Your choices regarding cookies on this site

ORACLE

By using our sites, Oracle and our third party partners may use cookies and similar technologies to collect user data for the following purposes:

- **required cookies** are necessary for the site to function, for example, to remember your log-in details and provide secure log-in
- **functional cookies** help us to optimize the site, for example, to collect statistics, to save your preferences for social interactions or to enable you to post comments on our site
- **advertising cookies** allow Oracle and our third party partners to provide you with interest-based advertising and tailored content across your browsers and devices

Please visit our privacy policy for more information.

Accept all Decline all View and change cookie preferences

Ora se
Ann

Descr

This Crit rity
Patch Up ment is
as accura ecurity
Patch Up

A Critica king
them eas ative
Critical P bilities
addressed in this Critical Security Patch Update affect multiple products. Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply Critical Security Patch Update patches as soon as possible.

Executive Summaries

Oracle Database Server Executive Summary

This Critical Security Patch Update contains 7 new security patches for Oracle Database Products. 3 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 9.9.

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

- Oracle Database Server, versions 19.3-19.33, 21.3-21.24, 23.4.0-23.26.4

Oracle APEX Executive Summary

This Critical Security Patch Update contains 2 new security patches for Oracle APEX. 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 APEX is 9.8.

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

- Oracle APEX, versions 24.1.22, 24.2.21, 26.1.5, 26.2.0

Oracle Autonomous Health Framework Executive Summary

This Critical Security Patch Update contains 3 new security patches for Oracle Autonomous Health Framework. 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 Autonomous Health Framework is 9.1.

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

- Oracle Autonomous Health Framework, versions 26.4-26.10

Oracle REST Data Services Executive Summary

This Critical Security Patch Update contains 9 new security patches for Oracle REST Data Services. 5 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 9.8.

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

- Oracle REST Data Services, versions 24.2.0-26.2.3

Oracle Application Testing Suite Executive Summary

This Critical Security Patch Update contains 3 new security patches for Oracle Application Testing Suite. 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 Application Testing Suite is 8.8.

The Oracle Application Testing Suite products and versions affected by vulnerabilities that are addressed in this Critical Security Patch Update are:

- Oracle Application Testing Suite, version 13.3.0.1

Oracle Commerce Executive Summary

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

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

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

- Oracle Commerce Guided Search / Oracle Commerce Experience Manager, version 11.4.0
- Oracle Commerce Platform, version 11.4.0

Oracle Communications Executive Summary

This Critical Security Patch Update contains 28 new security patches for Oracle Communications. 18 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 Security 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 Diameter Signaling Router (DSR), versions 9.0.0.0.0, 9.0.1.0.0, 9.1.0.0.0
- Oracle Communications Service Catalog and Design, versions 8.0-8.26
- 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, 7.7.0, 7.8.0, 8.0.1, 8.26.0

Oracle Construction and Engineering Executive Summary

This Critical Security Patch Update contains 2 new security patches for Oracle Construction and Engineering. 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 Construction and Engineering is 7.5.

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

- Primavera Unifier, versions 22.12.0-22.12.15, 23.12.0-23.12.16

Oracle E-Business Suite Executive Summary

This Critical Security Patch Update contains 72 new security patches for Oracle E-Business Suite. 22 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 Security Patch Update are:

- Oracle E-Business Suite, versions 12.2.3-12.2.15

Oracle Enterprise Manager Executive Summary

This Critical Security Patch Update contains 5 new security patches for Oracle Enterprise Manager. 3 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 Security Patch Update are:

- Oracle Enterprise Manager Base Platform, versions 13.5, 24.1

Oracle Financial Services Applications Executive Summary

This Critical Security Patch Update contains 11 new security patches for Oracle Financial Services Applications. 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 Financial Services Applications is 7.5.

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

- Oracle Financial Services Customer Screening, version 8.1.2.10
- Oracle Financial Services Enterprise Case Management, version 8.1.2.10
- Oracle Financial Services Regulatory Reporting, version 8.1.2.10

Oracle Fusion Middleware Executive Summary

This Critical Security Patch Update contains 71 new security patches for Oracle Fusion Middleware. 53 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 10.0.

