Oracle Critical Patch Update Advisory - April 2026

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 481 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 April 2026 Critical Patch Update: Executive Summary and Analysis.

Please note that since the release of the January 2026 Critical Patch Update, Oracle has released a Security Alert for Oracle Identity Manager and Oracle Web Services Manager, CVE-2026-21992 (March 20, 2026). Customers are strongly advised to apply the April 2026 Critical Patch Update for Fusion Middleware products, which includes patches for this Alert as well as additional patches.

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below.

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
JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.26.1	JD Edwards
Management Cloud Engine, version 25.2.0.0.0	Management Cloud Engine
MySQL Cluster, versions 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0	MySQL
MySQL Connectors, versions 9.0.0-9.6.0	MySQL
MySQL Enterprise Backup, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0	MySQL
MySQL Server, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0	MySQL
MySQL Shell, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0	MySQL
MySQL Workbench, versions 8.0.0-8.0.46	MySQL
Oracle Access Manager, version 14.1.2.0.0	Fusion Middleware
Oracle Adapter for Eclipse RDF4J, versions 3.12.0, 21.1.8, 24.1.0	Database
Oracle Agile Product Lifecycle Management for Process, version 6.2.4	Oracle Supply Chain Products
Oracle Application Development Framework (ADF), versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Application Express, versions 23.2.20, 23.2.21, 24.1.15, 24.1.16, 24.2.13, 24.2.15	Database
Oracle Application Testing Suite, version 13.3.0.1	Oracle Enterprise Manager
Oracle Autonomous Health Framework, versions 25.11-26.1	Oracle Autonomous Health Framew
Oracle AutoVue, version 21.1.0	Oracle Supply Chain Products
Oracle Banking Branch, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Cash Management, version 14.8.2.0.0	Contact Support
Oracle Banking Collections and Recovery, versions 14.6.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Corporate Lending, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Corporate Lending Process Management, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Credit Facilities Process Management, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Liquidity Management, versions 14.8.0.0.0, 14.8.1.0.0	Contact Support
Oracle Banking Origination, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Payments, versions 14.5.0.0.0-14.8.0.0.0	Contact Support

Affected Products and Versions	Patch Availability Document
Oracle Banking Supply Chain Finance, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Trade Finance, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Trade Finance Process Management, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Banking Virtual Account Management, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle BI Publisher, versions 7.6.0.0.0, 8.2.0.0.0	Oracle Analytics
Oracle Blockchain Platform, version 24.1.3	Oracle Blockchain Platform
Oracle Business Activity Monitoring, version 12.2.1.4.0	Fusion Middleware
Oracle Business Intelligence Enterprise Edition, versions 7.6.0.0.0, 8.2.0.0.0	Oracle Analytics
Oracle Business Process Management Suite, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Commerce Guided Search, version 11.4.0	Oracle Commerce
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 Billing and Revenue Management
Oracle Communications BRM - Elastic Charging Engine, versions 15.0.0.0-15.0.1.0, 15.1.0.0-15.2.0.0	Oracle Communications BRM - Elast Charging Engine
Oracle Communications Cloud Native Core Binding Support Function, version 25.1.200	Oracle Communications Cloud Nativ Core Binding Support Function
Oracle Communications Cloud Native Core Certificate Management, version 25.1.201	Oracle Communications Cloud Nativ Core Certificate Management
Oracle Communications Cloud Native Core Console, version 25.1.201	Oracle Communications Cloud Nativ Core Console
Oracle Communications Cloud Native Core DBTier, versions 25.1.200, 25.2.100	Oracle Communications Cloud Nativ Core DBTier
Oracle Communications Cloud Native Core Network Exposure Function, versions 24.2.1, 24.2.4	Oracle Communications Cloud Nativ Core Network Exposure Function
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 25.1.200, 25.2.200	Oracle Communications Cloud Nativ Core Network Function Cloud Native Environment
Oracle Communications Cloud Native Core Network Repository Function, version 25.1.204	Oracle Communications Cloud Nativ Core Network Repository Function
Oracle Communications Cloud Native Core Network Slice Selection Function, versions 25.1.100, 25.1.200	Oracle Communications Cloud Nativ Core Network Slice Selection Functi
Oracle Communications Cloud Native Core Policy, versions 25.1.200, 25.1.201, 25.1.202	Oracle Communications Cloud Nativ Core Policy

Affected Products and Versions	Patch Availability Document
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 25.1.200, 25.1.201, 25.2.100	Oracle Communications Cloud Nativ Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Service Communication Proxy, versions 25.1.100, 25.1.200, 25.1.202, 25.2.100	Oracle Communications Cloud Nativ Core Service Communication Proxy
Oracle Communications Cloud Native Core Unified Data Repository, versions 25.1.100, 25.1.200	Oracle Communications Cloud Nativ Core Unified Data Repository
Oracle Communications Convergence, version 3.0.3.4.0	Oracle Communications Convergenc
Oracle Communications EAGLE, version 47.0	Oracle Communications EAGLE (Software)
Oracle Communications EAGLE Application Processor, versions 17.0-17.1	Oracle Communications EAGLE Application Processor
Oracle Communications EAGLE Element Management System, version 47.0.0.1.0	Oracle Communications EAGLE Element Management System
Oracle Communications EAGLE LNP Application Processor, version 11.0	Oracle Communications EAGLE LNP Application Processor
Oracle Communications Element Manager, versions 9.0.0-9.0.4	Oracle Communications Element Manager
Oracle Communications Instant Messaging Server, version 10.0.1.8.0	Oracle Communications Instant Messaging Server
Oracle Communications LSMS, version 14.0	Oracle Communications LSMS
Oracle Communications Messaging Server, version 8.1.0.0.0	Oracle Communications Messaging Server
Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0, 8.0.0	Oracle Communications Network Integrity
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 Offline Mediation Controller
Oracle Communications Operations Monitor, versions 5.2, 6.0, 6.1	Oracle Communications Operations Monitor
Oracle Communications Order and Service Management, versions 7.5.0, 8.0.0	Oracle Communications Order and Service Management
Oracle Communications Performance Intelligence Center, versions 10.5.0.0-10.5.0.2	Oracle Communications Performanc Intelligence Center
Oracle Communications Policy Management, versions 15.0.0.0.0, 15.0.0.1.0	Oracle Communications Policy Management
Oracle Communications Service Catalog and Design, versions 8.0.0.6.0, 8.1.0.5.0, 8.2.0.2.0	Oracle Communications Service Cat and Design

Affected Products and Versions	Patch Availability Document
Oracle Communications Session Border Controller, versions 9.3.0, 10.0.0, 10.1.0	Oracle Communications Session Bor Controller
Oracle Communications Session Report Manager, versions 9.0.0-9.0.4	Oracle Communications Session Rep Manager
Oracle Communications Unified Assurance, versions 6.1.1-7.0.0	Oracle Communications Unified Assurance
Oracle Communications Unified Inventory Management, versions 7.5.0-7.5.1, 7.6.0-7.8.0, 8.0.0	Oracle Communications Unified Inventory Management
Oracle Configuration Manager, versions 13.5, 24.1	Oracle Enterprise Manager
Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Database Server, versions 12.1.0.2.0, 12.2.0.1.0, 19.3-19.30, 21.3-21.21, 23.4.0-23.26.1	Database
Oracle Documaker, versions 12.7.2-13.0.2	Contact Support
Oracle E-Business Suite, versions 12.2.3-12.2.15, 15.0	Oracle E-Business Suite
Oracle Enterprise Communications Broker, versions 4.2.0, 5.0.0	Oracle Enterprise Communications Broker
Oracle Enterprise Manager Base Platform, versions 13.5, 24.1	Oracle Enterprise Manager
Oracle Enterprise Manager for Fusion Middleware, versions 13.5, 24.1	Oracle Enterprise Manager
Oracle Enterprise Operations Monitor, version 6.1.0.0.0	Oracle Enterprise Operations Monitc
Oracle Essbase, version 21.8.1.0.0	Database
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.9, 8.0.8.7, 8.1.2.5	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.10, 8.1.2.11	Oracle Financial Services Behavior Detection Platform
Oracle Financial Services Compliance Studio, version 8.1.2.9	Oracle Financial Services Complianc Studio
Oracle Financial Services Customer Screening, version 8.1.2.8.0	Oracle Financial Services Customer Screening
Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.2.10, 8.1.2.11	Oracle Financial Services Enterprise Case Management
Oracle Financial Services Lending and Leasing, versions 14.8.0.0.0, 14.10.0.0.0-14.12.0.0.0	Contact Support
Oracle Financial Services Model Management and Governance, version 8.1.2.7	Oracle Financial Services Model Management and Governance
Oracle Financial Services Regulatory Reporting, versions 8.1.2.10, 8.1.2.11	Oracle Financial Services Regulatory Reporting

