0.0.3.0                                      | Oracle Communications Pricing Design Center                      |
| Oracle Communications Services Gatekeeper, versions 7.0  | Oracle Communications Services Gatekeeper                        |
| Oracle Communications Unified Inventory Management, versions 7.3.2, 7.3.4, 7.3.5, 7.4.0, 7.4.1       | Oracle Communications Unified Inventory Management               |
| Oracle Configuration Manager, version 12.1.2.0.8   | Enterprise Manager   |
| Oracle Data Integrator, versions 12.2.1.3.0, 12.2.1.4.0  | Fusion Middleware  |
| Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 19c   | Database   |
| Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10                                      | Oracle E-Business Suite  |
| Oracle Enterprise Data Quality, versions 12.2.1.3.0, 12.2.1.4.0                                      | Fusion Middleware  |
| Oracle Enterprise Repository, version 11.1.1.7.0   | Fusion Middleware  |
| Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.0.9, 8.1.0, 8.1.1 | Oracle Financial Services Analytical Applications Infrastructure |

| Affected Products and Versions  | Patch Availability Document  |
|---|--|
| Oracle Financial Services Crime and Compliance Investigation Hub, version 20.1.2          | Oracle Financial Services Crime and Compliance Investigation Hub   |
| Oracle Financial Services Regulatory Reporting with AgileREPORTER, version 8.0.9.6.3      | Oracle Financial Services Regulatory Reporting with AgileREPORTER  |
| Oracle Financial Services Revenue Management and Billing Analytics, versions 2.7.0, 2.8.0 | Oracle Financial Services Revenue Management and Billing Analytics |
| Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0                                  | Contact Support  |
| Oracle FLEXCUBE Universal Banking, versions 12.0-12.4, 14.0-14.4.0                        | Contact Support  |
| Oracle Fusion Middleware MapViewer, version 12.2.1.4.0                                    | Fusion Middleware  |
| Oracle GoldenGate Application Adapters, version 19.1.0.0.0                                | Fusion Middleware  |
| Oracle GraalVM Enterprise Edition, versions 20.3.2, 21.1.0                                | Java SE  |
| Oracle Hospitality Reporting and Analytics, version 9.1.0                                 | Oracle Hospitality Reporting and Analytics                         |
| Oracle Hospitality Suite8, versions 8.13, 8.14  | MICROS BellaVita   |
| Oracle Hyperion BI+, versions 11.1.2.4, 11.2.5.0  | Fusion Middleware  |
| Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0-11.3.0                    | Oracle Insurance Applications                                      |
| Oracle Insurance Policy Administration J2EE, version 11.0.2                               | Oracle Insurance Applications                                      |
| Oracle Insurance Rules Palette, versions 11.0.2, 11.1.0-11.3.0                            | Oracle Insurance Applications                                      |
| Oracle Java SE, versions 7u301, 8u291, 11.0.11, 16.0.1                                    | Java SE  |
| Oracle JDeveloper, versions 12.2.1.4.0  | Fusion Middleware  |
| Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0                             | Fusion Middleware  |
| Oracle Outside In Technology, version 8.5.5   | Fusion Middleware  |
| Oracle Policy Automation, versions 12.2.0-12.2.22   | Oracle Policy Automation   |
| Oracle Retail Back Office, version 14.1   | Retail Applications  |
| Oracle Retail Central Office, version 14.1  | Retail Applications  |
| Oracle Retail Customer Engagement, versions 16.0-19.0                                     | Retail Applications  |
| Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0         | Retail Applications  |
| Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3.0                | Retail Applications  |
| Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3.0                      | Retail Applications  |
| Oracle Retail Merchandising System, versions 14.1.3.2, 15.0.3.1, 16.0.3                   | Retail Applications  |

| Affected Products and Versions  | Patch Availability Document               |
|---|---|
| Oracle Retail Order Broker, versions 15.0, 16.0   | Retail Applications                       |
| Oracle Retail Order Management System Cloud Service, version 19.5                           | Retail Applications                       |
| Oracle Retail Point-of-Service, version 14.1  | Retail Applications                       |
| Oracle Retail Price Management, versions 14.0, 14.1, 15.0, 16.0                             | Retail Applications                       |
| Oracle Retail Returns Management, version 14.1  | Retail Applications                       |
| Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3.0                       | Retail Applications                       |
| Oracle Retail Xstore Point of Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1      | Retail Applications                       |
| Oracle SD-WAN Aware, versions 8.2, 9.0  | Oracle SD-WAN Aware                       |
| Oracle SD-WAN Edge, versions 8.2, 9.0, 9.1  | Oracle SD-WAN Edge                        |
| Oracle Secure Global Desktop, version 5.6   | Virtualization                            |
| Oracle Solaris, version 11  | Systems                                   |
| Oracle Solaris Cluster, version 4.4   | Systems                                   |
| Oracle Transportation Management, version 6.4.3   | Oracle Supply Chain Products              |
| Oracle VM VirtualBox, versions prior to 6.1.24  | Virtualization                            |
| Oracle WebCenter Portal, versions 11.1.1.9.0, 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                                   |
| OSS Support Tools, versions prior to 2.12.41  | Support Tools                             |
| PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2                                | PeopleSoft                                |
| PeopleSoft Enterprise HCM Candidate Gateway, version 9.2                                    | PeopleSoft                                |
| PeopleSoft Enterprise HCM Shared Components, version 9.2                                    | PeopleSoft                                |
| PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.58.8.59, 8.59                     | PeopleSoft                                |
| PeopleSoft Enterprise PT PeopleTools, versions 8.57, 8.58, 8.59                             | PeopleSoft                                |
| Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.11, 19.12.0-19.12.10, 20.12.0     | Oracle Construction and Engineering Suite |

| Affected Products and Versions   | Patch Availability Document             |
|--|---|
| Primavera P6 Enterprise Project Portfolio Management, versions 17.12.0-17.12.20, 18.8.0-18.8.23, 19.12.0-19.12.14, 20.12.0-20.12.3 | Oracle Construction and Engineering Sui |
| Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12   | Oracle Construction and Engineering Sui |
| Real-Time Decisions (RTD) Solutions, version 3.2.0.0   | Fusion Middleware                       |
| Siebel Applications, versions 21.5 and prior   | Siebel                                  |
| StorageTek Tape Analytics SW Tool, version 2.3   | Systems                                 |

## 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:

- Oxfoxone: CVE-2021-2452
- Andrej Simko of Accenture: CVE-2021-2436
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2021-2389, CVE-2021-2390, CVE-2021-2429
- Armaan Khurshid Pathan of Emirates Group: CVE-2021-2373
- Billy Jheng Bing Jhong of STAR Labs: CVE-2021-2443
- Devin Rosenbauer of Identity Works LLC: CVE-2021-2457
- Dimitris Doganos of COSMOTE - Mobile Telecommunications S.A.: CVE-2021-2345, CVE-2021-2346, CVE-2021-2348
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd: CVE-2021-2328, CVE-2021-2329, CVE-2021-2333, CVE-2021-2337
- Emad Al-Mousa: CVE-2021-2326
- Faraz Khan from Emirates Group: CVE-2021-2375
- Filip Ceglik: CVE-2021-2448
- Gianluca Danesin of Mondadori: CVE-2021-2412
- Girlelecta: CVE-2021-2419, CVE-2021-2420, CVE-2021-2423, CVE-2021-2430, CVE-2021-2431, CVE-2021-2449, CVE-2021-2450, CVE-2021-2451, CVE-2021-2453
- Guillaume Jacques of synacktiv: CVE-2021-2435

- Haya Shulman of Fraunhofer.de: CVE-2021-2432
- Huixin Ma of Tencent.com: CVE-2021-2388
- Jang Laptop of VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2021-2400, CVE-2021-2401
- Kajetan Rostojek: CVE-2021-2349, CVE-2021-2350
- KPC of Trend Micro's Zero Day Initiative: CVE-2021-2392
- Li Boheng of Tophant Starlight laboratory : CVE-2021-2394
- Longofo of Knownsec 404 Team: CVE-2021-2376, CVE-2021-2403, CVE-2021-2428, CVE-2021-2433, CVE-2021-2456
- Maciej Grabiec of ING Tech Poland: CVE-2021-2350
- Markus Loewe: CVE-2021-2369
- Martin Neumann of Accenture: CVE-2021-2359
- Matthias Kaiser of Apple Information Security: CVE-2021-2394, CVE-2021-2397
- Max Van Amerongen (maxploit): CVE-2021-2442
- Mohit Rawat: CVE-2021-2458
- Moritz Bechler of SySS GmbH: CVE-2021-2351
- Okan Basegmez: CVE-2021-2334, CVE-2021-2335, CVE-2021-2336
- Paul Barbé of synacktiv: CVE-2021-2347, CVE-2021-2435, CVE-2021-2439, CVE-2021-2445
- Peterjson of RedTeam@VNG Corporation working with Trend Micro Zero Day Initiative: CVE-2021-2456
- Philipp Jeitner of Fraunhofer.de: CVE-2021-2432
- Qiguang Zhu: CVE-2021-2333
- Quynh Le of VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2021-2391, CVE-2021-2396
- r00t4dm at Cloud-Penetrating Arrow Lab: CVE-2021-2376, CVE-2021-2403, CVE-2021-2428, CVE-2021-2433, CVE-2021-2456
- thiscodecc of MoyunSec V-Lab: CVE-2021-2382, CVE-2021-2394
- threedr3am: CVE-2021-2344, CVE-2021-2371, CVE-2021-2376, CVE-2021-2378
- Théo Louis-Tisserand of synacktiv: CVE-2021-2435
- Varnavas Papaioannou: CVE-2021-2341
- Ved Prabhu: CVE-2021-2460
- Vishnu Dev T J working with Trend Micro's Zero Day Initiative: CVE-2021-2409
- Waleed Ezz Eldin of Cysiv (Previously SecureMisr): CVE-2021-2380

- Yaoguang Chen of Ant Security Light-Year Lab: CVE-2021-2330, CVE-2021-2357, CVE-2021-2444

## 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:

- Aleksey Shipilev of Red Hat
- Brian Reilly [2 reports]
- Emad Al-Mousa
- Markus Loewe [2 reports]
- threedr3am [3 reports]

## 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:

- Abhishek Morla
- Adeel Khan
- Ashik Kunjumon
- Boumediene Kaddour
- Gaurang Maheta of gaurang maheta
- Hamoud Al-Helmani
- Husnain Iqbal
- Information Security Management
- Khalid matar Alharthi

- Marwan Albahar
- Mohamed Ahmed Naji
- Naman Shah
- Nik Czuprinski
- Pratik Khalane [2 reports]
- Rajnish Kumar Gupta
- Rakan Abdulrahman Al Khaled
- Sakhare Vinayak
- Snigdha Priya
- Sohamin Durkar
- Stefano Barber
- Tech Zone
- Vivek Panday
- Yash Sharma [2 reports]
- Zach Edwards of victorymedium.com
- Zoe Pentaleri

## Critical Patch Update Schedule

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

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

## References

- [Oracle Critical Patch Updates, Security Alerts and Bulletins](#)
- [Critical Patch Update - July 2021 Documentation Map](#)
- [Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions](#)
- [Risk Matrix Definitions](#)
- [Use of Common Vulnerability Scoring System \(CVSS\) by Oracle](#)
- [English text version of the risk matrices](#)

