Oracle Critical Patch Update Pre-Release Announcement - April 2026

Description

This Critical Patch Update Pre-Release Announcement provides advance information about the Oracle Critical Patch Update for April 2026, which will be released on Tuesday, April 21, 2026. While this Pre-Release Announcement is as accurate as possible at the time of publication, the information it contains may change before publication of the Critical Patch Update Advisory.

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. This Critical Patch Update addresses 483 new security patches. Some of the vulnerabilities addressed in this Critical Patch Update affect multiple products. Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply Critical Patch Update patches as soon as possible.

Executive Summaries

Oracle Database Server Executive Summary

This Critical Patch Update contains 8 new security patches for Oracle Database Products. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Database Server is 7.5.

The Oracle Database Server components and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Database Server, versions 19.3-19.30, 21.3-21.21, 23.4.0-23.26.1

Oracle Adapter for Eclipse RDF4J Executive Summary

This Critical Patch Update contains 2 new security patches for Oracle Adapter for Eclipse RDF4J. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Adapter for Eclipse RDF4J is 7.5.

The Oracle Adapter for Eclipse RDF4J products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Adapter for Eclipse RDF4J, versions 3.12.0, 24.1.0

Oracle Autonomous Health Framework Executive Summary

This Critical Patch Update contains 1 new security patch for Oracle Autonomous Health Framework. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Autonomous Health Framework is 5.9.

The Oracle Autonomous Health Framework products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Autonomous Health Framework, versions 25.11-26.1

Oracle Blockchain Platform Executive Summary

This Critical Patch Update contains 6 new security patches for Oracle Blockchain Platform. 4 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Blockchain Platform is 7.5.

The Oracle Blockchain Platform products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Blockchain Platform, version 24.1.3

Oracle GoldenGate Executive Summary

This Critical Patch Update contains 10 new security patches for Oracle GoldenGate. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle GoldenGate is 7.5.

The Oracle GoldenGate products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle GoldenGate, versions 23.4-23.26.1
- Oracle GoldenGate Big Data and Application Adapters, versions 19.1.0.0.0-19.1.0.0.21, 21.3-21.21, 23.4-23.10
- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.14

Oracle NoSQL Database Executive Summary

This Critical Patch Update contains 1 new security patch for Oracle NoSQL Database. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle NoSQL Database is 5.3.

The Oracle NoSQL Database products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle NoSQL Database, versions 1.6.5, 1.7.0

Oracle REST Data Services Executive Summary

This Critical Patch Update contains 2 new security patches for Oracle REST Data Services. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle REST Data Services is 7.5.

The Oracle REST Data Services products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle REST Data Services, versions 24.2.0, 24.2.1, 24.3.0, 24.3.1, 24.4.0, 25.1.1, 25.2.0, 25.2.1, 25.2.2, 25.2.3, 25.3.0, 25.3.1, 25.4.0

Oracle TimesTen In-Memory Database Executive Summary

This Critical Patch Update contains 1 new security patch for Oracle TimesTen In-Memory Database. This vulnerability is remotely exploitable without authentication, i.e., may be

exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle TimesTen In-Memory Database is 7.4.

The Oracle TimesTen In-Memory Database products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle TimesTen In-Memory Database, versions 18.1.4, 22.1.1

Oracle Commerce Executive Summary

This Critical Patch Update contains 3 new security patches for Oracle Commerce. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Commerce is 8.8.

The Oracle Commerce products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Commerce Guided Search, version 11.4.0

Oracle Communications Executive Summary

This Critical Patch Update contains 137 new security patches for Oracle Communications. 91 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Communications is 9.8.