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8	Oracle Financial Services Trade-Base Anti Money Laundering Enterprise Edition
Oracle Financial Services Transaction Filtering, version 8.1.2.8.0	Oracle Financial Services Transactio Filtering
Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 14.5.0.0.0-14.8.0.0.0	Contact Support
Oracle Fusion Middleware, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Global Lifecycle Management OPatchAuto, versions 12.2.0.1.16-12.2.0.1.49	Database
Oracle GoldenGate, versions 23.4-23.26.1	Database
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	Database
Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.14	Database
Oracle GraalVM Enterprise Edition, version 21.3.17	Java SE
Oracle GraalVM for JDK, versions 17.0.18, 21.0.10	Java SE
Oracle Graph Server and Client, versions 24.4.5, 25.4.1, 26.1.0	Database
Oracle Hospitality Cruise Shipboard Property Management (SPMS), versions 23.1.5-23.3.0	Oracle Hospitality Cruise Shipboard Property Management (SPMS)
Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Hyperion Infrastructure Technology, version 11.2.24.0.0	Oracle Enterprise Performance Management
Oracle Identity Manager, versions 12.2.1.4.0, 14.1.2.0.0, 14.1.2.1.0	Fusion Middleware
Oracle Identity Manager Connector, version 12.2.1.4.0	Fusion Middleware
Oracle Insurance Policy Administration J2EE, versions 11.3.1.0, 11.3.2.0, 12.0.5.0, 12.1.1.0	Oracle Insurance Applications
Oracle Insurance Policy Administration Operational Data Store for Life and Annuity, version 1.0.2.1	Contact Support
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	Java SE
Oracle Life Sciences Empirica Signal, versions 9.2.1-9.2.3	Oracle Life Science
Oracle Life Sciences InForm, versions 7.0.1.0, 7.0.1.1	Oracle Life Science
Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Middleware Common Libraries and Tools, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle NoSQL Database, versions 1.6.5, 1.7.0	Database
Oracle Outside In Technology, version 8.5.8	Fusion Middleware
Oracle Product Lifecycle Analytics, version 3.6.1	Oracle Supply Chain Products
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	Database
Oracle Retail Assortment Planning, versions 15.0, 16.0	Retail Applications
Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail EFTLink, versions 21.0.0-25.0.0	Retail Applications
Oracle Retail Extract Tranform and Load, version 13.0.5	Retail Applications
Oracle Retail Financial Integration, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Fiscal Management, version 14.2	Retail Applications
Oracle Retail Integration Bus, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Merchandise Financial Planning, versions 15.0, 16.0	Retail Applications
Oracle Retail Merchandising System, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Predictive Application Server, version 16.0.3	Retail Applications
Oracle Retail Price Management, version 16.0.3	Retail Applications
Oracle Retail Service Backbone, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Warehouse Management System, version 16.0	Retail Applications
Oracle Retail Xstore Point of Service, versions 21.0.5, 22.0.3	Retail Applications
Oracle Security Service, versions 12.1.3.0.0, 12.2.1.4.0	Fusion Middleware
Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Solaris, version 11.4	Systems
Oracle TimesTen In-Memory Database, versions 18.1.4, 22.1.1	Database
Oracle Tuxedo, versions 22.1.0, 22.1.1	Fusion Middleware
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 Applications
Oracle Utilities Live Energy Connect, versions 7.1.0.0.45, 25.12.0.0.0	Oracle Utilities Applications
Oracle Utilities Network Management System, versions 2.4.0.1.31, 2.5.0.1.16, 2.5.0.2.10, 2.6.0.1.10, 2.6.0.2.5, 2.6.0.2.6	Oracle Utilities Applications
Oracle Utilities Testing Accelerator, versions 7.0.0.0.7, 7.0.0.1.5, 25.4.0.0.2	Oracle Utilities Applications

Affected Products and Versions	Patch Availability Document
Oracle VM VirtualBox, version 7.2.6	Virtualization
Oracle Web Services Manager, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle WebCenter Forms Recognition, version 14.1.1.0.0	Fusion Middleware
Oracle WebCenter Sites, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0	Fusion Middleware
PeopleSoft Enterprise CC Common Application Objects, version 9.2	PeopleSoft
PeopleSoft Enterprise CS Student Records, version 9.2	PeopleSoft
PeopleSoft Enterprise FIN Contracts, version 9.2	PeopleSoft
PeopleSoft Enterprise FIN Maintenance Management, version 9.2	PeopleSoft
PeopleSoft Enterprise FIN Project Costing, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Absence Management, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Human Resources, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Shared Components, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.61-8.62	PeopleSoft
PeopleSoft Enterprise SCM Purchasing, version 9.2	PeopleSoft
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	Oracle Construction and Engineerin Suite
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 Construction and Engineerin Suite
Siebel Applications, versions 17.0-26.2	Siebel
Sun ZFS Storage Appliance Kit, version 8.8	Systems

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 ID. A vulnerability that affects multiple products will appear with the same CVE ID in all risk matrices.

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 conditions required to exploit the vulnerability and the potential impact of a successful exploit. Oracle provides this information 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.

Third party component vulnerabilities that are deemed not exploitable in the context of their inclusion in an Oracle product are listed, with VEX justifications, below the respective Oracle product's risk matrix.

The protocol in the risk matrix implies that all of its secure variants are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected.

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 that further supplements the Lifetime Support Policy as explained in My Oracle Support Note KB65129. 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:

- 4ra1n: CVE-2026-34317, CVE-2026-34318, CVE-2026-34319
- Aaron Esau: CVE-2026-35248
- Aleksei Veremeev of a2.solutions: CVE-2026-34312
- Anton Fedorov: CVE-2026-22017, CVE-2026-34303
- Anwar Dawa: CVE-2026-35246
- Bartosz Michałowski: CVE-2026-35251
- Co-tang X: CVE-2026-22010, CVE-2026-34310
- Diego Palacios: CVE-2026-35247
- ehdgks0627: CVE-2026-35245
- fstmpr: CVE-2026-35242
- HoraceYang of Tencent Security YUNDING LAB: CVE-2026-22005
- Jan Czerlunczakiewicz of STM CYBER: CVE-2026-34279
- Jan Kamiński: CVE-2026-35251
- Jingzhou Fu of WingTecher Lab of Tsinghua University: CVE-2026-22009
- Joakim Bülow: CVE-2026-34308
- John Kounelis: CVE-2026-34269
- Kamil Frankowicz: CVE-2026-35251

- Ken Pyle: CVE-2026-22007, CVE-2026-34268
- Khanh Nguyen Trong of Vietcombank: CVE-2026-34314, CVE-2026-34320, CVE-2026-34321, CVE-2026-35231
- Maxime Escourbiac of Michelin CERT: CVE-2026-22011
- Mert: CVE-2026-35250
- Nguyen Tuong Huy of HDBank: CVE-2026-34313
- nosocksinbirks: CVE-2026-35249
- Pavel Kohout of Aisle Research: CVE-2026-34270, CVE-2026-34271, CVE-2026-34276
- Pierre_Adams: CVE-2026-35244
- Thomas Beckers of Soptim: CVE-2026-22016
- VMBreakers (Gangmin Kim, Sangbin Kim, Un3xploitable) working with Trend Micro Zero Day Initiative: CVE-2026-35230
- Xiaodong Qi of Shui Mu Yu Lin: CVE-2026-22005
- Yassine Bengana of Michelin CERT: CVE-2026-22011
- yoloClin of Radiant Security: CVE-2026-34283, CVE-2026-34284, CVE-2026-34285, CVE-2026-34286, CVE-2026-34287, CVE-2026-34288, CVE-2026-34289, CVE-2026-34290, CVE-2026-34291, CVE-2026-34292, CVE-2026-34294, CVE-2026-34305, CVE-2026-34315, CVE-2026-35232, CVE-2026-35243
- Yuanyi Li of Shui Mu Yu Lin: CVE-2026-22005
- yx: CVE-2026-35240
- Zhiyong Wu of WingTecher Lab of Tsinghua University: CVE-2026-22009
- Zpt_dxpn of Pentest Team Viettel Cyber Security: CVE-2026-34296

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:

- Ahmed Ghalab
- Emad Al-Mousa of Saudi Aramco's Upstream Digital Center (UDC)
- Hanno Böck

- Maxime Escourbiac of Michelin CERT
- Thomas M.
- Viktor Lofgren
- Yassine Bengana of Michelin CERT
- yoloClin of Radiant Security [2 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:

- Matthew Maynard
- Nibin George
- notnotnotveg
- Parvatiananta11
- Peschel Frank
- Pim Dieleman
- samael0x4
- Susan Feindt
- Susmoy Khan Miran
- Suyash Kishor Sawant
- Thomas Pikaart of Caesars Entertainment
- WC [3 reports]

Critical Patch Update Schedule

Critical Patch Updates are released on the third Tuesday of January, April, July, and October. The next four dates are:

- 21 July 2026
- 20 October 2026
- 19 January 2027

- 20 April 2027

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - April 2026 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
- CSAF JSON version of the risk matrices
- Map of CVE to Advisory/Alert
- Oracle Lifetime Support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2026-April-21	Rev 1. Initial Release.
2026-April-24	Rev 2. Update links to My Oracle Support Note KA923 and My Oracle Support Note CPU59.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 26 new security patches for Oracle Database Products divided as follows:

- 8 new security patches for Oracle Database Products
- No new security patches for Oracle APEX, but third party patches are provided
- 2 new security patches for Oracle Autonomous Health Framework
- 3 new security patches for Oracle Blockchain Platform
- No new security patches for Oracle Essbase, but third party patches are provided
- No new security patches for Oracle Global Lifecycle Management, but third party patches are provided
- 10 new security patches for Oracle GoldenGate

- No new security patches for Oracle Graph Server and Client, but third party patches are provided
- No new security patches for Oracle NoSQL Database, but third party patches are provided
- 2 new security patches for Oracle REST Data Services
- 1 new security patch for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 8 new security patches, plus additional third party patches noted below, 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. 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 ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
CVE-2026-33870	Clusterware (Micronaut)	None	HTTP	Yes	7.5	Network	Low	Nor
CVE-2026-35229	Java VM	Create Session	Oracle Net	Yes	7.5	Network	Low	Nor
CVE-2026-31790	RDBMS (OpenSSL)	None	Multiple	No	7.2	Network	Low	Hig
CVE-2026-26007	RDBMS (Python)	Create Session	Multiple	Yes	6.5	Network	Low	Nor
CVE-2026-21999	XML Database	HTTP Listener	HTTPS	Yes	5.3	Network	High	Nor
CVE-2025-31948	Data Mining (Intel oneAPI Toolkit OpenMP)	Authenticated User	None	No	3.3	Local	Low	Lo
CVE-2025-48924	RDBMS (Apache	DBMS Developer	Multiple	No	3.3	Local	Low	Nor

CVE ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Rec
	Commons Lang)							
CVE-2026-34312	RDBMS	Row Access Method	Multiple	No	2.4	Network	Low	Hig

Additional CVEs addressed are:

- The patch for CVE-2026-33870 also addresses CVE-2026-33013.
- The patch for CVE-2026-31790 also addresses CVE-2025-15467.