- [CVRF XML version of the risk matrices](#)
- [Map of CVE to Advisory/Alert](#)
- [Oracle Lifetime support Policy](#)
- [JEP 290 Reference Blocklist Filter](#)

## Modification History

| Date              | Note   |
|-------------------|--|
| 2021-September-03 | Rev 7. Removed additional CVEs of the patch for CVE-2019-17195   |
| 2021-August-18    | Rev 6. Updated CVSS scores for Outside In Technology   |
| 2021-July-30      | Rev 5. Updated affected version for Oracle Communications Services Gatekeeper                          |
| 2021-July-26      | Rev 4. Removed Oracle JDeveloper version 12.2.1.3.0, updated Credit Statement                          |
| 2021-July-23      | Rev 3. Removed Oracle JDeveloper and ADF entry from the product table. Update Credit Statement.        |
| 2021-July-21      | Rev 2. Updated Credit Statement, Oracle BI Publisher affected versions updated, M note numbers updated |
| 2021-July-20      | Rev 1. Initial Release.  |

## Oracle Database Products Risk Matrices

This Critical Patch Update contains 27 new security patches for Oracle Database Products divided as follows:

- 16 new security patches for Oracle Database Products
- 2 new security patches for Oracle Big Data Graph
- 9 new security patches for Oracle Essbase

## Oracle Database Server Risk Matrix

This Critical Patch Update contains 16 new security patches plus additional third party patches noted below for Oracle Database Products. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 of these patches is applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found [here](#).

| CVE#                  | Component  | Package and/or Privilege Required           | Protocol   | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|-----------------------|--|---|------------|-------------------------------|----------------------|---------------|----------------|-------------|
|                       |  |   |            |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2021-2351</b>  | Advanced Networking Option                                 | None  | Oracle Net | Yes                           | 8.3                  | Network       | High           | None        |
| <b>CVE-2021-2328</b>  | Oracle Text  | Create Any Procedure, Alter Any Table       | Oracle Net | No                            | 7.2                  | Network       | Low            | High        |
| <b>CVE-2021-2329</b>  | Oracle XML DB  | Create Any Procedure, Create Public Synonym | Oracle Net | No                            | 7.2                  | Network       | Low            | High        |
| <b>CVE-2021-2337</b>  | Oracle XML DB  | Create Any Procedure, Create Public Synonym | Oracle Net | No                            | 7.2                  | Network       | Low            | High        |
| <b>CVE-2020-27193</b> | Oracle Application Express (CKEditor)                      | Valid User Account                          | HTTP       | No                            | 5.4                  | Network       | Low            | Low         |
| <b>CVE-2020-26870</b> | Oracle Application Express Application Builder (DOMPurify) | Valid User Account                          | HTTP       | No                            | 5.4                  | Network       | Low            | Low         |
| <b>CVE-2021-2460</b>  | Oracle Application Express Data Reporter                   | Valid User Account                          | HTTP       | No                            | 5.4                  | Network       | Low            | Low         |
| <b>CVE-2021-2333</b>  | Oracle XML DB  | Alter User                                  | Oracle Net | No                            | 4.9                  | Network       | Low            | High        |
| <b>CVE-2019-17545</b> | Oracle Spatial and Graph (GDAL)                            | Create Session                              | Oracle Net | No                            | 4.4                  | Local         | High           | Low         |

| CVE#                 | Component  | Package and/or Privilege Required | Protocol   | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|----------------------|--|-----------------------------------|------------|-------------------------------|----------------------|---------------|----------------|-------------|
|                      |  |                                   |            |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2021-2330</b> | Core RDBMS   | Create Table                      | Oracle Net | No                            | 4.3                  | Network       | Low            | Low         |
| <b>CVE-2020-7760</b> | Enterprise Manager Express User Interface (CodeMirror) | User Account                      | HTTP       | No                            | 4.3                  | Network       | Low            | Low         |
| <b>CVE-2021-2438</b> | Java VM  | Create Procedure                  | Oracle Net | No                            | 4.3                  | Network       | Low            | Low         |
| <b>CVE-2021-2334</b> | Oracle Database - Enterprise Edition Data Redaction    | Create Session                    | Oracle Net | No                            | 3.5                  | Network       | Low            | Low         |
| <b>CVE-2021-2335</b> | Oracle Database - Enterprise Edition Data Redaction    | Create Session                    | Oracle Net | No                            | 3.5                  | Network       | Low            | Low         |
| <b>CVE-2021-2336</b> | Oracle Database - Enterprise Edition Data Redaction    | Create Session                    | Oracle Net | No                            | 3.5                  | Network       | Low            | Low         |
| <b>CVE-2021-2326</b> | Database Vault   | DBA                               | Oracle Net | No                            | 2.7                  | Network       | Low            | High        |

### Notes:

1. The July 2021 Critical Patch Update introduces a number of Native Network Encryption changes to deal with vulnerability CVE-2021-2351 and prevent the use of weaker ciphers. Customers should review: “Changes in Native Network Encryption with the July 2021 Critical Patch Update” ([Doc ID 2791571.1](#)).

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

- MapViewer (OWASP ESAPI)Oracle Spatial and Graph (OpenJPEG): CVE-2020-27844, CVE-2018-21010, CVE-2019-12973, CVE-2020-15389, CVE-2020-27814, CVE-2020-27841, CVE-

2020-27842, CVE-2020-27843 and CVE-2020-27845.

- Oracle Database - Enterprise Edition (Kerberos): CVE-2020-28196.
- Oracle Database Migration Assistant for Unicode (Apache POI): CVE-2019-12415.
- Oracle Spatial and Graph (jackson-databind): CVE-2020-25649.
- Oracle Spatial and Graph MapViewer (Apache Batik): CVE-2020-11987 and CVE-2019-17566.
- Oracle Spatial and Graph MapViewer (Apache HttpClient): CVE-2020-13956.
- Oracle Spatial and Graph MapViewer (Apache XMLGraphics Commons): CVE-2020-11988.
- Oracle Spatial and Graph MapViewer (Google Guava): CVE-2020-8908.
- Oracle Spatial and Graph Network Data Model (jackson-databind): CVE-2020-25649.
- RDBMS (Perl): CVE-2020-10878, CVE-2020-10543 and CVE-2020-12723.
- RDBMS (Python): CVE-2021-23336.

### Oracle Database Server Client-Only Installations

- The following Oracle Database Server vulnerability included in this Critical Patch Update affects client-only installations: CVE-2021-2351.

## Oracle Big Data Graph Risk Matrix

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

| CVE#                  | Product                    | Component                      | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RISK ( |               |                |             |    |
|-----------------------|----------------------------|--------------------------------|----------|-------------------------------|-------------------------|---------------|----------------|-------------|----|
|                       |                            |                                |          |                               | Base Score              | Attack Vector | Attack Complex | Privs Req'd | In |
| <b>CVE-2019-5064</b>  | Big Data Spatial and Graph | Big Data Graph (OpenCV)        | HTTP     | Yes                           | 8.8                     | Network       | Low            | None        | Re |
| <b>CVE-2020-17527</b> | Big Data Spatial and Graph | Big Data Graph (Apache Tomcat) | HTTP     | Yes                           | 7.5                     | Network       | Low            | None        | M  |

**Additional CVEs addressed are:**

- The patch for CVE-2019-5064 also addresses CVE-2019-5063.

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

- Big Data Spatial and Graph
  - Big Data Graph (Lodash): CVE-2020-8203.
  - Big Data Graph (jackson-databind): 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, CVE-2020-36188 and CVE-2020-36189.

## Oracle Essbase Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Essbase. 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 |
| <b>CVE-2021-2244</b> | Essbase Analytic Provider Services       | JAPI                     | HTTP     | Yes                           | 10.0           | Network       | Low            | N     |
| <b>CVE-2021-2349</b> | Hyperion Essbase Administration Services | EAS Console              | HTTP     | Yes                           | 8.6            | Network       | Low            | N     |
| <b>CVE-2021-2435</b> | Essbase Analytic Provider Services       | JAPI                     | HTTP     | Yes                           | 8.1            | Network       | Low            | N     |
| <b>CVE-2019-0190</b> | Essbase                                  | Infrastructure (OpenSSL) | HTTPS    | Yes                           | 7.5            | Network       | Low            | N     |

| CVE#                  | Product                                  | Component                                | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3 |                  |                |    |
|-----------------------|--|--|----------|-------------------------------|----------------|------------------|----------------|----|
|                       |  |  |          |                               | Base Score     | Attack Vector    | Attack Complex | Pr |
| <b>CVE-2020-8285</b>  | Essbase                                  | Infrastructure (cURL)                    | Multiple | Yes                           | 7.5            | Network          | Low            | N  |
| <b>CVE-2021-2433</b>  | Essbase Analytic Provider Services       | Web Services                             | HTTP     | Yes                           | 7.5            | Network          | Low            | N  |
| <b>CVE-2021-2350</b>  | Hyperion Essbase Administration Services | EAS Console                              | HTTP     | Yes                           | 7.5            | Network          | Low            | N  |
| <b>CVE-2020-7760</b>  | Essbase                                  | Infrastructure (CodeMirror)              | HTTP     | Yes                           | 5.3            | Network          | Low            | N  |
| <b>CVE-2019-12402</b> | Essbase                                  | Infrastructure (Apache Commons Compress) | HTTP     | No                            | 4.1            | Adjacent Network | Low            | L  |

#### Additional CVEs addressed are:

- The patch for CVE-2019-0190 also addresses CVE-2020-1971, CVE-2021-23840, CVE-2021-23841, CVE-2021-3449 and CVE-2021-3450.
- The patch for CVE-2020-8285 also addresses CVE-2020-8284, CVE-2020-8286, CVE-2021-22876 and CVE-2021-22890.

## Oracle Commerce Risk Matrix

This Critical Patch Update contains 11 new security patches for Oracle Commerce. 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 |
| <b>CVE-2021-2463</b>  | Oracle Commerce Platform   | Dynamo Application Framework                           | HTTP     | Yes                           | 9.8              | Network       | Low            | Nc     |
| <b>CVE-2020-2555</b>  | Oracle Commerce Platform   | Dynamo Application Framework (Coherence)               | HTTP     | Yes                           | 9.8              | Network       | Low            | Nc     |
| <b>CVE-2020-2604</b>  | Oracle Commerce Guided Search                                      | Content Acquisition System (Java SE)                   | HTTP     | Yes                           | 8.1              | Network       | High           | Nc     |
| <b>CVE-2021-20190</b> | Oracle Commerce Guided Search / Oracle Commerce Experience Manager | Experience Manage (jackson-databind)                   | HTTP     | Yes                           | 8.1              | Network       | High           | Nc     |
| <b>CVE-2020-2604</b>  | Oracle Commerce Guided Search / Oracle Commerce Experience Manager | Tools and Frameworks (Java SE)                         | HTTP     | Yes                           | 8.1              | Network       | High           | Nc     |
| <b>CVE-2020-25649</b> | Oracle Commerce Platform   | Dynamo Application Framework (jackson-databind)        | HTTP     | Yes                           | 8.1              | Network       | High           | Nc     |
| <b>CVE-2021-26272</b> | Oracle Commerce Merchandising                                      | Experience Manager, Business Control Center (CKEditor) | HTTP     | Yes                           | 6.5              | Network       | Low            | Nc     |
| <b>CVE-2021-2462</b>  | Oracle Commerce  | Commerce Service                                       | HTTP     | Yes                           | 6.1              | Network       | Low            | Nc     |

| CVE#                 | Product  | Component            | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |        |
|----------------------|--|----------------------|----------|-------------------------------|------------------|---------------|----------------|--------|
|                      |  |                      |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Re |
|                      | Service Center   | Center               |          |                               |                  |               |                |        |
| <b>CVE-2021-2345</b> | Oracle Commerce Guided Search / Oracle Commerce Experience Manager | Tools and Frameworks | HTTP     | No                            | 5.4              | Network       | Low            | Lc     |
| <b>CVE-2021-2346</b> | Oracle Commerce Guided Search / Oracle Commerce Experience Manager | Tools and Frameworks | HTTP     | No                            | 5.4              | Network       | Low            | Lc     |
| <b>CVE-2021-2348</b> | Oracle Commerce Guided Search / Oracle Commerce Experience Manager | Tools and Frameworks | HTTP     | No                            | 4.3              | Network       | Low            | Lc     |

#### Additional CVEs addressed are:

- The patch for CVE-2020-25649 also addresses CVE-2020-36189.

## Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 33 new security patches for Oracle Communications Applications. 22 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE#                  | Product   | Component                     | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|---|-------------------------------|----------|-------------------------------|------------------|---------------|-------------------|
|                       |   |                               |          |                               | Base Score       | Attack Vector | Attack Complexity |
| <b>CVE-2021-21345</b> | Oracle Communications BRM - Elastic Charging Engine | CN ECE (XStream)              | HTTP     | No                            | 9.9              | Network       | Low               |
| <b>CVE-2021-21345</b> | Oracle Communications Unified Inventory Management  | Drools Ruleset (XStream)      | HTTP     | No                            | 9.9              | Network       | Low               |
| <b>CVE-2020-11612</b> | Oracle Communications BRM - Elastic Charging Engine | HTTP GW (Netty)               | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2021-3177</b>  | Oracle Communications Offline Mediation Controller  | UDC CORE (Python)             | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2020-17530</b> | Oracle Communications Pricing Design Center         | CNE (Apache Struts)           | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2019-17195</b> | Oracle Communications Pricing Design Center         | CNE (Nimbus JOSE+JWT)         | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2021-22112</b> | Oracle Communications Unified Inventory Management  | REST API (Spring Security)    | HTTP     | No                            | 8.8              | Network       | Low               |
| <b>CVE-2020-10878</b> | Oracle Communications Offline Mediation Controller  | UDC CORE (Perl)               | TCP/IP   | Yes                           | 8.6              | Network       | Low               |
| <b>CVE-2020-10878</b> | Oracle Communications Pricing Design Center         | Transformation for PDC (Perl) | HTTP     | Yes                           | 8.6              | Network       | Low               |

| CVE#                  | Product  | Component                                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|--|--|----------|-------------------------------|------------------|---------------|-------------------|
|                       |  |  |          |                               | Base Score       | Attack Vector | Attack Complexity |
| <b>CVE-2020-14195</b> | Oracle Communications Instant Messaging Server       | Managing Messages (jackson-databind)         | HTTP     | Yes                           | 8.1              | Network       | High              |
| <b>CVE-2021-3345</b>  | Oracle Communications Billing and Revenue Management | Accounts Receivable (libgcrypt)              | None     | No                            | 7.8              | Local         | Low               |
| <b>CVE-2020-27216</b> | Oracle Communications Offline Mediation Controller   | CN OCOMC (Eclipse Jetty)                     | None     | No                            | 7.8              | Local         | Low               |
| <b>CVE-2020-27216</b> | Oracle Communications Pricing Design Center          | Transformation for PDC (Eclipse Jetty)       | None     | No                            | 7.8              | Local         | Low               |
| <b>CVE-2020-8286</b>  | Oracle Communications Billing and Revenue Management | Balances (cURL)                              | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Billing and Revenue Management | Business Operation Center (jackson-databind) | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Convergent Charging Controller | Common fns (jackson-databind)                | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Network Charging and Control   | OUI (jackson-databind)                       | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2019-17566</b> | Oracle Communications                                | CN OCOMC (Apache Batik)                      | HTTP     | Yes                           | 7.5              | Network       | Low               |

| CVE#                  | Product  | Component   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|--|---|----------|-------------------------------|------------------|---------------|-------------------|
|                       |  |   |          |                               | Base Score       | Attack Vector | Attack Complexity |
|                       | Offline Mediation Controller                         |   |          |                               |                  |               |                   |
| <b>CVE-2020-28196</b> | Oracle Communications Offline Mediation Controller   | NM Core (Kerberos)                                | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-5258</b>  | Oracle Communications Pricing Design Center          | Server for PDC (dojo)                             | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-17527</b> | Oracle Communications Pricing Design Center          | Transformation for PDC (Apache Tomcat)            | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-28196</b> | Oracle Communications Pricing Design Center          | Transformation for PDC (Kerberos)                 | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25648</b> | Oracle Communications Pricing Design Center          | CNE (NSS)   | HTTPS    | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Unified Inventory Management   | Media Resource (jackson-databind)                 | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-8203</b>  | Oracle Communications Billing and Revenue Management | Billing Care (Lodash)                             | HTTP     | Yes                           | 7.4              | Network       | High              |
| <b>CVE-2019-10086</b> | Oracle Communications Pricing Design Center          | Transformation for PDC (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3              | Network       | Low               |

| CVE#                  | Product  | Component                                   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|--|---|----------|-------------------------------|------------------|---------------|-------------------|
|                       |  |   |          |                               | Base Score       | Attack Vector | Attack Complexity |
| <b>CVE-2020-9484</b>  | Oracle Communications Instant Messaging Server       | Managing Messages (Apache Tomcat)           | None     | No                            | 7.0              | Local         | High              |
| <b>CVE-2020-7017</b>  | Oracle Communications Billing and Revenue Management | Balance Monitoring Manager (Kibana)         | HTTP     | No                            | 6.7              | Network       | High              |
| <b>CVE-2019-3740</b>  | Oracle Communications Unified Inventory Management   | Inventory Organizer (BSAFE Crypto-J)        | HTTP     | Yes                           | 6.5              | Network       | Low               |
| <b>CVE-2020-17521</b> | Oracle Communications BRM - Elastic Charging Engine  | Elastic charging controller (Apache Groovy) | None     | No                            | 5.5              | Local         | Low               |
| <b>CVE-2021-21290</b> | Oracle Communications Design Studio                  | Modeling (Netty)                            | None     | No                            | 5.5              | Local         | Low               |
| <b>CVE-2021-20227</b> | Oracle Communications Network Charging and Control   | Common fns (SQLite)                         | None     | No                            | 5.5              | Local         | Low               |
| <b>CVE-2020-11987</b> | Oracle Communications Offline Mediation Controller   | UDC CORE (Apache Batik)                     | TCP/IP   | Yes                           | 5.3              | Network       | Low               |

#### Additional CVEs addressed are:

- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739.
- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723.
- The patch for CVE-2020-11612 also addresses CVE-2021-21290.

- The patch for CVE-2020-14195 also addresses CVE-2020-14060, CVE-2020-14061 and CVE-2020-14062.
- 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-2020-27216 also addresses CVE-2020-27218.
- The patch for CVE-2020-7017 also addresses CVE-2020-7016.
- The patch for CVE-2020-8286 also addresses CVE-2020-8284 and CVE-2020-8285.
- 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-2021-3177 also addresses CVE-2021-23336.

## Oracle Communications Risk Matrix

This Critical Patch Update contains 26 new security patches for Oracle Communications. 23 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 Complexity |
| <b>CVE-2019-17195</b> | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Configuration (Nimbus JOSE+JWT) | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2020-11612</b> | Oracle Communications Cloud Native Core Service Communication Proxy    | KPI (Netty)                     | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2020-11998</b> | Oracle Communications Diameter   | Provisioning (Apache ActiveMQ)  | HTTP     | Yes                           | 9.8              | Network       | Low               |

| CVE#                  | Product   | Component                                   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|---|---|----------|-------------------------------|------------------|---------------|-------------------|
|                       |   |   |          |                               | Base Score       | Attack Vector | Attack Complexity |
|                       | Signaling Router (DSR)  |   |          |                               |                  |               |                   |
| <b>CVE-2019-12260</b> | Oracle Communications EAGLE Software  | Measurements (VxWorks)                      | HTTP     | Yes                           | 9.8              | Network       | Low               |
| <b>CVE-2020-10878</b> | Oracle SD-WAN Aware   | Monitoring (Perl)                           | HTTP     | Yes                           | 8.6              | Network       | Low               |
| <b>CVE-2020-10543</b> | Oracle SD-WAN Edge  | Publications (Perl)                         | HTTP     | Yes                           | 8.6              | Network       | Low               |
| <b>CVE-2020-27216</b> | Oracle Communications Services Gatekeeper   | Call Control Common Service (Eclipse Jetty) | None     | No                            | 7.8              | Local         | Low               |
| <b>CVE-2020-5258</b>  | Oracle Communications Application Session Controller                              | Signaling (dojo)                            | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2019-10746</b> | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Configuration (Kibana)                      | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-7733</b>  | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Signaling (Kibana)                          | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2017-9735</b>  | Oracle Communications Cloud Native Core Policy                                    | Configuration (Jetty)                       | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-5398</b>  | Oracle Communications Cloud Native Core Policy                                    | Configuration (Spring Framework)            | HTTP     | Yes                           | 7.5              | Network       | High              |

| CVE#                  | Product   | Component   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|---|---|----------|-------------------------------|------------------|---------------|-------------------|
|                       |   |   |          |                               | Base Score       | Attack Vector | Attack Complexity |
| <b>CVE-2019-12399</b> | Oracle Communications Cloud Native Core Policy                  | Measurements (Apache Kafka)                                   | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Cloud Native Core Unified Data Repository | UDR (jackson-databind)  | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Evolved Communications Application Server | Session Design Center GUI (jackson-databind)                  | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2020-25649</b> | Oracle Communications Services Gatekeeper                       | OCSG Policy service (jackson-databind)                        | HTTP     | Yes                           | 7.5              | Network       | Low               |
| <b>CVE-2019-10086</b> | Oracle Communications Cloud Native Core Console                 | Signaling (Apache Commons BeanUtils)                          | HTTP     | Yes                           | 7.3              | Network       | Low               |
| <b>CVE-2019-10086</b> | Oracle Communications Cloud Native Core Policy                  | Measurements (Apache Commons BeanUtils)                       | HTTP     | Yes                           | 7.3              | Network       | Low               |
| <b>CVE-2019-10086</b> | Oracle Communications Cloud Native Core Unified Data Repository | Measurements (Apache Commons BeanUtils)                       | HTTP     | Yes                           | 7.3              | Network       | Low               |
| <b>CVE-2019-10086</b> | Oracle Communications Evolved Communications Application Server | Managing and Using Subscriber Data (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3              | Network       | Low               |
| <b>CVE-2018-15686</b> | Oracle Communications Cloud Native                              | Signaling (Calico)  | None     | No                            | 6.3              | Local         | High              |

| CVE#                  | Product  | Component                          | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |
|-----------------------|--|------------------------------------|----------|-------------------------------|------------------|---------------|-------------------|
|                       |  |                                    |          |                               | Base Score       | Attack Vector | Attack Complexity |
|                       | Core Network Function Cloud Native Environment                           |                                    |          |                               |                  |               |                   |
| <b>CVE-2020-24553</b> | Oracle Communications Cloud Native Core Policy                           | Signaling (Go)                     | HTTP     | Yes                           | 6.1              | Network       | Low               |
| <b>CVE-2020-17521</b> | Oracle Communications Evolved Communications Application Server          | Control Engine (Apache Groovy)     | None     | No                            | 5.5              | Local         | Low               |
| <b>CVE-2020-29582</b> | Oracle Communications Cloud Native Core Network Slice Selection Function | Signaling (Calico)                 | HTTP     | Yes                           | 5.3              | Network       | Low               |
| <b>CVE-2020-27218</b> | Oracle Communications Services Gatekeeper                                | Subscriber profile (Eclipse Jetty) | HTTP     | Yes                           | 4.8              | Network       | High              |
| <b>CVE-2016-0762</b>  | Oracle Communications Diameter Signaling Router (DSR)                    | Provisioning (Apache Tomcat)       | HTTP     | Yes                           | 4.3              | Network       | Low               |

#### Additional CVEs addressed are:

- The patch for CVE-2016-0762 also addresses CVE-2021-30369, CVE-2021-30640 and CVE-2021-33037.
- The patch for CVE-2017-9735 also addresses CVE-2017-7656, CVE-2017-7657 and CVE-2017-7658.
- The patch for CVE-2019-10746 also addresses CVE-2019-15604, CVE-2019-15605 and CVE-2019-15606.
- The patch for CVE-2020-10543 also addresses CVE-2020-10878 and CVE-2020-12723.
- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723.