The Oracle Communications products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Communications Billing and Revenue Management, versions 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0-15.2.0.0.0
- Oracle Communications BRM - Elastic Charging Engine, versions 15.0.0.0-15.0.1.0.0, 15.1.0.0-15.2.0.0.0
- Oracle Communications Cloud Native Core Binding Support Function, version 25.1.200
- Oracle Communications Cloud Native Core Certificate Management, version 25.1.201
- Oracle Communications Cloud Native Core Console, version 25.1.201
- Oracle Communications Cloud Native Core DBTier, version 25.2.100

- Oracle Communications Cloud Native Core Network Exposure Function, versions 24.2.1, 24.2.4
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 25.1.200, 25.2.200
- Oracle Communications Cloud Native Core Network Repository Function, versions 25.1.203, 25.1.204
- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 25.1.100, 25.1.200
- Oracle Communications Cloud Native Core Policy, versions 25.1.200, 25.1.202
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 25.1.200, 25.1.201, 25.2.100
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 25.1.100, 25.1.200, 25.1.202, 25.2.100
- Oracle Communications Cloud Native Core Unified Data Repository, versions 25.1.100, 25.1.200
- Oracle Communications Convergence, version 3.0.3.4.0
- Oracle Communications EAGLE, version 47.0
- Oracle Communications EAGLE Application Processor, versions 17.0-17.1
- Oracle Communications EAGLE Element Management System, version 47.0.0.1.0
- Oracle Communications EAGLE LNP Application Processor, version 11.0
- Oracle Communications Element Manager, versions 9.0.0-9.0.4.0.2
- Oracle Communications Instant Messaging Server, version 10.0.1.8.0
- Oracle Communications LSMS, version 14.0
- Oracle Communications Messaging Server, version 8.1.0.0.0
- Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0, 8.0.0
- Oracle Communications Offline Mediation Controller, versions 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0-15.2.0.0.0
- Oracle Communications Operations Monitor, versions 5.2, 6.0, 6.1
- Oracle Communications Order and Service Management, versions 7.5.0, 8.0.0
- Oracle Communications Performance Intelligence Center, versions 10.5.0.0-10.5.0.2
- Oracle Communications Policy Management, versions 15.0.0.0.0, 15.0.0.1.0
- Oracle Communications Service Catalog and Design, versions 8.0.0.6.0, 8.1.0.5.0, 8.2.0.2.0
- Oracle Communications Session Border Controller, versions 9.3.0, 10.0.0, 10.1.0
- Oracle Communications Session Report Manager, versions 9.0.0.0.0-9.0.4.0.2
- Oracle Communications Unified Assurance, versions 6.1.1-7.0.0

- Oracle Communications Unified Inventory Management, versions 7.5.0-7.5.1, 7.6.0-7.8.0, 8.0.0
- Oracle Enterprise Communications Broker, versions 4.2.0, 5.0.0
- Oracle Enterprise Operations Monitor, version 6.1.0.0.0

Oracle Construction and Engineering Executive Summary

This Critical Patch Update contains 4 new security patches for Oracle Construction and Engineering. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Construction and Engineering is 6.5.

The Oracle Construction and Engineering products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Primavera P6 Enterprise Project Portfolio Management, versions 21.12.0.0-21.12.21.6, 22.12.0.0-22.12.21.1, 23.12.0.0-23.12.18.0, 24.12.0.0-24.12.13.0, 25.12.0.0-25.12.2.0
- Primavera Unifier, versions 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.16, 24.12.0-24.12.13, 25.12.0-25.12.3

Oracle E-Business Suite Executive Summary

This Critical Patch Update contains 18 new security patches for Oracle E-Business Suite. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle E-Business Suite is 9.8.

The Oracle E-Business Suite products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle E-Business Suite, versions 12.2.3-12.2.15, 15.0

Oracle Enterprise Manager Executive Summary

This Critical Patch Update contains 10 new security patches for Oracle Enterprise Manager. 9 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 highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Enterprise Manager is 9.1.

The Oracle Enterprise Manager products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Configuration Manager, versions 13.5, 24.1
- Oracle Enterprise Manager Base Platform, versions 13.5, 24.1
- Oracle Enterprise Manager for Fusion Middleware, versions 13.5, 24.1

Oracle Financial Services Applications Executive Summary

This Critical Patch Update contains 73 new security patches for Oracle Financial Services Applications. 57 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Financial Services Applications is 9.8.