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

- Database (Apache Tomcat): CVE-2025-66614, CVE-2025-58050, CVE-2026-24733 and CVE-2026-24734 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- GraalVM Multilingual Engine: CVE-2026-21945, CVE-2025-12183, CVE-2025-43368, CVE-2025-47219, CVE-2025-6021, CVE-2025-6052, CVE-2025-7425, CVE-2026-21925, CVE-2026-21932, CVE-2026-21933 and CVE-2026-21947 [VEX Justification: vulnerable_code_not_in_execute_path].
- Java VM (Apache Hive): CVE-2025-62728 [VEX Justification: vulnerable_code_not_in_execute_path].
- RDBMS (libexpat): CVE-2026-25210 and CVE-2026-24515 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- RDBMS (Nhttp2): CVE-2026-27135 [VEX Justification: vulnerable_code_not_in_execute_path].
- Spatial and Graph (SQLite): CVE-2025-6965 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- SQLcl (Apache Log4j): CVE-2025-68161 [VEX Justification: vulnerable_code_not_in_execute_path].
- SQLcl (assertj): CVE-2026-24400 [VEX Justification: vulnerable_code_not_in_execute_path].
- SQLcl (MCP Java SDK): CVE-2026-34237 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].

Oracle Database Server Client-Only Installations

- The following Oracle Database Server vulnerability included in this Critical Patch Update affects client-only installations: CVE-2025-48924.

Oracle Adapter for Eclipse RDF4J Risk Matrix

This Critical Patch Update contains 2 new security patches, plus additional third party patches noted below, 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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2025-48976	Oracle Adapter for Eclipse RDF4J	Adapter for Eclipse RDF (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	None	
CVE-2023-46750	Oracle Adapter for Eclipse RDF4J	Jena adapter (Apache Shiro)	HTTP	Yes	6.1	Network	Low	None	Re

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

- Oracle Adapter for Eclipse RDF4J
  - Adapter for Eclipse RDF (Apache Commons BeanUtils): CVE-2025-48734 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Adapter for Eclipse RDF (Apache Commons Lang): CVE-2025-48924 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Adapter for Eclipse RDF (Eclipse Jetty): CVE-2025-5115 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle APEX Risk Matrix

This Critical Patch Update contains no new security patches for exploitable vulnerabilities but does include third party patches, noted below, for the following non-exploitable third party CVEs for Oracle APEX. Please refer to previous Critical Patch Update Advisories if the last

Critical Patch Update was not applied for Oracle APEX. The English text form of this Risk Matrix can be found here.

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

- Oracle Application Express
  - General (DOMPurify): CVE-2026-0540 [VEX Justification: vulnerable_code_not_in_execute_path].
  - General (turndown): CVE-2025-9670 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Autonomous Health Framework Risk Matrix

This Critical Patch Update contains 2 new security patches, plus additional third party patches noted below, for Oracle Autonomous Health Framework. 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 ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2025-15467	Oracle Autonomous Health Framework	Trace File Analyzer (OpenSSL)	Multiple	No	7.2	Network	Low	High
CVE-2025-9232	Oracle Autonomous Health Framework	Command Line Interface and SDK (pynacl)	HTTP	Yes	5.9	Network	High	None

Additional CVEs addressed are:

- The patch for CVE-2025-9232 also addresses CVE-2025-9230.
- The patch for CVE-2025-15467 also addresses CVE-2025-11187.

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

- Oracle Autonomous Health Framework
  - Command Line Interface and SDK (urllib3): CVE-2026-21441 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
  - Trace File Analyzer (Apache Log4j): CVE-2025-68161 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].

Oracle Blockchain Platform Risk Matrix

This Critical Patch Update contains 3 new security patches, plus additional third party patches noted below, for Oracle Blockchain Platform. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2025-61729	Oracle Blockchain Platform	BCS Console (Golang Go)	HTTP	Yes	7.5	Network	Low	None
CVE-2025-59465	Oracle Blockchain Platform	BCS Console (Node.js)	HTTP/2	Yes	7.5	Network	Low	None
CVE-2025-5318	Oracle Blockchain Platform	BCS Console (libssh)	HTTP	No	5.4	Network	Low	Low

Additional CVEs addressed are:

- The patch for CVE-2025-59465 also addresses CVE-2025-27209, CVE-2025-27210, CVE-2025-55130, CVE-2025-55131, CVE-2025-55132, CVE-2025-59466, CVE-2026-21636, and CVE-2026-21637.
- The patch for CVE-2025-5318 also addresses CVE-2025-4877, CVE-2025-4878, CVE-2025-5351, CVE-2025-5372, CVE-2025-5449, and CVE-2025-5987.
- The patch for CVE-2025-61729 also addresses CVE-2024-24789, CVE-2024-24790, CVE-2025-47910, CVE-2025-47912, CVE-2025-58183, CVE-2025-58185, CVE-2025-58186, CVE-2025-58187, CVE-2025-58188, CVE-2025-58189, CVE-2025-61723, CVE-2025-61724, CVE-2025-61725, and CVE-2025-61727.

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

- Oracle Blockchain Platform
  - BCS Console (Apache Commons Lang): CVE-2025-48924 [VEX Justification: vulnerable_code_not_in_execute_path].
  - BCS Console (Python): CVE-2025-8194, CVE-2024-12718, CVE-2024-9287, CVE-2025-4138, CVE-2025-4330, CVE-2025-4435, CVE-2025-4517 and CVE-2025-6069 [VEX Justification: vulnerable_code_not_in_execute_path].
  - BCS Console (urllib3): CVE-2025-66418 and CVE-2025-66471 [VEX Justification: vulnerable_code_not_in_execute_path].
  - BCS Console (LibTIFF): CVE-2025-9900, CVE-2025-8176, CVE-2025-8177 and CVE-2025-8961 [VEX Justification: vulnerable_code_not_in_execute_path].
  - BCS Console (glibc): CVE-2025-8058 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Essbase Risk Matrix

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

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

- Oracle Essbase
  - Essbase Web Platform (Apache HTTP Server): CVE-2025-58098, CVE-2025-55753, CVE-2025-59775, CVE-2025-65082 and CVE-2025-66200 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Essbase Web Platform (curl): CVE-2025-14017, CVE-2025-13034, CVE-2025-14524, CVE-2025-14819, CVE-2025-15079 and CVE-2025-15224 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Essbase Web Platform (OpenSSL): CVE-2025-15467, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795 and CVE-2026-22796 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Global Lifecycle Management Risk Matrix

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

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

- Oracle Global Lifecycle Management OPatchAuto
  - Database extensions (jackson-core): CVE-2025-52999 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].

Oracle GoldenGate Risk Matrix

This Critical Patch Update contains 10 new security patches, plus additional third party patches noted below, 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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2025-66566	Oracle GoldenGate Stream Analytics	General (lz4-java)	HTTP	Yes	7.5	Network	Low	None
CVE-2025-67735	Oracle GoldenGate Big Data and Application Adapters	AWS SDK (Netty)	HTTP	Yes	6.5	Network	Low	None
CVE-2025-67735	Oracle GoldenGate Big Data	Java Delivery (Netty)	HTTP	Yes	6.5	Network	Low	None

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
	and Application Adapters							
CVE-2024-7254	Oracle GoldenGate Big Data and Application Adapters	Third Party (Google Protobuf-Java)	HTTP	No	6.5	Network	Low	Low
CVE-2025-33042	Oracle GoldenGate Big Data and Application Adapters	Third Party (Apache Avro)	None	No	5.9	Local	Low	None
CVE-2026-34273	Oracle GoldenGate	Libraries	HTTP	Yes	5.3	Network	Low	None
CVE-2025-8916	Oracle GoldenGate Big Data and Application Adapters	Java Delivery (Bouncy Castle Java Library)	HTTPS	Yes	5.3	Network	Low	None
CVE-2025-68161	Oracle GoldenGate	Third Party (Apache Log4j)	TLS	Yes	4.7	Network	High	None
CVE-2025-48924	Oracle GoldenGate Big Data and Application Adapters	Third Party (Apache Commons Lang)	HTTP	No	4.3	Network	Low	Low
CVE-2025-11143	Oracle GoldenGate Big Data and Application Adapters	Java Delivery (Eclipse Jetty)	HTTP	Yes	3.7	Network	High	None

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

- Oracle GoldenGate Big Data and Application Adapters
  - Third Party (Aircompressor): CVE-2025-67721 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
  - Third Party (MessagePack): CVE-2026-21452 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle GoldenGate Stream Analytics
  - General (Apache Hive): CVE-2025-62728 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Third Party (Apache Avro): CVE-2025-33042 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Third Party (Apache Log4j): CVE-2025-68161 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Graph Server and Client Risk Matrix

This Critical Patch Update contains no new security patches for exploitable vulnerabilities but does include third party patches, noted below, for the following non-exploitable third party CVEs for Oracle Graph Server and Client. Please refer to previous Critical Patch Update Advisories if the last Critical Patch Update was not applied for the Oracle Graph Server and Client. The English text form of this Risk Matrix can be found here.