- 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-2020-27218 also addresses CVE-2020-27216.
- The patch for CVE-2020-29582 also addresses CVE-2019-0205, CVE-2019-0210, CVE-2019-16942, CVE-2019-16943, CVE-2019-17531, CVE-2019-20330, CVE-2020-13949, CVE-2020-28052, CVE-2020-8554, CVE-2020-8908 and CVE-2021-21275.
- The patch for CVE-2020-7733 also addresses CVE-2020-7016 and CVE-2020-7017.

## Oracle Construction and Engineering Risk Matrix

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

| CVE#                  | Product                   | Component                   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3 |               |                |    |
|-----------------------|---------------------------|-----------------------------|----------|-------------------------------|----------------|---------------|----------------|----|
|                       |                           |                             |          |                               | Base Score     | Attack Vector | Attack Complex | Pr |
| <b>CVE-2019-17195</b> | Primavera Gateway         | Admin (Nimbus JOSE+JWT)     | HTTP     | Yes                           | 9.8            | Network       | Low            | Ni |
| <b>CVE-2021-25122</b> | Instantis EnterpriseTrack | HTTP Server (Apache Tomcat) | HTTP     | Yes                           | 7.5            | Network       | Low            | Ni |
| <b>CVE-2020-25649</b> | Primavera Gateway         | Admin (jackson-databind)    | HTTP     | Yes                           | 7.5            | Network       | Low            | Ni |
| <b>CVE-2020-8203</b>  | Primavera Gateway         | Admin (Lodash)              | HTTP     | Yes                           | 7.4            | Network       | High           | Ni |

| CVE#                  | Product  | Component                           | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3 |               |                |       |
|-----------------------|--|-------------------------------------|----------|-------------------------------|----------------|---------------|----------------|-------|
|                       |  |                                     |          |                               | Base Score     | Attack Vector | Attack Complex | Pr Re |
| <b>CVE-2021-2366</b>  | Primavera P6 Enterprise Project Portfolio Management | Web Access                          | HTTP     | No                            | 6.4            | Network       | Low            | L     |
| <b>CVE-2021-21409</b> | Primavera Gateway                                    | Admin (Netty)                       | HTTP     | Yes                           | 5.9            | Network       | High           | No    |
| <b>CVE-2021-27906</b> | Primavera Unifier                                    | Core (Apache PDFbox)                | None     | No                            | 5.5            | Local         | Low            | No    |
| <b>CVE-2021-2386</b>  | Primavera P6 Enterprise Project Portfolio Management | Web Access                          | HTTP     | No                            | 4.3            | Network       | Low            | L     |
| <b>CVE-2020-5258</b>  | Primavera Unifier                                    | Core UI (dojo)                      | HTTP     | No                            | 4.3            | Network       | Low            | L     |
| <b>CVE-2020-25649</b> | Primavera Unifier                                    | Project Delivery (jackson-databind) | None     | No                            | 3.9            | Local         | Low            | L     |

#### Additional CVEs addressed are:

- The patch for CVE-2020-25649 also addresses CVE-2020-36189.
- The patch for CVE-2021-21409 also addresses CVE-2021-21290.
- The patch for CVE-2021-25122 also addresses CVE-2021-25329.
- The patch for CVE-2021-27906 also addresses CVE-2021-27807 and CVE-2021-31811.

## Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 17 new security patches for Oracle E-Business Suite. 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](#).

Oracle E-Business Suite products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle E-Business Suite products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that customers apply the July 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 (July 2021), [My Oracle Support Note 2770321.1](#).

| CVE#                 | Product                            | Component                     | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |       |
|----------------------|------------------------------------|-------------------------------|----------|-------------------------------|------------------|---------------|----------------|-------|
|                      |                                    |                               |          |                               | Base Score       | Attack Vector | Attack Complex | Pr Re |
| <b>CVE-2021-2355</b> | Oracle Marketing                   | Marketing Administration      | HTTP     | Yes                           | 9.1              | Network       | Low            | Nc    |
| <b>CVE-2021-2436</b> | Oracle Common Applications         | CRM User Management Framework | HTTP     | Yes                           | 8.2              | Network       | Low            | Nc    |
| <b>CVE-2021-2359</b> | Oracle Marketing                   | Marketing Administration      | HTTP     | Yes                           | 8.2              | Network       | Low            | Nc    |
| <b>CVE-2021-2361</b> | Oracle Advanced Inbound Telephony  | SDK client integration        | HTTP     | No                            | 8.1              | Network       | Low            | Lc    |
| <b>CVE-2021-2398</b> | Oracle Advanced Outbound Telephony | Region Mapping                | HTTP     | No                            | 8.1              | Network       | Low            | Lc    |
| <b>CVE-2021-2360</b> | Oracle Approvals Management        | AME Page rendering            | HTTP     | No                            | 8.1              | Network       | Low            | Lc    |

| CVE#                 | Product   | Component                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |                     |
|----------------------|---|------------------------------|----------|-------------------------------|------------------|---------------|-------------------|---------------------|
|                      |   |                              |          |                               | Base Score       | Attack Vector | Attack Complexity | Privileges Required |
| <b>CVE-2021-2406</b> | Oracle Collaborative Planning                   | User Interface               | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2393</b> | Oracle E-Records                                | E-signatures                 | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2405</b> | Oracle Engineering                              | Change Management            | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2362</b> | Oracle Field Service                            | Wireless                     | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2365</b> | Oracle Human Resources                          | People Management            | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2364</b> | Oracle iSupplier Portal                         | Accounts                     | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2363</b> | Oracle Public Sector Financials (International) | Authorization                | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2415</b> | Oracle Time and Labor                           | Timecard                     | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2434</b> | Oracle Web Applications Desktop Integrator      | Application Service          | HTTP     | No                            | 8.1              | Network       | Low               | Local               |
| <b>CVE-2021-2380</b> | Oracle Applications Framework                   | Attachments / File Upload    | HTTP     | No                            | 7.6              | Network       | Low               | Local               |
| <b>CVE-2021-2343</b> | Oracle Workflow                                 | Workflow Notification Mailer | HTTP     | No                            | 4.3              | Network       | Low               | Local               |

## Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 8 new security patches for Oracle Enterprise Manager. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found [here](#).

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the July 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 July 2021 Patch Availability Document for Oracle Products, [My Oracle Support Note 2773670.1](#).

| CVE#                  | Product                          | Component                               | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |         |
|-----------------------|----------------------------------|---|----------|-------------------------------|------------------|---------------|----------------|---------|
|                       |                                  |   |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Rec |
| <b>CVE-2020-10683</b> | Enterprise Manager Base Platform | Application Service Level Mgmt (dom4j)  | HTTP     | Yes                           | 9.8              | Network       | Low            | No      |
| <b>CVE-2019-5064</b>  | Enterprise Manager Base Platform | Application Service Level Mgmt (OpenCV) | HTTP     | Yes                           | 8.8              | Network       | Low            | No      |
| <b>CVE-2020-10878</b> | Oracle Configuration Manager     | Content Server (Perl)                   | HTTP     | Yes                           | 8.6              | Network       | Low            | No      |
| <b>CVE-2020-1971</b>  | Enterprise Manager Base Platform | Discovery Framework (OpenSSL)           | HTTPS    | Yes                           | 7.5              | Network       | Low            | No      |
| <b>CVE-2019-2897</b>  | Enterprise Manager Base Platform | Enterprise Config Management            | HTTP     | Yes                           | 7.4              | Network       | High           | No      |

| CVE#                  | Product                          | Component  | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |         |
|-----------------------|----------------------------------|--|----------|-------------------------------|------------------|---------------|----------------|---------|
|                       |                                  |  |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Rec |
| <b>CVE-2019-2897</b>  | Enterprise Manager Base Platform | System Monitoring                                    | HTTP     | Yes                           | 7.4              | Network       | High           | No      |
| <b>CVE-2019-10086</b> | Oracle Application Testing Suite | Load Testing for Web Apps (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3              | Network       | Low            | No      |
| <b>CVE-2017-14735</b> | Enterprise Manager Base Platform | UI Framework (AntiSamy)                              | HTTP     | Yes                           | 6.1              | Network       | Low            | No      |

#### Additional CVEs addressed are:

- The patch for CVE-2019-5064 also addresses CVE-2019-5063.
- The patch for CVE-2020-10878 also addresses CVE-2020-10543 and CVE-2020-12723.
- The patch for CVE-2020-1971 also addresses CVE-2020-1967.

## Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 22 new security patches for Oracle Financial Services Applications. 17 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE#                  | Product                                      | Component             | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                |   |
|-----------------------|--|-----------------------|----------|-------------------------------|--------------|---------------|----------------|---|
|                       |  |                       |          |                               | Base Score   | Attack Vector | Attack Complex | I |
| <b>CVE-2021-21345</b> | Oracle Banking Enterprise Default Management | Collections (XStream) | HTTP     | No                            | 9.9          | Network       | Low            |   |
| <b>CVE-2021-21345</b> | Oracle Banking Platform                      | Collections (XStream) | HTTP     | No                            | 9.9          | Network       | Low            |   |

| CVE#                  | Product  | Component                               | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                   |
|-----------------------|--|---|----------|-------------------------------|--------------|---------------|-------------------|
|                       |  |   |          |                               | Base Score   | Attack Vector | Attack Complexity |
| <b>CVE-2019-0228</b>  | Oracle Banking Liquidity Management                              | Onboarding (Apache PDFbox)              | HTTP     | Yes                           | 9.8          | Network       | Low               |
| <b>CVE-2021-26117</b> | Oracle FLEXCUBE Private Banking                                  | Financial Planning (Apache ActiveMQ)    | HTTP     | Yes                           | 9.8          | Network       | Low               |
| <b>CVE-2020-5413</b>  | Oracle FLEXCUBE Private Banking                                  | Financial Planning (Spring Integration) | HTTP     | Yes                           | 9.8          | Network       | Low               |
| <b>CVE-2020-11998</b> | Oracle FLEXCUBE Private Banking                                  | Financial Planning (Apache ActiveMQ)    | HTTP     | Yes                           | 9.8          | Network       | Low               |
| <b>CVE-2020-27218</b> | Oracle FLEXCUBE Private Banking                                  | Financial Planning (Eclipse Jetty)      | HTTP     | Yes                           | 9.4          | Network       | Low               |
| <b>CVE-2020-24750</b> | Oracle Banking Liquidity Management                              | Onboarding (jackson-databind)           | HTTP     | Yes                           | 8.1          | Network       | High              |
| <b>CVE-2020-25649</b> | Oracle Banking Treasury Management                               | Accounting (jackson-databind)           | HTTP     | Yes                           | 7.5          | Network       | Low               |
| <b>CVE-2020-11979</b> | Oracle Banking Treasury Management                               | Capital Workflow (Apache Ant)           | HTTP     | Yes                           | 7.5          | Network       | Low               |
| <b>CVE-2020-11979</b> | Oracle Financial Services Analytical Applications Infrastructure | Rate Management (Apache Ant)            | HTTP     | Yes                           | 7.5          | Network       | Low               |
| <b>CVE-2020-11979</b> | Oracle FLEXCUBE Private Banking                                  | Order Management (Apache Ant)           | HTTP     | Yes                           | 7.5          | Network       | Low               |
| <b>CVE-2020-8203</b>  | Oracle Banking Liquidity Management                              | DashBoard (Lodash)                      | HTTP     | Yes                           | 7.4          | Network       | High              |

| CVE#                  | Product  | Component                             | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                   |
|-----------------------|--|---------------------------------------|----------|-------------------------------|--------------|---------------|-------------------|
|                       |  |                                       |          |                               | Base Score   | Attack Vector | Attack Complexity |
| <b>CVE-2019-10086</b> | Oracle Financial Services Revenue Management and Billing Analytics | Dashboards (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3          | Network       | Low               |
| <b>CVE-2020-7712</b>  | Oracle Financial Services Regulatory Reporting with AgileREPORTER  | Reports (Apache ZooKeeper)            | HTTP     | No                            | 7.2          | Network       | Low               |
| <b>CVE-2020-27193</b> | Oracle Banking Party Management                                    | Web UI (CKEditor)                     | HTTP     | Yes                           | 6.1          | Network       | Low               |
| <b>CVE-2020-27193</b> | Oracle Financial Services Analytical Applications Infrastructure   | Rate Management (CKEditor)            | HTTP     | Yes                           | 6.1          | Network       | Low               |
| <b>CVE-2020-11022</b> | Oracle Financial Services Revenue Management and Billing Analytics | Dashboards (jQuery)                   | HTTP     | Yes                           | 6.1          | Network       | Low               |
| <b>CVE-2021-2323</b>  | Oracle FLEXCUBE Universal Banking                                  | Flex-Branch                           | HTTP     | Yes                           | 5.9          | Network       | High              |
| <b>CVE-2020-11987</b> | Oracle FLEXCUBE Universal Banking                                  | General Ledger (Apache Batik)         | HTTP     | Yes                           | 5.3          | Network       | Low               |
| <b>CVE-2021-2324</b>  | Oracle FLEXCUBE Universal Banking                                  | Loans And Deposits                    | HTTP     | No                            | 4.6          | Network       | Low               |
| <b>CVE-2021-2448</b>  | Oracle Financial Services Crime and Compliance                     | Reports                               | None     | No                            | 3.7          | Local         | High              |

| CVE# | Product           | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                |
|------|-------------------|-----------|----------|-------------------------------|--------------|---------------|----------------|
|      |                   |           |          |                               | Base Score   | Attack Vector | Attack Complex |
|      | Investigation Hub |           |          |                               |              |               |                |

### Additional CVEs addressed are:

- The patch for CVE-2020-11022 also addresses CVE-2020-11023.
- The patch for CVE-2020-11998 also addresses CVE-2020-11973 and CVE-2020-1941.
- 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-2020-27193 also addresses CVE-2021-26271 and CVE-2021-26272.
- The patch for CVE-2020-27218 also addresses CVE-2020-27216.
- The patch for CVE-2020-5413 also addresses CVE-2019-10086 and CVE-2020-9489.
- 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-2021-26117 also addresses CVE-2020-11973 and CVE-2020-1941.

## Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Food and Beverage Applications. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none 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 |
| <b>CVE-2021-2395</b> | Oracle Hospitality Reporting and Analytics | iCare, Configuration | HTTP     | No                            | 8.1                  | Network       | Low            | Low         |

| CVE#                 | Product                                | Component                         | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|----------------------|--|-----------------------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
|                      |  |                                   |          |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2021-3156</b> | MICROS Compact Workstation 3           | Workstation 310 (Sudo)            | None     | No                            | 7.8                  | Local         | Low            | Low         |
| <b>CVE-2021-3156</b> | MICROS ES400 Series                    | Express Station 4 (Sudo)          | None     | No                            | 7.8                  | Local         | Low            | Low         |
| <b>CVE-2021-3156</b> | MICROS Kitchen Display System Hardware | Kitchen Display System 210 (Sudo) | None     | No                            | 7.8                  | Local         | Low            | Low         |
| <b>CVE-2021-3156</b> | MICROS Workstation 5A                  | Workstation 5A (Sudo)             | None     | No                            | 7.8                  | Local         | Low            | Low         |
| <b>CVE-2021-3156</b> | MICROS Workstation 6                   | Workstation 6 (Sudo)              | None     | No                            | 7.8                  | Local         | Low            | Low         |

## Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 48 new security patches for Oracle Fusion Middleware. 35 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security updates are not listed in the Oracle Fusion Middleware risk matrix. However, since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the Critical Patch Update July 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 July 2021 Patch Availability Document for Oracle Products, [My Oracle Support Note 2773670.1](#).

| CVE#                  | Product   | Component                                       | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 F |               |                |           |
|-----------------------|---|---|----------|-------------------------------|--------------------|---------------|----------------|-----------|
|                       |   |   |          |                               | Base Score         | Attack Vector | Attack Complex | Priv Req' |
| <b>CVE-2021-21345</b> | Oracle BAM (Business Activity Monitoring)       | General (XStream)                               | HTTP     | No                            | 9.9                | Network       | Low            | Low       |
| <b>CVE-2021-21345</b> | Oracle WebCenter Portal                         | Security Framework (XStream)                    | HTTP     | No                            | 9.9                | Network       | Low            | Low       |
| <b>CVE-2021-2456</b>  | Oracle Business Intelligence Enterprise Edition | Analytics Web General                           | HTTP     | Yes                           | 9.8                | Network       | Low            | Non       |
| <b>CVE-2019-17195</b> | Oracle Data Integrator                          | Runtime Java agent for ODI (Nimbus JOSE+JWT)    | HTTP     | Yes                           | 9.8                | Network       | Low            | Non       |
| <b>CVE-2020-10683</b> | Oracle JDeveloper                               | Oracle JDeveloper (dom4j)                       | HTTP     | Yes                           | 9.8                | Network       | Low            | Non       |
| <b>CVE-2020-28052</b> | Oracle WebCenter Portal                         | Security Framework (Bouncy Castle Java Library) | HTTPS    | Yes                           | 9.8                | Network       | Low            | Non       |
| <b>CVE-2021-2394</b>  | Oracle WebLogic Server                          | Core  | T3, IIOP | Yes                           | 9.8                | Network       | Low            | Non       |
| <b>CVE-2021-2397</b>  | Oracle WebLogic Server                          | Core  | T3, IIOP | Yes                           | 9.8                | Network       | Low            | Non       |
| <b>CVE-2021-2382</b>  | Oracle WebLogic Server                          | Security  | T3, IIOP | Yes                           | 9.8                | Network       | Low            | Non       |

| CVE#                  | Product                        | Component                  | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 F |               |                |           |
|-----------------------|--------------------------------|----------------------------|----------|-------------------------------|--------------------|---------------|----------------|-----------|
|                       |                                |                            |          |                               | Base Score         | Attack Vector | Attack Complex | Priv Req' |
| <b>CVE-2021-2392</b>  | Oracle BI Publisher            | BI Publisher Security      | HTTP     | No                            | 8.8                | Network       | Low            | Low       |
| <b>CVE-2021-2396</b>  | Oracle BI Publisher            | E-Business Suite - XDO     | HTTP     | No                            | 8.8                | Network       | Low            | Low       |
| <b>CVE-2021-2391</b>  | Oracle BI Publisher            | Scheduler                  | HTTP     | No                            | 8.8                | Network       | Low            | Low       |
| <b>CVE-2020-5421</b>  | Oracle Enterprise Data Quality | General (Spring Framework) | HTTP     | No                            | 8.8                | Network       | Low            | Low       |
| <b>CVE-2021-2428</b>  | Oracle Coherence               | Core                       | T3, IIOP | Yes                           | 8.1                | Network       | High           | Non       |
| <b>CVE-2021-2458</b>  | Identity Manager               | Identity Console           | HTTP     | No                            | 7.6                | Network       | Low            | Low       |
| <b>CVE-2021-2400</b>  | Oracle BI Publisher            | E-Business Suite - XDO     | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2371</b>  | Oracle Coherence               | Core                       | T3, IIOP | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2344</b>  | Oracle Coherence               | Core                       | T3, IIOP | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2020-25649</b> | Oracle GoldenGate              | Application Adapters       | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |

| CVE#                  | Product                             | Component   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 F |               |                |           |
|-----------------------|-------------------------------------|---|----------|-------------------------------|--------------------|---------------|----------------|-----------|
|                       |                                     |   |          |                               | Base Score         | Attack Vector | Attack Complex | Priv Req' |
|                       | Application Adapters                | (jackson-databind)  |          |                               |                    |               |                |           |
| <b>CVE-2019-12402</b> | Oracle JDeveloper                   | Oracle JDeveloper (Apache Commons Compress)               | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-25122</b> | Oracle Managed File Transfer        | MFT Runtime Server (Apache Tomcat)                        | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2378</b>  | Oracle WebLogic Server              | Core  | T3, IIOP | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2376</b>  | Oracle WebLogic Server              | Web Services  | T3, IIOP | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2015-0254</b>  | Oracle WebLogic Server              | Third Party Tools (Apache Standard Taglibs)               | HTTP     | Yes                           | 7.3                | Network       | Low            | Non       |
| <b>CVE-2019-10086</b> | Real-Time Decisions (RTD) Solutions | WLS Deployment Template for RT (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3                | Network       | Low            | Non       |
| <b>CVE-2021-2450</b>  | Oracle Outside In Technology        | Outside In Filters  | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2451</b>  | Oracle Outside In Technology        | Outside In Filters  | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |

| CVE#                  | Product                      | Component                                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 F |               |                |           |
|-----------------------|------------------------------|--|----------|-------------------------------|--------------------|---------------|----------------|-----------|
|                       |                              |  |          |                               | Base Score         | Attack Vector | Attack Complex | Priv Req' |
| <b>CVE-2021-2419</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2420</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2423</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2449</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2452</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2430</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2431</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2453</b>  | Oracle Outside In Technology | Outside In Filters                           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2020-1945</b>  | Oracle Data Integrator       | Install, config, upgrade (Apache Ant)        | None     | No                            | 6.3                | Local         | High           | Low       |
| <b>CVE-2019-11358</b> | Identity Manager             | UI Platform (jQuery)                         | HTTP     | Yes                           | 6.1                | Network       | Low            | Non       |
| <b>CVE-2019-12415</b> | Oracle JDeveloper            | OAM (Apache POI)                             | None     | No                            | 5.5                | Local         | Low            | Low       |
| <b>CVE-2021-27906</b> | Oracle Outside In Technology | Outside In Clean Content SDK (Apache PDFBox) | None     | No                            | 5.5                | Local         | Low            | Non       |
| <b>CVE-2021-2457</b>  | Identity Manager             | Request Management                           | HTTP     | Yes                           | 5.3                | Network       | Low            | Non       |

| CVE#                  | Product                            | Component                                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 F |                  |                |           |
|-----------------------|------------------------------------|--|----------|-------------------------------|--------------------|------------------|----------------|-----------|
|                       |                                    |  |          |                               | Base Score         | Attack Vector    | Attack Complex | Priv Req' |
|                       |                                    | & Workflow                                   |          |                               |                    |                  |                |           |
| <b>CVE-2021-2401</b>  | Oracle BI Publisher                | E-Business Suite - XDO                       | HTTP     | Yes                           | 5.3                | Network          | Low            | Non       |
| <b>CVE-2020-13956</b> | Oracle Data Integrator             | Install, config, upgrade (Apache HttpClient) | HTTP     | Yes                           | 5.3                | Network          | Low            | Non       |
| <b>CVE-2020-11987</b> | Oracle Enterprise Repository       | Security Subsystem - 12c (Apache Batik)      | HTTP     | Yes                           | 5.3                | Network          | Low            | Non       |
| <b>CVE-2020-11987</b> | Oracle Fusion Middleware MapViewer | Install (Apache Batik)                       | HTTP     | Yes                           | 5.3                | Network          | Low            | Non       |
| <b>CVE-2021-2403</b>  | Oracle WebLogic Server             | Core   | HTTP     | Yes                           | 5.3                | Network          | Low            | Non       |
| <b>CVE-2021-2358</b>  | Oracle Access Manager              | Rest interfaces for Access Mgr               | HTTPS    | No                            | 4.9                | Network          | Low            | High      |
| <b>CVE-2020-8908</b>  | Oracle Data Integrator             | Install, config, upgrade (Guava)             | None     | No                            | 3.3                | Local            | Low            | Low       |
| <b>CVE-2020-2555</b>  | Oracle Access Manager              | Installation Component (Oracle Coherence)    | HTTPS    | No                            | 3.1                | Adjacent Network | High           | High      |

### 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-2020-1945 also addresses CVE-2020-11979.
- The patch for CVE-2020-5421 also addresses CVE-2021-22118.
- The patch for CVE-2021-21345 also addresses CVE-2019-10173, 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-2021-2397 also addresses CVE-2020-14756.
- The patch for CVE-2021-25122 also addresses CVE-2021-25329.
- The patch for CVE-2021-27906 also addresses CVE-2021-27807.

## Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Hospitality 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 | In |
| <b>CVE-2021-21290</b> | Oracle Hospitality Suite8 | Spa and Leisure (Netty) | None     | No                            | 5.5                   | Local         | Low            | Low         | M  |

## Oracle Hyperion Risk Matrix

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

| CVE#                  | Product                            | Component   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |         |
|-----------------------|------------------------------------|---|----------|-------------------------------|------------------|---------------|----------------|---------|
|                       |                                    |   |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Rec |
| <b>CVE-2019-2729</b>  | Hyperion Infrastructure Technology | Installation and Configuration (Oracle WebLogic Server) | HTTP     | Yes                           | 9.8              | Network       | Low            | Noi     |
| <b>CVE-2019-17566</b> | Hyperion Financial Reporting       | Installation (Apache Batik)                             | HTTP     | Yes                           | 7.5              | Network       | Low            | Noi     |
| <b>CVE-2017-14735</b> | Hyperion Infrastructure Technology | Common Security (AntiSamy)                              | HTTP     | Yes                           | 6.1              | Network       | Low            | Noi     |
| <b>CVE-2021-2445</b>  | Hyperion Infrastructure Technology | Lifecycle Management                                    | HTTP     | No                            | 5.7              | Network       | High           | Hiğ     |
| <b>CVE-2021-2347</b>  | Hyperion Infrastructure Technology | Lifecycle Management                                    | HTTP     | No                            | 5.2              | Network       | Low            | Hiğ     |
| <b>CVE-2021-2439</b>  | Oracle Hyperion BI+                | UI and Visualization                                    | HTTP     | Yes                           | 4.3              | Network       | Low            | Noi     |

### Additional CVEs addressed are:

- The patch for CVE-2019-2729 also addresses CVE-2019-2725.

## Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Insurance 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 |               |                |         |
|-----------------------|------------------|----------------------|----------|-------------------------------|------------------|---------------|----------------|---------|
|                       |                  |                      |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Rec |
| <b>CVE-2021-22112</b> | Oracle Insurance | Architecture (Spring | HTTP     | No                            | 8.8              | Network       | Low            | Lc      |

| CVE#                  | Product                                     | Component                               | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |       |
|-----------------------|---|---|----------|-------------------------------|------------------|---------------|----------------|-------|
|                       |   |   |          |                               | Base Score       | Attack Vector | Attack Complex | Pr Re |
|                       | Policy Administration                       | Security)                               |          |                               |                  |               |                |       |
| <b>CVE-2020-35490</b> | Oracle Insurance Policy Administration J2EE | Security Information (jackson-databind) | HTTP     | Yes                           | 8.1              | Network       | High           | Nc    |
| <b>CVE-2020-25649</b> | Oracle Insurance Policy Administration      | Architecture (jackson-databind)         | HTTP     | Yes                           | 7.5              | Network       | Low            | Nc    |
| <b>CVE-2020-25649</b> | Oracle Insurance Rules Palette              | Architecture (jackson-databind)         | HTTP     | Yes                           | 7.5              | Network       | Low            | Nc    |

### Additional CVEs addressed are:

- The patch for CVE-2020-35490 also addresses CVE-2020-35491.

## Oracle Java SE Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Java SE. 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 RISI |               |                |             |
|-----------------------|-----------------------------------|--|----------|-------------------------------|-----------------------|---------------|----------------|-------------|
|                       |                                   |  |          |                               | Base Score            | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2021-29921</b> | Oracle GraalVM Enterprise Edition | Python interpreter and runtime (CPython) | Multiple | Yes                           | 9.8                   | Network       | Low            | None        |
| <b>CVE-2021-2388</b>  | Java SE, Oracle GraalVM           | Hotspot                                  | Multiple | Yes                           | 7.5                   | Network       | High           | None        |

| CVE#                  | Product                                    | Component                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|-----------------------|--|------------------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
|                       |  |                              |          |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
|                       | Enterprise Edition                         |                              |          |                               |                      |               |                |             |
| <b>CVE-2020-28928</b> | Oracle GraalVM Enterprise Edition          | LLVM Interpreter (musl libc) | None     | No                            | 5.5                  | Local         | Low            | Low         |
| <b>CVE-2021-2369</b>  | Java SE, Oracle GraalVM Enterprise Edition | Library                      | Multiple | Yes                           | 4.3                  | Network       | Low            | None        |
| <b>CVE-2021-2432</b>  | Java SE                                    | JNDI                         | Multiple | Yes                           | 3.7                  | Network       | High           | None        |
| <b>CVE-2021-2341</b>  | Java SE, Oracle GraalVM Enterprise Edition | Networking                   | Multiple | Yes                           | 3.1                  | Network       | High           | None        |

**Notes:**

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability 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.

## Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 9 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 3.1 |               |                |        |
|-----------------------|---------------------------------------|--|----------|-------------------------------|------------------|---------------|----------------|--------|
|                       |                                       |  |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Re |
| <b>CVE-2019-13990</b> | JD Edwards EnterpriseOne Orchestrator | E1 IOT Orchestrator Security (Quartz)          | HTTP     | Yes                           | 9.8              | Network       | Low            | No     |
| <b>CVE-2019-17195</b> | JD Edwards EnterpriseOne Orchestrator | E1 IOT Orchestrator Security (Nimbus JOSE+JWT) | HTTP     | Yes                           | 9.8              | Network       | Low            | No     |
| <b>CVE-2019-17195</b> | JD Edwards EnterpriseOne Tools        | Business Logic Inf SEC (Nimbus JOSE+JWT)       | HTTP     | Yes                           | 9.8              | Network       | Low            | No     |
| <b>CVE-2019-17195</b> | JD Edwards EnterpriseOne Tools        | Web Runtime SEC (Nimbus JOSE+JWT)              | HTTP     | Yes                           | 9.8              | Network       | Low            | No     |
| <b>CVE-2020-25649</b> | JD Edwards EnterpriseOne Orchestrator | E1 IOT Orchestrator Security                   | HTTP     | Yes                           | 7.5              | Network       | Low            | No     |

| CVE#                  | Product                        | Component   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |        |
|-----------------------|--------------------------------|---|----------|-------------------------------|------------------|---------------|----------------|--------|
|                       |                                |   |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Re |
|                       |                                | (jackson-databind)                                |          |                               |                  |               |                |        |
| <b>CVE-2020-25649</b> | JD Edwards EnterpriseOne Tools | Monitoring and Diagnostics SEC (jackson-databind) | HTTP     | Yes                           | 7.5              | Network       | Low            | No     |
| <b>CVE-2020-25649</b> | JD Edwards EnterpriseOne Tools | Web Runtime SEC (jackson-databind)                | HTTP     | Yes                           | 7.5              | Network       | Low            | No     |
| <b>CVE-2021-2375</b>  | JD Edwards EnterpriseOne Tools | Web Runtime                                       | HTTP     | Yes                           | 6.1              | Network       | Low            | No     |
| <b>CVE-2021-2373</b>  | JD Edwards EnterpriseOne Tools | Web Runtime                                       | HTTP     | No                            | 5.4              | Network       | Low            | Lc     |

#### Additional CVEs addressed are:

- The patch for CVE-2020-25649 also addresses CVE-2020-36189.