The Oracle Financial Services Applications products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Banking Branch, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Cash Management, version 14.8.2.0.0
- Oracle Banking Collections and Recovery, versions 14.6.0.0.0-14.8.0.0.0
- Oracle Banking Corporate Lending, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Corporate Lending Process Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Credit Facilities Process Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Liquidity Management, versions 14.8.0.0.0, 14.8.1.0.0
- Oracle Banking Origination, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Payments, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Supply Chain Finance, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Trade Finance, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Trade Finance Process Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Virtual Account Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Documaker, versions 12.7.2-13.0.2
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.9, 8.0.8.7, 8.1.2.5

- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.10, 8.1.2.11
- Oracle Financial Services Compliance Studio, version 8.1.2.9
- Oracle Financial Services Customer Screening, version 8.1.2.8.0
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.2.10, 8.1.2.11
- Oracle Financial Services Lending and Leasing, versions 14.8.0.0.0, 14.10.0.0.0-14.12.0.0.0
- Oracle Financial Services Model Management and Governance, version 8.1.2.7
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8
- Oracle Financial Services Transaction Filtering, version 8.1.2.8.0
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Insurance Policy Administration J2EE, versions 11.3.1.0, 11.3.2.0, 12.0.5.0, 12.1.1.0
- Oracle Insurance Policy Administration Operational Data Store for Life and Annuity, version 1.0.2.1

Oracle Fusion Middleware Executive Summary

This Critical Patch Update contains 59 new security patches for Oracle Fusion Middleware. 46 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Fusion Middleware is 9.8.

The Oracle Fusion Middleware products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Access Manager, version 14.1.2.0.0
- Oracle Application Development Framework (ADF), versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Business Activity Monitoring, version 12.2.1.4.0
- Oracle Business Process Management Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Fusion Middleware, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Identity Manager, versions 12.2.1.4.0, 14.1.2.0.0, 14.1.2.1.0
- Oracle Identity Manager Connector, version 12.2.1.4.0
- Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Middleware Common Libraries and Tools, versions 12.2.1.4.0, 14.1.2.0.0

- Oracle Outside In Technology, version 8.5.8
- Oracle Security Service, versions 12.1.3.0.0, 12.2.1.4.0
- Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Tuxedo, versions 22.1.0, 22.1.1
- Oracle Web Services Manager, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebCenter Forms Recognition, version 14.1.1.0.0
- Oracle WebCenter Sites, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0

Oracle Analytics Executive Summary

This Critical Patch Update contains 16 new security patches for Oracle Analytics. 12 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Analytics is 9.8.

The Oracle Analytics products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle BI Publisher, versions 7.6.0.0.0, 8.2.0.0.0
- Oracle Business Intelligence Enterprise Edition, versions 7.6.0.0.0, 8.2.0.0.0, 12.2.1.4.0

Oracle Life Science Applications Executive Summary

This Critical Patch Update contains 2 new security patches for Oracle Life Science Applications. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Life Science Applications is 6.5.

The Oracle Life Science Applications products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Life Sciences InForm, versions 7.0.1.0, 7.0.1.1

Oracle Hospitality Applications Executive Summary

This Critical Patch Update contains 1 new security patch for Oracle Hospitality Applications. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a

network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Hospitality Applications is 7.5.

The Oracle Hospitality Applications products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Hospitality Cruise Shipboard Property Management (SPMS), versions 23.1.5-23.3.0

Oracle Hyperion Executive Summary

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 highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Hyperion is 7.5.

The Oracle Hyperion products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Hyperion Infrastructure Technology, version 11.2.24.0.0

Oracle Java SE Executive Summary

This Critical Patch Update contains 12 new security patches for Oracle Java SE. 8 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Java SE is 7.5.

The Oracle Java SE products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle GraalVM Enterprise Edition, version 21.3.17
- Oracle GraalVM for JDK, versions 17.0.18, 21.0.10
- Oracle Java SE, versions 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.1, 25.0.2, 26

Oracle JD Edwards Executive Summary

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

network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle JD Edwards is 7.5.