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

- Oracle Graph Server and Client
  - Packaging (Apache Tomcat): CVE-2026-24734 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle NoSQL Database Risk Matrix

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

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

- Oracle NoSQL Database
  - Administration (Apache Commons Lang): CVE-2025-48924 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle REST Data Services Risk Matrix

This Critical Patch Update contains 2 new security patches, plus additional third party patches noted below, 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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2025-5115	Oracle REST Data Services	Third Party (Eclipse Jetty)	HTTP/2	Yes	7.5	Network	Low	None	N
CVE-2025-66453	Oracle REST Data Services	REST Services (Rhino)	HTTP	Yes	5.3	Network	Low	None	N

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

- Oracle REST Data Services
  - General (React): CVE-2026-23864, CVE-2025-55182, CVE-2025-55183, CVE-2025-55184 and CVE-2025-67779 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle TimesTen In-Memory Database Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2025-68121	Oracle TimesTen In-Memory Database	Third-party components (Golang Go)	HTTPS	Yes	7.4	Network	High	None	

Additional CVEs addressed are:

- The patch for CVE-2025-68121 also addresses CVE-2025-61727, CVE-2025-61729, and CVE-2025-61732.

Oracle Commerce Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2025-48734	Oracle Commerce Guided Search	Experience Manager (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low	Low
CVE-2024-56406	Oracle Commerce Guided Search	Endeca Application Controller (Perl)	HTTP	Yes	8.6	Network	Low	None
CVE-2026-24734	Oracle Commerce Guided Search	Content Acquisition System, Endeca Application Controller, Experience Manager (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	None