## Oracle MySQL Risk Matrix

This Critical Patch Update contains 41 new security patches for Oracle MySQL. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE#                  | Product       | Component                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |        |
|-----------------------|---------------|------------------------------|----------|-------------------------------|------------------|---------------|----------------|--------|
|                       |               |                              |          |                               | Base Score       | Attack Vector | Attack Complex | Pri Re |
| <b>CVE-2021-22884</b> | MySQL Cluster | Cluster: JS module (Node.js) | Multiple | Yes                           | 8.8              | Network       | Low            | N      |

| CVE#                  | Product                  | Component                           | Protocol       | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |                     |
|-----------------------|--------------------------|-------------------------------------|----------------|-------------------------------|------------------|---------------|-------------------|---------------------|
|                       |                          |                                     |                |                               | Base Score       | Attack Vector | Attack Complexity | Privileges Required |
| <b>CVE-2021-22901</b> | MySQL Server             | Server: Packaging (curl)            | Multiple       | Yes                           | 8.1              | Network       | High              | None                |
| <b>CVE-2021-25122</b> | MySQL Enterprise Monitor | Monitoring: General (Apache Tomcat) | HTTPS/2        | Yes                           | 7.5              | Network       | Low               | None                |
| <b>CVE-2019-17543</b> | MySQL Server             | Server: Compiling (LZ4)             | MySQL Protocol | No                            | 7.5              | Network       | High              | Low                 |
| <b>CVE-2021-3450</b>  | MySQL Connectors         | Connector/C++ (OpenSSL)             | MySQL Protocol | Yes                           | 7.4              | Network       | High              | None                |
| <b>CVE-2021-3450</b>  | MySQL Connectors         | Connector/ODBC (OpenSSL)            | MySQL Protocol | Yes                           | 7.4              | Network       | High              | None                |
| <b>CVE-2021-3450</b>  | MySQL Enterprise Monitor | Monitoring: General (OpenSSL)       | HTTPS          | Yes                           | 7.4              | Network       | High              | None                |
| <b>CVE-2021-2417</b>  | MySQL Server             | Server: GIS                         | MySQL Protocol | No                            | 6.0              | Network       | Low               | High                |
| <b>CVE-2021-2389</b>  | MySQL Server             | InnoDB                              | MySQL Protocol | Yes                           | 5.9              | Network       | High              | None                |
| <b>CVE-2021-2390</b>  | MySQL Server             | InnoDB                              | MySQL Protocol | Yes                           | 5.9              | Network       | High              | None                |
| <b>CVE-2021-2429</b>  | MySQL Server             | InnoDB                              | MySQL Protocol | Yes                           | 5.9              | Network       | High              | None                |
| <b>CVE-2021-2356</b>  | MySQL Server             | Server: Replication                 | MySQL Protocol | No                            | 5.9              | Network       | High              | Low                 |
| <b>CVE-2021-2385</b>  | MySQL Server             | Server: Replication                 | MySQL Protocol | No                            | 5.0              | Network       | High              | High                |

| CVE#                 | Product      | Component         | Protocol       | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |                     |
|----------------------|--------------|-------------------|----------------|-------------------------------|------------------|---------------|-------------------|---------------------|
|                      |              |                   |                |                               | Base Score       | Attack Vector | Attack Complexity | Privileges Required |
| <b>CVE-2021-2339</b> | MySQL Server | Server: DDL       | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2352</b> | MySQL Server | Server: DDL       | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2399</b> | MySQL Server | Server: DDL       | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2370</b> | MySQL Server | Server: DML       | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2440</b> | MySQL Server | Server: DML       | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2354</b> | MySQL Server | Server: Federated | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2402</b> | MySQL Server | Server: Locking   | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2342</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2357</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2367</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2412</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2383</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2384</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2387</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2444</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2410</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2418</b> | MySQL Server | Server: Optimizer | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |

| CVE#                 | Product       | Component                | Protocol       | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                   |                     |
|----------------------|---------------|--------------------------|----------------|-------------------------------|------------------|---------------|-------------------|---------------------|
|                      |               |                          |                |                               | Base Score       | Attack Vector | Attack Complexity | Privileges Required |
| <b>CVE-2021-2425</b> | MySQL Server  | Server: Optimizer        | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2426</b> | MySQL Server  | Server: Optimizer        | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2427</b> | MySQL Server  | Server: Optimizer        | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2437</b> | MySQL Server  | Server: Optimizer        | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2441</b> | MySQL Server  | Server: Optimizer        | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2422</b> | MySQL Server  | Server: PS               | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2424</b> | MySQL Server  | Server: Stored Procedure | MySQL Protocol | No                            | 4.9              | Network       | Low               | None                |
| <b>CVE-2021-2372</b> | MySQL Server  | InnoDB                   | MySQL Protocol | No                            | 4.4              | Network       | High              | None                |
| <b>CVE-2021-2374</b> | MySQL Server  | InnoDB                   | None           | No                            | 4.1              | Local         | High              | None                |
| <b>CVE-2021-2411</b> | MySQL Cluster | Cluster: JS module       | Multiple       | Yes                           | 3.7              | Network       | High              | None                |
| <b>CVE-2021-2340</b> | MySQL Server  | Server: Memcached        | MySQL Protocol | No                            | 2.7              | Network       | Low               | None                |

#### Additional CVEs addressed are:

- The patch for CVE-2021-22884 also addresses CVE-2021-22883 and CVE-2021-23840.
- The patch for CVE-2021-22901 also addresses CVE-2021-22897 and CVE-2021-22898.
- The patch for CVE-2021-25122 also addresses CVE-2021-25329.
- The patch for CVE-2021-3450 also addresses CVE-2021-3449.

## Oracle PeopleSoft Risk Matrix

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

| CVE#                  | Product                                     | Component                             | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |          |
|-----------------------|---|---------------------------------------|----------|-------------------------------|------------------|---------------|----------------|----------|
|                       |   |                                       |          |                               | Base Score       | Attack Vector | Attack Complex | Priv Req |
| <b>CVE-2019-17195</b> | PeopleSoft Enterprise PeopleTools           | REST Services (Nimbus JOSE+JWT)       | HTTP     | Yes                           | 9.8              | Network       | Low            | Nor      |
| <b>CVE-2021-27568</b> | PeopleSoft Enterprise PeopleTools           | REST Services (netplex json-smart-v1) | HTTP     | Yes                           | 9.1              | Network       | Low            | Nor      |
| <b>CVE-2021-22884</b> | PeopleSoft Enterprise PeopleTools           | Elastic Search (Node.js)              | HTTP     | Yes                           | 7.5              | Network       | High           | Nor      |
| <b>CVE-2021-3450</b>  | PeopleSoft Enterprise PeopleTools           | Security (OpenSSL)                    | TLS      | Yes                           | 7.4              | Network       | High           | Nor      |
| <b>CVE-2020-7017</b>  | PeopleSoft Enterprise PeopleTools           | Elastic Search (Kibana)               | HTTP     | No                            | 6.7              | Network       | High           | Low      |
| <b>CVE-2021-2421</b>  | PeopleSoft Enterprise CS Campus Community   | Integration and Interfaces            | HTTP     | No                            | 6.5              | Network       | Low            | Low      |
| <b>CVE-2021-2404</b>  | PeopleSoft Enterprise HCM Candidate Gateway | e-mail notification                   | HTTP     | Yes                           | 6.5              | Network       | Low            | Nor      |
| <b>CVE-2021-2455</b>  | PeopleSoft Enterprise HCM Shared Components | Person Search                         | HTTP     | No                            | 6.5              | Network       | Low            | High     |
| <b>CVE-2021-2408</b>  | PeopleSoft Enterprise PT PeopleTools        | Notification Configuration            | HTTP     | Yes                           | 6.1              | Network       | Low            | Nor      |

| CVE#                  | Product                              | Component                         | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |          |
|-----------------------|--------------------------------------|-----------------------------------|----------|-------------------------------|------------------|---------------|----------------|----------|
|                       |                                      |                                   |          |                               | Base Score       | Attack Vector | Attack Complex | Priv Req |
| <b>CVE-2021-21290</b> | PeopleSoft Enterprise PeopleTools    | Elastic Search (Netty)            | None     | No                            | 5.5              | Local         | Low            | Low      |
| <b>CVE-2021-2407</b>  | PeopleSoft Enterprise PeopleTools    | Portal                            | HTTP     | Yes                           | 5.3              | Network       | Low            | None     |
| <b>CVE-2020-13956</b> | PeopleSoft Enterprise PT PeopleTools | Cloud Manager (Apache HttpClient) | HTTP     | Yes                           | 5.3              | Network       | Low            | None     |
| <b>CVE-2021-2377</b>  | PeopleSoft Enterprise PeopleTools    | SQR                               | HTTP     | No                            | 4.3              | Network       | Low            | Low      |
| <b>CVE-2020-8908</b>  | PeopleSoft Enterprise PeopleTools    | Elastic Search (Google Guava)     | None     | No                            | 3.3              | Local         | Low            | Low      |

#### Additional CVEs addressed are:

- The patch for CVE-2020-7017 also addresses CVE-2020-7016.
- The patch for CVE-2021-22884 also addresses CVE-2018-7160 and CVE-2021-22883.
- The patch for CVE-2021-3450 also addresses CVE-2021-23839, CVE-2021-23840, CVE-2021-23841 and CVE-2021-3449.

## Oracle Policy Automation Risk Matrix

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

| CVE#                  | Product                  | Component             | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|-----------------------|--------------------------|-----------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
|                       |                          |                       |          |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2019-17195</b> | Oracle Policy Automation | Hub (Nimbus JOSE+JWT) | HTTP     | Yes                           | 9.8                  | Network       | Low            | None        |

## Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 23 new security patches for Oracle Retail Applications. 15 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE#                  | Product   | Component   | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                |  |
|-----------------------|---|---|----------|-------------------------------|--------------|---------------|----------------|--|
|                       |   |   |          |                               | Base Score   | Attack Vector | Attack Complex |  |
| <b>CVE-2021-21345</b> | Oracle Retail Xstore Point of Service                         | Xenvironment (XStream)                            | HTTP     | No                            | 9.9          | Network       | Low            |  |
| <b>CVE-2019-0219</b>  | Oracle Retail Xstore Point of Service                         | Xenvironment (Apache cordova-plugin-inappbrowser) | HTTP     | Yes                           | 9.8          | Network       | Low            |  |
| <b>CVE-2020-5421</b>  | Oracle Retail Customer Management and Segmentation Foundation | Promotions (Spring Framework)                     | HTTP     | No                            | 8.8          | Network       | Low            |  |
| <b>CVE-2020-5421</b>  | Oracle Retail Merchandising System                            | Foundation (Spring Framework)                     | HTTP     | No                            | 8.8          | Network       | Low            |  |
| <b>CVE-2021-22118</b> | Oracle Retail Financial Integration                           | PeopleSoft Integration Bugs (Spring Framework)    | None     | No                            | 7.8          | Local         | Low            |  |

| CVE#                  | Product                               | Component                                | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                |
|-----------------------|---------------------------------------|--|----------|-------------------------------|--------------|---------------|----------------|
|                       |                                       |  |          |                               | Base Score   | Attack Vector | Attack Complex |
| <b>CVE-2021-22118</b> | Oracle Retail Integration Bus         | RIB Kernal (Spring Framework)            | None     | No                            | 7.8          | Local         | Low            |
| <b>CVE-2021-22118</b> | Oracle Retail Order Broker            | System Administration (Spring Framework) | None     | No                            | 7.8          | Local         | Low            |
| <b>CVE-2020-5398</b>  | Oracle Retail Back Office             | Pricing (Spring Framework)               | HTTP     | Yes                           | 7.5          | Network       | High           |
| <b>CVE-2020-5398</b>  | Oracle Retail Central Office          | Transaction Tracker (Spring Framework)   | HTTP     | Yes                           | 7.5          | Network       | High           |
| <b>CVE-2020-11979</b> | Oracle Retail Merchandising System    | Procurement (Apache Ant)                 | HTTP     | Yes                           | 7.5          | Network       | Low            |
| <b>CVE-2020-5398</b>  | Oracle Retail Point-of-Service        | Queue Management (Spring Framework)      | HTTP     | Yes                           | 7.5          | Network       | High           |
| <b>CVE-2020-5398</b>  | Oracle Retail Returns Management      | Main Dashboard (Spring Framework)        | HTTP     | Yes                           | 7.5          | Network       | High           |
| <b>CVE-2020-25649</b> | Oracle Retail Service Backbone        | RSB Installation (jackson-databind)      | HTTP     | Yes                           | 7.5          | Network       | Low            |
| <b>CVE-2020-17527</b> | Oracle Retail Xstore Point of Service | Xenvironment (Apache Tomcat)             | HTTP     | Yes                           | 7.5          | Network       | Low            |
| <b>CVE-2020-8277</b>  | Oracle Retail Xstore Point of Service | Xenvironment (Node.js)                   | HTTP     | Yes                           | 7.5          | Network       | Low            |
| <b>CVE-2020-25649</b> | Oracle Retail Xstore Point of         | Xenvironment (jackson-                   | HTTP     | Yes                           | 7.5          | Network       | Low            |