The Oracle JD Edwards products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.26.1

Oracle MySQL Executive Summary

This Critical Patch Update contains 34 new security patches for Oracle MySQL. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle MySQL is 9.8.

The Oracle MySQL products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- MySQL Cluster, versions 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0
- MySQL Enterprise Backup, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0
- MySQL Server, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0
- MySQL Shell, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0
- MySQL Workbench, versions 8.0.0-8.0.46

Oracle PeopleSoft Executive Summary

This Critical Patch Update contains 21 new security patches for Oracle PeopleSoft. 7 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle PeopleSoft is 8.8.

The Oracle PeopleSoft products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise CS Student Records, version 9.2
- PeopleSoft Enterprise FIN Contracts, version 9.2
- PeopleSoft Enterprise FIN Maintenance Management, version 9.2

- PeopleSoft Enterprise FIN Project Costing, version 9.2
- PeopleSoft Enterprise HCM Absence Management, version 9.2
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise HCM Shared Components, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.61-8.62
- PeopleSoft Enterprise SCM Purchasing, version 9.2

Oracle Retail Applications Executive Summary

This Critical Patch Update contains 17 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 highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Retail Applications is 7.5.

The Oracle Retail Applications products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Retail Assortment Planning, versions 15.0, 16.0
- Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1
- Oracle Retail EFTLink, versions 21.0.0-25.0.0
- Oracle Retail Extract Tranform and Load, version 13.0.5
- Oracle Retail Financial Integration, versions 16.0.3, 19.0.1
- Oracle Retail Fiscal Management, version 14.2
- Oracle Retail Integration Bus, versions 16.0.3, 19.0.1
- Oracle Retail Merchandise Financial Planning, versions 15.0, 16.0
- Oracle Retail Merchandising System, versions 16.0.3, 19.0.1
- Oracle Retail Predictive Application Server, version 16.0.3
- Oracle Retail Price Management, version 16.0.3
- Oracle Retail Service Backbone, versions 16.0.3, 19.0.1
- Oracle Retail Warehouse Management System, version 16.0
- Oracle Retail Xstore Point of Service, versions 21.0.3, 21.0.5, 22.0.3

Oracle Siebel CRM Executive Summary

This Critical Patch Update contains 14 new security patches for Oracle Siebel CRM. 13 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a

network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Siebel CRM is 7.7.

The Oracle Siebel CRM products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Siebel Applications, versions 17.0-26.2

Oracle Supply Chain Executive Summary

This Critical Patch Update contains 4 new security patches for Oracle Supply Chain. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Supply Chain is 8.8.

The Oracle Supply Chain products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Agile Product Lifecycle Management for Process, version 6.2.4
- Oracle AutoVue, version 21.1.0
- Oracle Product Lifecycle Analytics, version 3.6.1

Oracle Systems Executive Summary

This Critical Patch Update contains 2 new security patches for Oracle Systems. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Systems is 9.0.

The Oracle Systems products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Solaris, version 11.4
- Sun ZFS Storage Appliance Kit, version 8.8

Oracle Utilities Applications Executive Summary

This Critical Patch Update contains 7 new security patches for Oracle Utilities Applications. 6 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Utilities Applications is 7.5.

The Oracle Utilities Applications products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle Utilities Application Framework, versions 4.3.0.5.0-4.3.0.6.0, 4.4.0.0.0-4.4.0.4.0, 4.5.0.0.0-4.5.0.2.0, 25.4, 25.10, 26.4
- Oracle Utilities Live Energy Connect, versions 7.1.0.0.49, 25.12.0.0.0
- Oracle Utilities Network Management System, versions 2.5.0.1.16, 2.5.0.2.10, 2.6.0.1.10, 2.6.0.2.6
- Oracle Utilities Testing Accelerator, versions 7.0.0.0.7, 7.0.0.1.5, 25.4.0.0.2

Oracle Virtualization Executive Summary

This Critical Patch Update contains 9 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 highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Virtualization is 7.5.

The Oracle Virtualization products and versions affected by vulnerabilities that are addressed in this Critical Patch Update are:

- Oracle VM VirtualBox, version 7.2.6