Oracle Communications Risk Matrix

This Critical Patch Update contains 139 new security patches, plus additional third party patches noted below, for Oracle Communications. 93 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 ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2025-6965	Oracle Communications Cloud Native Core Network Exposure Function	Platform (SQLite)	HTTP	Yes	9.8	Network	Low
CVE-2025-68615	Oracle Communications	Other (Net-SNMP)	UDP	Yes	9.8	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	EAGLE						
CVE-2025-68615	Oracle Communications EAGLE Application Processor	Other (Net-SNMP)	HTTP	Yes	9.8	Network	Low
CVE-2025-68615	Oracle Communications EAGLE LNP Application Processor	Patches (Net-SNMP)	HTTP	Yes	9.8	Network	Low
CVE-2025-68615	Oracle Communications LSMS	Platform (Net-SNMP)	HTTP	Yes	9.8	Network	Low
CVE-2025-68615	Oracle Communications Messaging Server	Security (Net-SNMP)	HTTP	Yes	9.8	Network	Low
CVE-2025-68615	Oracle Communications Operations Monitor	Developer Infrastructure (Net-SNMP)	HTTP	Yes	9.8	Network	Low
CVE-2026-25968	Oracle Communications Operations Monitor	Mediation Engine (ImageMagick)	HTTP	Yes	9.8	Network	Low
CVE-2025-68615	Oracle Communications Policy Management	Configuration Management Platform (Net-SNMP)	HTTP	Yes	9.8	Network	Low
CVE-2025-48913	Oracle Communications Unified Assurance	Core (Apache CXF)	HTTP	Yes	9.8	Network	Low
CVE-2025-12543	Oracle Communications Cloud Native Core Policy	Alarms, KPI, and Measurements (Undertow)	HTTP	Yes	9.6	Network	Low
CVE-2025-12543	Oracle Communications	Install (Undertow)	HTTP	Yes	9.6	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Cloud Native Core Unified Data Repository						
CVE-2024-5535	Oracle Communications Cloud Native Core Network Slice Selection Function	Install (OpenSSL)	TLS	Yes	9.1	Network	Low
CVE-2025-55130	Oracle Communications Cloud Native Core Policy	Install (Node.js)	HTTP	Yes	9.1	Network	Low
CVE-2025-58050	Oracle Communications Operations Monitor	Mediation Engine (PCRE2)	HTTP	Yes	9.1	Network	Low
CVE-2025-15467	Oracle Communications Cloud Native Core Certificate Management	Configuration (OpenSSL)	HTTPS	Yes	8.8	Network	Low
CVE-2025-15467	Oracle Communications Cloud Native Core Console	Configuration (OpenSSL)	TLS	Yes	8.8	Network	Low
CVE-2025-9900	Oracle Communications Cloud Native Core Network Repository Function	Signaling (LibTIFF)	HTTP	Yes	8.8	Network	Low
CVE-2025-9900	Oracle Communications Cloud Native Core Network Slice Selection Function	Install (LibTIFF)	HTTP	Yes	8.8	Network	Low
CVE-2026-0861	Oracle Communications Cloud Native	Configuration (glibc)	None	No	8.4	Local	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Core Network Function Cloud Native Environment						
CVE-2025-55754	Oracle Communications Unified Assurance	Core (Apache Pulsar)	HTTP	No	8.4	Network	Low
CVE-2026-0861	Oracle Communications Unified Inventory Management	Third Party (glibc)	None	No	8.4	Local	Low
CVE-2026-0861	Oracle Enterprise Operations Monitor	Mediation Engine (glibc)	None	No	8.4	Local	Low
CVE-2025-58098	Oracle Communications Cloud Native Core Security Edge Protection Proxy	ATS Framework (Apache HTTP Server)	HTTP	No	8.3	Network	Low
CVE-2025-58098	Oracle Communications Cloud Native Core Service Communication Proxy	ATS Framework (Apache HTTP Server)	HTTP	No	8.3	Network	Low
CVE-2025-58098	Oracle Communications Cloud Native Core Unified Data Repository	ATS Framework (Apache HTTP Server)	HTTP	No	8.3	Network	Low
CVE-2025-32990	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Configuration (GnuTLS)	TLS	Yes	8.2	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2025-32990	Oracle Communications Cloud Native Core Service Communication Proxy	Signaling (GnuTLS)	TLS	Yes	8.2	Network	Low
CVE-2026-22022	Oracle Communications Unified Assurance	Core (Apache Solr)	HTTP	Yes	8.2	Network	Low
CVE-2025-5318	Oracle Communications Cloud Native Core Network Repository Function	Signaling (libssh)	SFTP	No	8.1	Network	Low
CVE-2025-5318	Oracle Communications Cloud Native Core Security Edge Protection Proxy	ATS Framework (libssh)	SFTP	No	8.1	Network	Low
CVE-2025-5318	Oracle Communications Cloud Native Core Service Communication Proxy	Install (libssh)	SFTP	No	8.1	Network	Low
CVE-2025-5318	Oracle Communications EAGLE Application Processor	Other (libssh)	SFTP	No	8.1	Network	Low
CVE-2025-5318	Oracle Communications EAGLE LNP Application Processor	Patches (libssh)	SFTP	No	8.1	Network	Low
CVE-2025-5318	Oracle Communications LSMS	Platform (libssh)	SFTP	No	8.1	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2026-25646	Oracle Communications Policy Management	Configuration Management Platform (libpng)	HTTP	Yes	8.1	Network	High
CVE-2025-5318	Oracle Communications Session Border Controller	Routing (libssh)	SFTP	No	8.1	Network	Low
CVE-2026-27099	Oracle Communications Cloud Native Core Binding Support Function	Install (Jenkins)	HTTP	No	8.0	Network	Low
CVE-2026-27099	Oracle Communications Cloud Native Core Network Exposure Function	Install (Jenkins)	HTTP	No	8.0	Network	Low
CVE-2026-27099	Oracle Communications Cloud Native Core Network Repository Function	Install (Jenkins)	HTTP	No	8.0	Network	Low
CVE-2026-27099	Oracle Communications Cloud Native Core Policy	Alarms, KPI, and Measurements (Jenkins)	HTTP	No	8.0	Network	Low
CVE-2026-27099	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Automated Test Suite (Jenkins)	HTTP	No	8.0	Network	Low
CVE-2026-27099	Oracle Communications Cloud Native Core Service	ATS Framework (Jenkins)	HTTP	No	8.0	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Communication Proxy						
CVE-2025-68973	Oracle Communications Cloud Native Core Certificate Management	Configuration (GnuPG)	None	No	7.8	Local	High
CVE-2025-68973	Oracle Communications Cloud Native Core Console	Configuration (GnuPG)	None	No	7.8	Local	High
CVE-2025-66566	Oracle Communications BRM - Elastic Charging Engine	Security (lz4-java)	HTTP	Yes	7.5	Network	Low
CVE-2026-21945	Oracle Communications Cloud Native Core Certificate Management	Oracle Java SE	HTTP	Yes	7.5	Network	Low
CVE-2026-21945	Oracle Communications Cloud Native Core Console	Oracle Java SE	HTTP	Yes	7.5	Network	Low
CVE-2025-8194	Oracle Communications Cloud Native Core DBTier	Configuration (Python)	HTTP	Yes	7.5	Network	Low
CVE-2025-41253	Oracle Communications Cloud Native Core Network Exposure Function	Install (Spring Cloud Gateway)	HTTP	Yes	7.5	Network	Low
CVE-2025-41249	Oracle Communications Cloud Native Core Network Exposure Function	Install (Spring Framework)	HTTP	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2025-48976	Oracle Communications Cloud Native Core Network Exposure Function	Platform (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low
CVE-2024-8184	Oracle Communications Cloud Native Core Network Exposure Function	Platform (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2025-13151	Oracle Communications Cloud Native Core Network Exposure Function	Platform (Libtasn1)	HTTP	Yes	7.5	Network	Low
CVE-2023-34453	Oracle Communications Cloud Native Core Network Exposure Function	Platform (Snappy)	HTTP	Yes	7.5	Network	Low
CVE-2025-55163	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	Configuration (Netty)	HTTP/2	Yes	7.5	Network	Low
CVE-2025-41253	Oracle Communications Cloud Native Core Network Repository Function	Install (Spring Cloud Gateway)	HTTP	Yes	7.5	Network	Low
CVE-2025-48976	Oracle Communications Cloud Native Core Network	Signaling (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Repository Function						
CVE-2025-41248	Oracle Communications Cloud Native Core Network Repository Function	Signaling (Spring Security)	HTTP	Yes	7.5	Network	Low
CVE-2025-66418	Oracle Communications Cloud Native Core Network Repository Function	Signaling (urllib3)	HTTP	Yes	7.5	Network	Low
CVE-2025-55163	Oracle Communications Cloud Native Core Network Repository Function	Signaling (Netty)	HTTP/2	Yes	7.5	Network	Low
CVE-2025-67635	Oracle Communications Cloud Native Core Network Slice Selection Function	Install (Jenkins)	HTTP	Yes	7.5	Network	Low
CVE-2025-13151	Oracle Communications Cloud Native Core Network Slice Selection Function	Install (Libtasn1)	HTTP	Yes	7.5	Network	Low
CVE-2025-41253	Oracle Communications Cloud Native Core Network Slice Selection Function	Install (Spring Cloud Gateway)	HTTP	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2026-21452	Oracle Communications Cloud Native Core Policy	Configuration (MessagePack)	HTTP	Yes	7.5	Network	Low
CVE-2026-23490	Oracle Communications Cloud Native Core Policy	Configuration (pyasn1)	HTTP	Yes	7.5	Network	Low
CVE-2026-21441	Oracle Communications Cloud Native Core Policy	Configuration (urllib3)	HTTP	Yes	7.5	Network	Low
CVE-2026-33870	Oracle Communications Cloud Native Core Policy	Install (Netty)	HTTP	Yes	7.5	Network	Low
CVE-2021-0341	Oracle Communications Cloud Native Core Policy	Install (OkHttp)	HTTP	Yes	7.5	Network	Low
CVE-2025-67635	Oracle Communications Cloud Native Core Security Edge Protection Proxy	ATS Framework (Jenkins)	HTTP	Yes	7.5	Network	Low
CVE-2025-66418	Oracle Communications Cloud Native Core Security Edge Protection Proxy	ATS Framework (urllib3)	HTTP	Yes	7.5	Network	Low
CVE-2025-5115	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Automated Test Suite (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2025-41249	Oracle Communications Cloud Native	Signaling (Spring Framework)	HTTP	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Core Security Edge Protection Proxy						
CVE-2025-55163	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Signaling (Netty)	HTTP/2	Yes	7.5	Network	Low
CVE-2025-5115	Oracle Communications Cloud Native Core Service Communication Proxy	Install (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2025-67635	Oracle Communications Cloud Native Core Service Communication Proxy	Signaling (Jenkins)	HTTP	Yes	7.5	Network	Low
CVE-2025-58057	Oracle Communications Cloud Native Core Service Communication Proxy	Signaling (Netty)	HTTP	Yes	7.5	Network	Low
CVE-2025-66418	Oracle Communications Cloud Native Core Service Communication Proxy	Signaling (urllib3)	HTTP	Yes	7.5	Network	Low
CVE-2025-13151	Oracle Communications Cloud Native Core Unified Data Repository	ATS Framework (Libtasn1)	HTTP	Yes	7.5	Network	Low
CVE-2025-66418	Oracle Communications Cloud Native	ATS Framework (urllib3)	HTTP	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Core Unified Data Repository						
CVE-2026-21441	Oracle Communications Cloud Native Core Unified Data Repository	Install (urllib3)	HTTP	Yes	7.5	Network	Low
CVE-2025-5115	Oracle Communications EAGLE Element Management System	Security (Eclipse Jetty)	HTTP	Yes	7.5	Network	Low
CVE-2026-24734	Oracle Communications Element Manager	Third Party (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2025-26333	Oracle Communications Network Integrity	Other (BSAFE Crypto-J)	HTTP	Yes	7.5	Network	Low
CVE-2025-69223	Oracle Communications Operations Monitor	Mediation Engine (AIOHTTP)	HTTP	Yes	7.5	Network	Low
CVE-2026-24734	Oracle Communications Policy Management	Configuration Management Platform (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2026-21441	Oracle Communications Policy Management	Configuration Management Platform (urllib3)	HTTP	Yes	7.5	Network	Low
CVE-2025-58057	Oracle Communications Service Catalog and Design	Patch Request (Netty)	HTTP	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2025-66566	Oracle Communications Service Catalog and Design	Patch Request (lz4-java)	HTTP	Yes	7.5	Network	Low
CVE-2026-24734	Oracle Communications Session Report Manager	Third Party (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2025-26333	Oracle Communications Unified Inventory Management	Security Component (BSAFE Crypto-J)	HTTPS	Yes	7.5	Network	Low
CVE-2025-12383	Oracle Communications Cloud Native Core Policy	Configuration (Eclipse Jersey)	HTTP	Yes	7.4	Network	High
CVE-2025-33042	Oracle Communications Unified Assurance	Core (Apache Avro)	HTTP	Yes	7.3	Network	Low
CVE-2026-3288	Oracle Communications Unified Assurance	Core (Ingress NGINX Controller)	HTTP	No	6.8	Network	Low
CVE-2025-5372	Oracle Communications Unified Assurance	Core (libssh)	SSH	No	6.8	Network	Low
CVE-2025-68615	Oracle Communications Unified Assurance	Core (Net-SNMP)	UDP	No	6.8	Network	Low
CVE-2026-26007	Oracle Communications Cloud Native Core Binding Support Function	Install (Cryptography)	HTTP	Yes	6.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2026-26007	Oracle Communications Cloud Native Core Network Repository Function	Signaling (Cryptography)	HTTP	Yes	6.5	Network	Low
CVE-2026-26007	Oracle Communications Cloud Native Core Policy	Alarms, KPI, and Measurements (Cryptography)	HTTP	Yes	6.5	Network	Low
CVE-2026-26007	Oracle Communications Cloud Native Core Security Edge Protection Proxy	ATS Framework (Cryptography)	Multiple	Yes	6.5	Network	Low
CVE-2026-26007	Oracle Communications Cloud Native Core Service Communication Proxy	ATS Framework (Cryptography)	HTTP	Yes	6.5	Network	Low
CVE-2026-26007	Oracle Communications Operations Monitor	Mediation Engine (Cryptography)	HTTP	Yes	6.5	Network	Low
CVE-2026-25210	Oracle Communications Unified Assurance	Core (LibExpat)	None	No	6.5	Local	Low
CVE-2025-52967	Oracle Communications Unified Assurance	Core (mlflow)	HTTP	No	6.4	Network	High
CVE-2025-14017	Oracle Communications Cloud Native Core Unified Data Repository	ATS Framework (curl)	None	No	6.3	Local	High
CVE-2025-14104	Oracle Communications	Configuration (util-linux)	None	No	6.1	Local	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Cloud Native Core Certificate Management						
CVE-2025-14104	Oracle Communications Cloud Native Core Console	Configuration (util-linux)	None	No	6.1	Local	Low
CVE-2025-26791	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	Configuration (DOMPurify)	HTTP	Yes	6.1	Network	Low
CVE-2026-1642	Oracle Communications Operations Monitor	Mediation Engine (nginx)	HTTP	Yes	5.9	Network	High
CVE-2024-45339	Oracle Communications Unified Assurance	Core (Golang Go)	None	No	5.8	Local	Low
CVE-2025-48795	Oracle Communications Cloud Native Core Unified Data Repository	Security (Apache CXF)	HTTP	Yes	5.6	Network	High
CVE-2025-5318	Oracle Enterprise Communications Broker	Third Party (libssh)	SSH	No	5.4	Network	Low
CVE-2025-61795	Oracle Communications EAGLE Element Management System	Security (Apache Tomcat)	HTTP	No	5.3	Network	High
CVE-2026-23903	Oracle Communications Element Manager	Third Party (Apache Shiro)	HTTP	Yes	5.3	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2026-23903	Oracle Communications Session Report Manager	Third Party (Apache Shiro)	HTTP	Yes	5.3	Network	Low
CVE-2025-15284	Oracle Communications Unified Assurance	Core (qs)	HTTP	No	4.9	Network	Low
CVE-2025-66418	Oracle Communications Unified Assurance	Core (urllib3)	HTTP	No	4.9	Network	Low
CVE-2025-9230	Oracle Communications Unified Assurance	Core (OpenSSL)	HTTPS	No	4.9	Network	Low
CVE-2025-68161	Oracle Communications Billing and Revenue Management	Platform (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications BRM - Elastic Charging Engine	Security issues (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications Convergence	Configuration (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications EAGLE Element Management System	Security (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications Instant Messaging Server	Installation (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications	Installation (Apache	TLS	Yes	4.8	Network	High