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

- Helidon, versions 3.0.0-3.2.22, 4.0.0-4.5.6, 27.0.0-27.0.1
- Oracle Access Manager, versions 12.2.1.4.0, 14.1.2.1.0
- Oracle Application Development Framework (ADF), versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Business Process Management Suite, 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 Connector, versions 12.2.1.4.0, 14.1.2.1.0
- Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Middleware Common Libraries and Tools, version 14.1.2.0.0
- Oracle Platform Security for Java, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Service Bus, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebCenter Content, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebCenter Portal, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebCenter Sites, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0
- Service Delivery Platform, versions 12.2.1.4.0, 14.1.2.0.0

Oracle Analytics Executive Summary

This Critical Security Patch Update contains 29 new security patches for Oracle Analytics. 9 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 10.0.

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

- Oracle BI Publisher, versions 8.2.0.0.0, 12.2.1.4.0, 26.1.0.0.0
- Oracle Business Intelligence Enterprise Edition, versions 8.2.0.0.0, 12.2.1.4.0, 26.1.0.0.0

Oracle Hyperion Executive Summary

This Critical Security Patch Update contains 267 new security patches for Oracle Hyperion. 107 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 9.9.

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

- Oracle Hyperion Data Relationship Management, version 11.2.26.0.0
- Oracle Hyperion Financial Close Management, version 11.2.26.0.0
- Oracle Hyperion Financial Data Quality Management, Enterprise Edition, version 11.2.26.0.0
- Oracle Hyperion Financial Management, version 11.2.26.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.26.0.0
- Oracle Hyperion Planning, version 11.2.26.0.0
- Oracle Hyperion Profitability and Cost Management, version 11.2.26.0.0
- Oracle Hyperion Workspace, version 11.2.26.0.0

Oracle Java SE Executive Summary

This Critical Security Patch Update contains 11 new security patches for Oracle Java SE. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle Java SE is 8.1.

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

- Oracle GraalVM Enterprise Edition, version 21.3.20.0.3
- Oracle GraalVM for JDK, versions 17.0.21, 21.0.13
- Oracle Java SE, versions 8u511, 8u511-perf, 11.0.33, 17.0.21, 21.0.13, 25.0.5, 27.0.1
- Oracle JavaFX, versions 21.0.13, 25.0.5, 27.0.1

Oracle JD Edwards Executive Summary

This Critical Security Patch Update contains 1 new security patch for Oracle JD Edwards. This vulnerability is not remotely exploitable without authentication, i.e., may not be exploited over a network without requiring user credentials.

The highest CVSS v3.1 Base Score of vulnerabilities affecting Oracle JD Edwards is 6.5.

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

- JD Edwards EnterpriseOne Localizations, version 9.2

Oracle MySQL Executive Summary

This Critical Security Patch Update contains 8 new security patches for Oracle MySQL. 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 MySQL is 9.1.

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

- MySQL Cluster, versions 8.0.0-8.0.50, 8.4.0-8.4.13, 9.7.0-9.7.4
- MySQL Server, MySQL Cluster, versions 8.0.0-8.0.50, 8.4.0-8.4.13, 9.7.0-9.7.4

Oracle PeopleSoft Executive Summary

This Critical Security Patch Update contains 13 new security patches for Oracle PeopleSoft. 5 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 9.3.

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

- PeopleSoft Enterprise PeopleTools, versions 8.61-8.63

Oracle Siebel CRM Executive Summary

This Critical Security Patch Update contains 19 new security patches for Oracle Siebel CRM. 9 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 8.8.

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

- Siebel Applications, versions 17.0-26.9

Oracle Supply Chain Executive Summary

This Critical Security Patch Update contains 74 new security patches for Oracle Supply Chain. 36 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 9.9.

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

- Oracle Agile Engineering Data Management, version 6.2.1
- Oracle Agile PLM, version 9.3.6
- Oracle Agile Product Lifecycle Management for Process, version 6.2.4
- Oracle AutoVue, versions 21.1.0, 21.1.0.7
- Product Lifecycle Analytics, version 3.6.1

Oracle Virtualization Executive Summary

This Critical Security Patch Update contains 11 new security patches for Oracle Virtualization. 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 Virtualization is 8.6.

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

- Oracle VM VirtualBox, version 7.2.22

© 2026 Oracle Privacy / Do Not Sell My Info Cookie Preferences Ad Choices Careers Subscribe to emails

Integrity Helpline Resources Contact Us