| CVE#                  | Product   | Component                                    | Protocol | Remote Exploit without Auth.? | CVSS VERSION |               |                |
|-----------------------|---|--|----------|-------------------------------|--------------|---------------|----------------|
|                       |   |  |          |                               | Base Score   | Attack Vector | Attack Complex |
|                       | Service   | databind)                                    |          |                               |              |               |                |
| <b>CVE-2020-25638</b> | Oracle Retail Customer Management and Segmentation Foundation | Segment (Hibernate)                          | HTTP     | Yes                           | 7.4          | Network       | High           |
| <b>CVE-2019-10086</b> | Oracle Retail Merchandising System                            | Foundation (Apache Commons BeanUtils)        | HTTP     | Yes                           | 7.3          | Network       | Low            |
| <b>CVE-2019-10086</b> | Oracle Retail Price Management                                | Manage Allocation (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3          | Network       | Low            |
| <b>CVE-2020-5421</b>  | Oracle Retail Customer Engagement                             | Internal Operations (Spring Framework)       | HTTP     | No                            | 6.5          | Network       | High           |
| <b>CVE-2021-27807</b> | Oracle Retail Customer Management and Segmentation Foundation | Segment (Apache PDFbox)                      | HTTP     | No                            | 6.5          | Network       | High           |
| <b>CVE-2020-11987</b> | Oracle Retail Order Broker                                    | Store Connect (Apache Batik)                 | HTTP     | Yes                           | 5.3          | Network       | Low            |
| <b>CVE-2020-11987</b> | Oracle Retail Order Management System Cloud Service           | Internal Operations (Apache Batik)           | HTTP     | Yes                           | 5.3          | Network       | Low            |

#### Additional CVEs addressed are:

- The patch for CVE-2020-11987 also addresses CVE-2019-17566.
- 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-2020-5398 also addresses CVE-2020-5397 and CVE-2020-5421.
- The patch for CVE-2020-5421 also addresses CVE-2020-5413.
- The patch for CVE-2020-8277 also addresses CVE-2020-8174.
- 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 and CVE-2021-21351.
- The patch for CVE-2021-27807 also addresses CVE-2021-27906.

## Oracle Siebel CRM Risk Matrix

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

| CVE#                  | Product                        | Component                           | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 F |               |                |           |
|-----------------------|--------------------------------|-------------------------------------|----------|-------------------------------|--------------------|---------------|----------------|-----------|
|                       |                                |                                     |          |                               | Base Score         | Attack Vector | Attack Complex | Priv Req' |
| <b>CVE-2020-24750</b> | Siebel Core - Server Framework | Services (jackson-databind)         | HTTP     | Yes                           | 8.1                | Network       | High           | Non       |
| <b>CVE-2020-27216</b> | Siebel Core - Automation       | Test Automation (Eclipse Jetty)     | None     | No                            | 7.8                | Local         | Low            | Low       |
| <b>CVE-2017-5637</b>  | Siebel Core - Server Framework | Cloud Gateway (Zookeeper)           | HTTP     | Yes                           | 7.5                | Network       | Low            | Non       |
| <b>CVE-2021-2338</b>  | Siebel Apps - Marketing        | Email Marketing Stand-Alone         | HTTP     | Yes                           | 6.1                | Network       | Low            | Non       |
| <b>CVE-2021-2368</b>  | Siebel CRM                     | Siebel Core - Server Infrastructure | HTTPS    | Yes                           | 5.9                | Network       | High           | Non       |
| <b>CVE-2021-2353</b>  | Siebel Core - Server Framework | Logging                             | None     | No                            | 4.4                | Local         | Low            | High      |

**Additional CVEs addressed are:**

- The patch for CVE-2017-5637 also addresses CVE-2019-0201 and CVE-2020-11612.
- The patch for CVE-2020-27216 also addresses CVE-2020-27218.

## Oracle Supply Chain Risk Matrix

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

| CVE#                  | Product                                  | Component                                      | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 |               |                |        |
|-----------------------|--|--|----------|-------------------------------|------------------|---------------|----------------|--------|
|                       |  |  |          |                               | Base Score       | Attack Vector | Attack Complex | Prereq |
| <b>CVE-2020-11979</b> | Oracle Agile Engineering Data Management | Installation Issues (Apache Ant)               | HTTP     | Yes                           | 7.5              | Network       | Low            | No     |
| <b>CVE-2020-13935</b> | Oracle Agile Engineering Data Management | Installation Issues (Apache Tomcat)            | HTTP     | Yes                           | 7.5              | Network       | Low            | No     |
| <b>CVE-2012-0881</b>  | Oracle Transportation Management         | UI Infrastructure (Apache Xerces2 Java Parser) | HTTP     | Yes                           | 7.5              | Network       | Low            | No     |
| <b>CVE-2021-26272</b> | Oracle Agile PLM                         | Security (CKEditor)                            | HTTP     | Yes                           | 6.5              | Network       | Low            | No     |
| <b>CVE-2021-24122</b> | Oracle Agile PLM                         | Folders, Files & Attachments (Apache Tomcat)   | HTTP     | Yes                           | 5.9              | Network       | High           | No     |

**Additional CVEs addressed are:**

- The patch for CVE-2020-11979 also addresses CVE-2020-1945.
- The patch for CVE-2020-13935 also addresses CVE-2020-13934.

- The patch for CVE-2021-24122 also addresses CVE-2020-17527, CVE-2021-25122 and CVE-2021-25329.
- The patch for CVE-2021-26272 also addresses CVE-2020-27193 and CVE-2021-26271.

## Oracle Support Tools Risk Matrix

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

| CVE#                  | Product           | Component                     | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RISK ( |               |                |             |       |
|-----------------------|-------------------|-------------------------------|----------|-------------------------------|-------------------------|---------------|----------------|-------------|-------|
|                       |                   |                               |          |                               | Base Score              | Attack Vector | Attack Complex | Privs Req'd | U Int |
| <b>CVE-2020-11023</b> | OSS Support Tools | Diagnostic Assistant (jQuery) | HTTP     | Yes                           | 6.1                     | Network       | Low            | None        | Re    |

### Additional CVEs addressed are:

- The patch for CVE-2020-11023 also addresses CVE-2019-11358 and CVE-2020-11022.

## Oracle Systems Risk Matrix

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

| CVE#                 | Product                                     | Component          | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|----------------------|---|--------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
|                      |   |                    |          |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2017-5461</b> | Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, | XCP Firmware (NSS) | HTTP     | Yes                           | 9.8                  | Network       | Low            | None        |

| CVE#                  | Product  | Component  | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|-----------------------|--|--|----------|-------------------------------|----------------------|---------------|----------------|-------------|
|                       |  |  |          |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
|                       | M12-2S Servers   |  |          |                               |                      |               |                |             |
| <b>CVE-2017-16931</b> | Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers | XCP Firmware (libxml2)                             | HTTP     | Yes                           | 9.8                  | Network       | Low            | None        |
| <b>CVE-2018-7183</b>  | Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers | XCP Firmware (NTP)                                 | NTP      | Yes                           | 9.8                  | Network       | Low            | None        |
| <b>CVE-2021-3177</b>  | Oracle ZFS Storage Appliance Kit                           | Operating System Image                             | Multiple | Yes                           | 9.8                  | Network       | Low            | None        |
| <b>CVE-2020-10683</b> | StorageTek Tape Analytics SW Tool                          | Software (dom4j)                                   | HTTP     | Yes                           | 9.8                  | Network       | Low            | None        |
| <b>CVE-2019-10086</b> | Oracle Solaris Cluster                                     | Application Integration (Apache Commons BeanUtils) | HTTP     | Yes                           | 7.3                  | Network       | Low            | None        |
| <b>CVE-2018-0739</b>  | Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers | XCP Firmware (OpenSSL)                             | TLS      | Yes                           | 6.5                  | Network       | Low            | None        |

| CVE#                 | Product  | Component                   | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RIS |               |                |             |
|----------------------|--|-----------------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
|                      |  |                             |          |                               | Base Score           | Attack Vector | Attack Complex | Privs Req'd |
| <b>CVE-2020-5421</b> | StorageTek Tape Analytics SW Tool                          | Software (Spring Framework) | HTTP     | No                            | 6.5                  | Network       | High           | Low         |
| <b>CVE-2019-3740</b> | StorageTek Tape Analytics SW Tool                          | Software (BSAFE Crypto-J)   | HTTPS    | Yes                           | 6.5                  | Network       | Low            | None        |
| <b>CVE-2016-4429</b> | Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers | XCP Firmware (glibc)        | Multiple | Yes                           | 5.9                  | Network       | High           | None        |
| <b>CVE-2021-2381</b> | Oracle Solaris   | Kernel                      | None     | No                            | 3.9                  | Local         | Low            | Low         |

#### Additional CVEs addressed are:

- The patch for CVE-2018-0739 also addresses CVE-2017-3735, CVE-2018-0737 and CVE-2020-1968.
- The patch for CVE-2018-7183 also addresses CVE-2020-11868.
- The patch for CVE-2019-3740 also addresses CVE-2019-3738 and CVE-2019-3739.
- The patch for CVE-2021-3177 also addresses CVE-2020-27783, CVE-2021-20227, CVE-2021-23839, CVE-2021-23840, CVE-2021-23841, CVE-2021-28041, CVE-2021-29921, CVE-2021-3449, CVE-2021-3450, CVE-2021-3520 and CVE-2021-3560.

## Oracle Virtualization Risk Matrix

This Critical Patch Update contains 6 new security patches for Oracle Virtualization. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE#                 | Product                      | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 RISK |               |                |             |        |
|----------------------|------------------------------|-----------|----------|-------------------------------|-----------------------|---------------|----------------|-------------|--------|
|                      |                              |           |          |                               | Base Score            | Attack Vector | Attack Complex | Privs Req'd | Impact |
| <b>CVE-2021-2447</b> | Oracle Secure Global Desktop | Server    | Multiple | No                            | 9.9                   | Network       | Low            | Low         |        |
| <b>CVE-2021-2446</b> | Oracle Secure Global Desktop | Client    | Multiple | Yes                           | 9.6                   | Network       | Low            | None        | R      |
| <b>CVE-2021-2409</b> | Oracle VM VirtualBox         | Core      | None     | No                            | 8.2                   | Local         | Low            | High        |        |
| <b>CVE-2021-2443</b> | Oracle VM VirtualBox         | Core      | None     | No                            | 7.3                   | Local         | Low            | High        |        |
| <b>CVE-2021-2454</b> | Oracle VM VirtualBox         | Core      | None     | No                            | 7.0                   | Local         | High           | Low         |        |
| <b>CVE-2021-2442</b> | Oracle VM VirtualBox         | Core      | None     | No                            | 6.0                   | Local         | Low            | High        |        |

**Notes:**

1. This vulnerability applies to Solaris x86 and Linux systems only.

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