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
	Offline Mediation Controller	Log4j)					
CVE-2025-68161	Oracle Communications Order and Service Management	Security (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications Performance Intelligence Center	Management (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications Policy Management	Configuration Management Platform (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications Unified Assurance	Core (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Oracle Communications Unified Inventory Management	Security Component (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-58057	Oracle Communications Unified Assurance	Core (Netty)	HTTP	No	4.5	Network	Low
CVE-2025-41249	Oracle Communications Unified Assurance	Core (Spring Framework)	HTTP	No	4.5	Network	Low
CVE-2025-41248	Oracle Communications Unified Assurance	Core (Spring Security)	HTTP	No	4.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIO		
					Base Score	Attack Vector	Attack Complex
CVE-2025-9086	Oracle Communications Unified Assurance	Core (curl)	HTTP	No	4.5	Network	Low
CVE-2026-26007	Oracle Communications Unified Assurance	Core (Cryptography)	HTTPS	No	4.5	Network	Low
CVE-2026-24734	Oracle Communications Unified Assurance	Core (Apache Tomcat)	TLS	No	4.5	Network	Low
CVE-2026-21637	Oracle Communications Unified Assurance	Core (Node.js)	TLS	No	4.5	Network	Low
CVE-2025-27821	Oracle Communications Unified Assurance	Core (Apache Hadoop)	HTTP	No	4.3	Network	Low
CVE-2025-61984	Oracle Communications Policy Management	Configuration Management Platform (OpenSSH)	None	No	3.6	Local	High
CVE-2025-58181	Oracle Communications Unified Assurance	Core (Golang Crypto)	SSH	No	2.4	Network	Low

Additional CVEs addressed are:

- The patch for CVE-2025-66418 also addresses CVE-2025-66471 and CVE-2026-21441.
- The patch for CVE-2025-5115 also addresses CVE-2025-59474, CVE-2025-59475, and CVE-2025-59476.
- The patch for CVE-2025-58057 also addresses CVE-2024-29857, CVE-2024-30172, CVE-2024-34447, CVE-2025-55163, and CVE-2025-58056.
- The patch for CVE-2025-69223 also addresses CVE-2025-69224, CVE-2025-69225, CVE-2025-69226, CVE-2025-69227, CVE-2025-69228, CVE-2025-69229, and CVE-2025-69230.

- The patch for CVE-2025-67635 also addresses CVE-2025-67636, CVE-2025-67637, CVE-2025-67638, and CVE-2025-67639.
- The patch for CVE-2026-27099 also addresses CVE-2025-67635 and CVE-2026-27100.
- The patch for CVE-2025-55754 also addresses CVE-2022-46337, CVE-2024-52046, CVE-2025-30065, and CVE-2025-47436.
- The patch for CVE-2025-9086 also addresses CVE-2025-10148.
- The patch for CVE-2025-8194 also addresses CVE-2025-6069.
- The patch for CVE-2026-24734 also addresses CVE-2025-66614 and CVE-2026-24733.
- The patch for CVE-2025-14017 also addresses CVE-2025-13034, CVE-2025-14524, CVE-2025-14819, CVE-2025-15079, and CVE-2025-15224.
- The patch for CVE-2026-25968 also addresses CVE-2026-24481, CVE-2026-24484, CVE-2026-24485, CVE-2026-25576, CVE-2026-25637, CVE-2026-25638, CVE-2026-25794, CVE-2026-25795, CVE-2026-25796, CVE-2026-25797, CVE-2026-25798, CVE-2026-25799, CVE-2026-25897, CVE-2026-25898, CVE-2026-25965, CVE-2026-25966, CVE-2026-25967, CVE-2026-25969, CVE-2026-25970, CVE-2026-25971, CVE-2026-25982, CVE-2026-25983, CVE-2026-25985, CVE-2026-25986, CVE-2026-25987, CVE-2026-25988, CVE-2026-25989, CVE-2026-26066, CVE-2026-26283, CVE-2026-26284, CVE-2026-26983, CVE-2026-27798, CVE-2026-27799, CVE-2026-28493, CVE-2026-28494, CVE-2026-28686, CVE-2026-28687, CVE-2026-28688, CVE-2026-28689, CVE-2026-28690, CVE-2026-28691, CVE-2026-28692, CVE-2026-28693, CVE-2026-30883, CVE-2026-30929, CVE-2026-30931, CVE-2026-30935, and CVE-2026-30936.
- The patch for CVE-2025-9900 also addresses CVE-2025-8176, CVE-2025-8177, and CVE-2025-8961.
- The patch for CVE-2025-32990 also addresses CVE-2025-32988, CVE-2025-32989, and CVE-2025-6395.
- The patch for CVE-2026-0861 also addresses CVE-2026-0915.
- The patch for CVE-2026-23903 also addresses CVE-2026-23901.
- The patch for CVE-2026-22022 also addresses CVE-2026-22444.
- The patch for CVE-2025-48913 also addresses CVE-2023-3894, CVE-2024-28752, CVE-2024-29736, CVE-2024-32007, CVE-2024-41172, and CVE-2025-23184.
- The patch for CVE-2026-21637 also addresses CVE-2025-55130, CVE-2025-59465, CVE-2025-59466, and CVE-2026-21636.
- The patch for CVE-2025-58098 also addresses CVE-2025-55753, CVE-2025-59775, CVE-2025-65082, and CVE-2025-66200.
- The patch for CVE-2026-3288 also addresses CVE-2026-24512.
- The patch for CVE-2026-25646 also addresses CVE-2025-64505, CVE-2025-64506, CVE-2025-64720, CVE-2025-65018, CVE-2026-22695, and CVE-2026-22801.
- The patch for CVE-2025-58181 also addresses CVE-2025-22869 and CVE-2025-47914.

- The patch for CVE-2025-52967 also addresses CVE-2024-37059, CVE-2025-0453, CVE-2025-11200, CVE-2025-11201, and CVE-2025-14279.
- The patch for CVE-2025-9230 also addresses CVE-2025-9231 and CVE-2025-9232.

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

- Management Cloud Engine
  - BEServer (Apache Tomcat): CVE-2025-61795 [VEX Justification: inline_mitigations_already_exist].
  - Security (Spring Framework): CVE-2025-41249 [VEX Justification: component_not_present].
  - Security (libssh): CVE-2025-5318 and CVE-2025-4877 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
  - Security (Apache Log4j): CVE-2025-68161 [VEX Justification: component_not_present].
- Oracle Communications Cloud Native Core Binding Support Function
  - Install (LibExpat): CVE-2026-25210 and CVE-2026-24515 [VEX Justification: component_not_present].
- Oracle Communications Cloud Native Core Console
  - Configuration (PCRE2): CVE-2025-58050 [VEX Justification: vulnerable_code_not_present].
- Oracle Communications Cloud Native Core DBTier
  - Install (urllib3): CVE-2026-21441 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Communications Cloud Native Core Network Exposure Function
  - Platform (lz4-java): CVE-2025-66566 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment
  - Configuration (Ingress NGINX Controller): CVE-2026-24512, CVE-2026-1580, CVE-2026-24513 and CVE-2026-24514 [VEX Justification: component_not_present].
  - Configuration (Node.js): CVE-2025-59465, CVE-2025-55130, CVE-2025-55131, CVE-2025-55132, CVE-2025-59466, CVE-2026-21636 and CVE-2026-21637 [VEX Justification: vulnerable_code_not_present].
  - Configuration (OpenSSL): CVE-2025-15467 and CVE-2025-68160 [VEX Justification: vulnerable_code_not_present].

- Oracle Communications Cloud Native Core Network Repository Function
  - Install (Apache Tika): CVE-2025-66516 [VEX Justification: component_not_present].
  - Signaling (Undertow): CVE-2025-12543 and CVE-2024-3884 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Signaling (lz4-java): CVE-2025-66566 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Communications Cloud Native Core Network Slice Selection Function
  - Install (PCRE2): CVE-2025-58050 [VEX Justification: vulnerable_code_not_present].
  - Install (Pillow): CVE-2026-25990 [VEX Justification: vulnerable_code_not_present].
  - Install (lz4-java): CVE-2025-66566 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Communications Cloud Native Core Policy
  - Alarms, KPI, and Measurements (PCRE2): CVE-2025-58050 [VEX Justification: vulnerable_code_not_present].
  - Install (Apache Tika): CVE-2025-66516 [VEX Justification: component_not_present].
  - Alarms, KPI, and Measurements (LibExpat): CVE-2026-25210 and CVE-2026-24515 [VEX Justification: vulnerable_code_not_present].
- Oracle Communications Cloud Native Core Security Edge Protection Proxy
  - Configuration (Pillow): CVE-2026-25990 [VEX Justification: vulnerable_code_not_present].
  - Signaling (PCRE2): CVE-2025-58050 [VEX Justification: vulnerable_code_not_present].
  - Signaling (Spring Security): CVE-2025-41248 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Communications Cloud Native Core Service Communication Proxy
  - Install (LibTIFF): CVE-2025-9900 and CVE-2025-8176 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Install (lz4-java): CVE-2025-66566 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Signaling (Eclipse Jetty): CVE-2025-5115 [VEX Justification: component_not_present].
  - Signaling (PCRE2): CVE-2025-58050 [VEX Justification: vulnerable_code_not_present].
- Oracle Communications Cloud Native Core Unified Data Repository
  - Install (PCRE2): CVE-2025-58050 [VEX Justification: vulnerable_code_not_present].
  - Install (lz4-java): CVE-2025-66566 [VEX Justification: vulnerable_code_not_in_execute_path].

- Oracle Communications Session Border Controller
  - Third Party (OpenSSL): CVE-2025-15467 and CVE-2025-68160 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Enterprise Communications Broker
  - Third Party (OpenSSL): CVE-2025-15467 [VEX Justification: component_not_present].

Oracle Construction and Engineering Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-52999	Primavera P6 Enterprise Project Portfolio Management	Web Access (jackson-core)	HTTP	Yes	6.5	Network	Low	Non
CVE-2025-48795	Primavera P6 Enterprise Project Portfolio Management	P6 Web Services (Apache CXF)	HTTP	Yes	5.6	Network	High	Non

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-68161	Primavera Unifier	Platform (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-26791	Primavera P6 Enterprise Project Portfolio Management	P6WS (DOMPurify)	HTTP	No	4.1	Network	Low	Lov

Additional CVEs addressed are:

- The patch for CVE-2025-48795 also addresses CVE-2025-23184.

Oracle E-Business Suite Risk Matrix

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 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 April 2026 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 (April 2026), My Oracle Support Note KA923.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2026-34275	Oracle Advanced Inbound Telephony	Setup and Administration	HTTP	Yes	9.8	Network	Low
CVE-2024-51504	Oracle Enterprise Command Center Framework	Core (Apache ZooKeeper)	TCP	Yes	9.1	Network	Low
CVE-2025-48734	Oracle Advanced Supply Chain Planning	User Interface (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low
CVE-2025-48734	Oracle Flow Manufacturing	Security (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low
CVE-2025-48734	Oracle Global Order Promising	Web Service (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low
CVE-2025-48734	Oracle iProcurement	iProcurement ECC shopping (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low
CVE-2025-48734	Oracle Rapid Planning	User Interface (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low
CVE-2025-48734	Oracle Yard Management	Installation (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2026-22011	Oracle Applications DBA	ADPatch	HTTP	No	7.6	Network	High
CVE-2025-58057	Oracle Enterprise Command Center Framework	ECC Core (Netty)	HTTP	Yes	7.5	Network	Low
CVE-2026-34297	Oracle HCM Common Architecture	Knowledge Integration	HTTP	Yes	7.5	Network	Low
CVE-2026-34274	Oracle Configurator	User Interface	HTTP	Yes	6.1	Network	Low
CVE-2025-41242	Oracle Enterprise Command Center Framework	ECC Core (Spring Framework)	HTTP	Yes	5.9	Network	High
CVE-2026-34302	Oracle Workflow	Workflow Loader	HTTP	No	5.5	Network	Low
CVE-2025-31672	Oracle Enterprise Command Center Framework	ECC Core (Apache POI)	HTTP	Yes	5.3	Network	Low
CVE-2025-68161	Oracle Enterprise Command Center Framework	ECC Core (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2026-34298	Oracle Applications Framework	Personalization	HTTP	No	4.7	Network	Low
CVE-2026-22014	Oracle User Management	Workflow and Business Events	HTTP	No	3.8	Network	Low

Additional CVEs addressed are:

- The patch for CVE-2025-41242 also addresses CVE-2024-38820 and CVE-2025-22233.

- The patch for CVE-2025-58057 also addresses CVE-2023-44981, CVE-2024-13009, CVE-2024-23944, CVE-2024-47535, CVE-2024-51504, CVE-2024-6763, CVE-2025-24970, and CVE-2025-25193.

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Enterprise Manager. 8 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 April 2026 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 April 2026 Patch Availability Document for Oracle Products, My Oracle Support Note CPU59.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2026-34279	Oracle Enterprise Manager Base Platform	Event Management	HTTP	No	9.1	Network	Low	Hi
CVE-2024-56406	Oracle Enterprise Manager Base Platform	Agent Next Gen (Perl)	HTTP	Yes	8.6	Network	Low	No
CVE-2024-56406	Oracle Enterprise Manager	Enterprise Manager Install (Perl)	HTTP	Yes	8.6	Network	Low	No

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Base Platform							
CVE-2025-26333	Oracle Application Testing Suite	Load Testing for Web Apps (BSAFE Crypto-J)	HTTPS	Yes	7.5	Network	Low	No
CVE-2025-52999	Oracle Enterprise Manager Base Platform	Security Framework (jackson-core)	HTTP	Yes	7.5	Network	Low	No
CVE-2025-41249	Oracle Enterprise Manager for Fusion Middleware	Infrastructure Management (Spring Framework)	HTTP	Yes	7.5	Network	Low	No
CVE-2025-68161	Oracle Configuration Manager	OCM Request Tunnel (Apache Log4j)	TLS	Yes	4.8	Network	High	No
CVE-2025-68161	Oracle Enterprise Manager Base Platform	Enterprise Manager Install (Apache Log4j)	TLS	Yes	4.8	Network	High	No
CVE-2025-68161	Oracle Enterprise Manager Base Platform	Oracle Management Service (Apache Log4j)	TLS	Yes	4.8	Network	High	No

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 75 new security patches, plus additional third party patches noted below, for Oracle Financial Services Applications. 59 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 ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
CVE-2023-34034	Oracle Banking Origination	Onboarding Batch Processes (Spring Security)	HTTP	Yes	9.8	Network	Low	I
CVE-2023-44981	Oracle Banking Corporate Lending Process Management	Base (Apache ZooKeeper)	HTTP	Yes	9.1	Network	Low	I
CVE-2023-44981	Oracle Banking Supply Chain Finance	Security (Apache ZooKeeper)	HTTP	Yes	9.1	Network	Low	I
CVE-2023-44981	Oracle Banking Trade Finance Process Management	Common (Apache ZooKeeper)	HTTP	Yes	9.1	Network	Low	I
CVE-2025-48734	Oracle Banking Corporate Lending Process Management	Base (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low	
CVE-2025-48734	Oracle Banking Origination	Configuration (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low	
CVE-2025-48734	Oracle Insurance Policy Administration Operational Data Store for Life and Annuity	Logger (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low	
CVE-2026-25210	Oracle Financial Services	Third Party (LibExpat)	None	No	7.8	Local	Low	

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
	Behavior Detection Platform							
CVE-2026-25210	Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition	Platform (LibExpat)	None	No	7.8	Local	Low	
CVE-2025-41249	Oracle Banking Branch	Reports (Spring Framework)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-41248	Oracle Banking Branch	Reports (Spring Security)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-66566	Oracle Banking Branch	Reports (lz4-java)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-41249	Oracle Banking Cash Management	Accessibility (Spring Framework)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-66566	Oracle Banking Cash Management	Common (lz4-java)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Collections and Recovery	Infrastructure (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-41249	Oracle Banking Corporate Lending	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-41249	Oracle Banking Corporate Lending Process Management	Base (Spring Framework)	HTTP	Yes	7.5	Network	Low	I

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
CVE-2025-66566	Oracle Banking Corporate Lending Process Management	Base (lz4-java)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Corporate Lending Process Management	Core (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-27817	Oracle Banking Corporate Lending Process Management	Base (Apache Kafka)	HTTPS	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Credit Facilities Process Management	Common (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-5115	Oracle Banking Credit Facilities Process Management	Common (Eclipse Jetty)	HTTP/2	Yes	7.5	Network	Low	I
CVE-2025-27817	Oracle Banking Credit Facilities Process Management	Common (Apache Kafka)	HTTPS	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Origination	Configuration (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-41249	Oracle Banking Origination	Configuration (Spring Framework)	HTTP	Yes	7.5	Network	Low	I

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
CVE-2025-66566	Oracle Banking Origination	Configuration (lz4-java)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-1948	Oracle Banking Origination	Configuration (Eclipse Jetty)	HTTP/2	Yes	7.5	Network	Low	I
CVE-2025-55163	Oracle Banking Origination	Configuration (Netty)	HTTP/2	Yes	7.5	Network	Low	I
CVE-2025-27817	Oracle Banking Origination	Configuration (Apache Kafka)	HTTPS	Yes	7.5	Network	Low	I
CVE-2025-55163	Oracle Banking Payments	Payments (Netty)	HTTP/2	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Supply Chain Finance	Security (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-27817	Oracle Banking Supply Chain Finance	Security (Apache Kafka)	HTTPS	Yes	7.5	Network	Low	I
CVE-2025-41249	Oracle Banking Trade Finance	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Trade Finance Process Management	Dashboard (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-55163	Oracle Banking Trade Finance Process Management	Dashboard (Netty)	HTTP/2	Yes	7.5	Network	Low	I
CVE-2025-27817	Oracle Banking Trade Finance	Dashboard (Apache Kafka)	HTTPS	Yes	7.5	Network	Low	I

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
	Process Management							
CVE-2025-41249	Oracle Banking Virtual Account Management	Common Core (Spring Framework)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle Banking Virtual Account Management	Core (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-27817	Oracle Banking Virtual Account Management	Core (Apache Kafka)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-55163	Oracle Banking Virtual Account Management	Core (Netty)	HTTP/2	Yes	7.5	Network	Low	I
CVE-2026-34310	Oracle Financial Services Analytical Applications Infrastructure	Platform	HTTP	Yes	7.5	Network	Low	I
CVE-2026-22010	Oracle Financial Services Analytical Applications Infrastructure	Platform	HTTP	Yes	7.5	Network	Low	I
CVE-2025-27820	Oracle Financial Services Analytical Applications Infrastructure	Platform (Apache HttpClient)	HTTP	Yes	7.5	Network	Low	I

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
CVE-2026-25990	Oracle Financial Services Compliance Studio	Reports (Pillow)	HTTP	Yes	7.5	Network	Low	I
CVE-2026-34320	Oracle Financial Services Customer Screening	User Interface	HTTP	Yes	7.5	Network	Low	I
CVE-2025-27820	Oracle Financial Services Regulatory Reporting	Installer (Apache HttpClient)	HTTP	Yes	7.5	Network	Low	I
CVE-2026-35231	Oracle Financial Services Transaction Filtering	User Interface	HTTP	Yes	7.5	Network	Low	I
CVE-2025-48976	Oracle FLEXCUBE Enterprise Limits and Collateral Management	Infrastructure (Apache Commons FileUpload)	HTTP	Yes	7.5	Network	Low	I
CVE-2025-27821	Oracle Financial Services Model Management and Governance	Installer (Apache Hadoop)	HTTP	Yes	7.3	Network	Low	I
CVE-2026-34314	Oracle Financial Services Analytical Applications Infrastructure	Platform	HTTP	No	6.8	Network	High	
CVE-2026-34325	Oracle Financial	User Interface	None	No	6.8	Local	Low	

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Services Analytical Applications Infrastructure							
CVE-2025-67735	Oracle Banking Liquidity Management	Infrastructure (Netty)	HTTP	Yes	6.5	Network	Low	
CVE-2025-12183	Oracle Banking Liquidity Management	Infrastructure (lz4-java)	HTTP	No	6.5	Network	Low	
CVE-2026-34313	Oracle Financial Services Analytical Applications Infrastructure	Platform	HTTP	No	6.5	Network	Low	
CVE-2023-20863	Oracle Insurance Policy Administration Operational Data Store for Life and Annuity	Logger (Spring Framework)	HTTP	No	6.5	Network	Low	
CVE-2021-28168	Oracle Financial Services Analytical Applications Infrastructure	Platform (Eclipse Jersey)	None	No	5.5	Local	Low	
CVE-2025-48924	Oracle Banking Trade Finance	Core (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	
CVE-2025-48924	Oracle Banking Virtual Account Management	Common Core (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
CVE-2025-48924	Oracle Banking Virtual Account Management	Platform (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	I
CVE-2025-48924	Oracle Documaker	Documaker Core (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	I
CVE-2025-41249	Oracle Documaker	Documaker Core (Spring Framework)	HTTP	Yes	5.3	Network	Low	I
CVE-2025-48924	Oracle Financial Services Lending and Leasing	Apache Commons (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	I
CVE-2025-46392	Oracle Banking Virtual Account Management	Common Core (Apache Commons Configuration)	HTTP	No	4.9	Network	Low	
CVE-2025-48976	Oracle Banking Virtual Account Management	Platform (Apache Commons FileUpload)	HTTP	No	4.9	Network	Low	
CVE-2025-58057	Oracle Banking Virtual Account Management	Platform (Netty)	HTTP	No	4.9	Network	Low	
CVE-2025-68161	Oracle Banking Virtual Account Management	Platform (Apache Log4j)	TLS	Yes	4.8	Network	High	I
CVE-2026-34321	Oracle Financial Services Analytical	User Interface	HTTP	No	4.8	Network	High	

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
	Applications Infrastructure							
CVE-2025-68161	Oracle Financial Services Analytical Applications Infrastructure	Platform (Apache Log4j)	TLS	Yes	4.8	Network	High	
CVE-2025-68161	Oracle Financial Services Behavior Detection Platform	Third Party (Apache Log4j)	TLS	Yes	4.8	Network	High	
CVE-2025-68161	Oracle Financial Services Enterprise Case Management	Installers (Apache Log4j)	TLS	Yes	4.8	Network	High	
CVE-2025-68161	Oracle Financial Services Model Management and Governance	Installer (Apache Log4j)	TLS	Yes	4.8	Network	High	
CVE-2025-68161	Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition	Platform (Apache Log4j)	TLS	Yes	4.8	Network	High	
CVE-2025-68161	Oracle Insurance Policy Administration J2EE	Architecture (Apache Log4j)	TLS	Yes	4.8	Network	High	

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	I P
CVE-2025-41254	Oracle Financial Services Analytical Applications Infrastructure	Platform (Spring Framework)	HTTP	Yes	4.3	Network	Low	I
CVE-2025-27636	Oracle Banking Virtual Account Management	Platform (Apache Camel)	HTTP	No	4.1	Network	High	

Additional CVEs addressed are:

- The patch for CVE-2025-41249 also addresses CVE-2025-22233 and CVE-2025-41242.
- The patch for CVE-2026-25210 also addresses CVE-2026-24515.
- The patch for CVE-2023-34034 also addresses CVE-2023-20862 and CVE-2023-34035.
- The patch for CVE-2025-27817 also addresses CVE-2025-27818.
- The patch for CVE-2025-58057 also addresses CVE-2025-58056.

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

- Oracle Banking Liquidity Management
  - Common (Apache Tika): CVE-2025-66516 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Banking Virtual Account Management
  - Platform (Apache Tika): CVE-2025-66516 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 59 new security patches, plus additional third party patches noted below, 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 English text form of this Risk Matrix can be found here.

To get the full list of current and previously released Critical Patch Update patches for Oracle Fusion Middleware products, refer to My Oracle Support Doc ID KA1182.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2022-45047	Oracle Managed File Transfer	Runtime Server (Apache Mina SSHD)	SSH	Yes	9.8	Network	Low	Nor
CVE-2025-68615	Oracle Tuxedo	Docs-ATMI-IB (Net-SNMP)	UDP	Yes	9.8	Network	Low	Nor
CVE-2026-34285	Oracle Identity Manager Connector	Core	HTTPS	Yes	9.1	Network	Low	Nor
CVE-2026-34286	Oracle Identity Manager Connector	Core	HTTPS	Yes	9.1	Network	Low	Nor
CVE-2026-34287	Oracle Identity Manager Connector	Core	HTTPS	Yes	9.1	Network	Low	Nor
CVE-2021-45046	Oracle Business Activity Monitoring	Centralized Thirdparty Jars (Apache Log4j)	HTTP	Yes	9.0	Network	High	Nor
CVE-2026-34291	Oracle HTTP Server	Core	HTTP	Yes	8.7	Network	High	Nor
CVE-2025-58098	Oracle HTTP Server	Core (Apache HTTP Server)	HTTP	No	8.3	Network	Low	Lo
CVE-2026-25646	Oracle Outside In Technology	DC-Specific Component (libpng)	HTTP	Yes	8.1	Network	High	Nor

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2026-35243	Oracle Application Development Framework (ADF)	ADF Faces	None	No	7.8	Local	Low	Lo
CVE-2026-25210	Oracle Outside In Technology	DC-Specific Component (LibExpat)	None	No	7.8	Local	Low	Lo
CVE-2026-22184	Oracle Outside In Technology	Outside In Maintenance (zlib)	None	No	7.8	Local	Low	Lo
CVE-2025-52999	Oracle Business Process Management Suite	Document Service (jackson-core)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2024-43394	Oracle HTTP Server	Core (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2025-59775	Oracle HTTP Server	Core (Apache HTTP Server)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2026-34290	Oracle Identity Manager Connector	Core	TCP	Yes	7.5	Network	Low	Nor
CVE-2024-29857	Oracle SOA Suite	B2B Engine (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	Nor
CVE-2025-41249	Oracle WebCenter Forms Recognition	Learnset Manager (Spring Framework)	HTTP	Yes	7.5	Network	Low	Nor
CVE-2026-34305	Oracle WebLogic Server	Web Services	HTTP	Yes	7.5	Network	Low	Nor

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-12383	Oracle SOA Suite	B2B Engine (Eclipse Jersey)	HTTPS	Yes	7.4	Network	High	Non
CVE-2025-0725	Oracle Access Manager	Web Server Plugin (curl)	HTTP	Yes	7.3	Network	Low	Non
CVE-2025-33042	Oracle Business Process Management Suite	Composer (Apache Avro)	HTTP	Yes	7.3	Network	Low	Non
CVE-2025-33042	Oracle Middleware Common Libraries and Tools	Third Party (Apache Avro)	HTTP	Yes	7.3	Network	Low	Non
CVE-2025-35036	Oracle Middleware Common Libraries and Tools	Third Party (Validator)	HTTP	Yes	7.3	Network	Low	Non
CVE-2021-22573	Oracle Middleware Common Libraries and Tools	Third Party (Google OAuth Client)	HTTPS	No	7.3	Network	Low	Lo
CVE-2025-33042	Oracle SOA Suite	Adapters (Apache Avro)	HTTP	Yes	7.3	Network	Low	Non
CVE-2025-35036	Oracle WebLogic Server	Centralized Thirdparty Jars (Validator)	HTTP	Yes	7.3	Network	Low	Non
CVE-2024-13009	Oracle Identity Manager	Third Party (jackson-databind)	HTTP	Yes	7.2	Network	Low	Non
CVE-2026-34292	Oracle WebLogic Server	Core	HTTP	No	7.2	Network	Low	Hig

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2023-2976	Oracle Managed File Transfer	Oracle MFT Installer (Google Guava)	None	No	7.1	Local	Low	Lo
CVE-2025-68431	Oracle Outside In Technology	DC-Specific Component (libheif)	HTTP	Yes	7.1	Network	Low	Nor
CVE-2026-21939	Oracle Fusion Middleware	Oracle Database Client for Fusion Middleware	None	No	7.0	Local	High	Nor
CVE-2025-65082	Oracle HTTP Server	Core (Apache HTTP Server)	HTTP	Yes	6.5	Network	Low	Nor
CVE-2026-34315	Oracle WebLogic Server	Web Services	HTTP	Yes	6.5	Network	Low	Nor
CVE-2025-46392	Oracle WebLogic Server	Centralized Thirdparty Jars (Apache Commons Lang)	HTTPS	No	6.5	Network	Low	Lo
CVE-2026-35252	Oracle Security Service	C Oracle SSL API	HTTPS	No	6.4	Network	High	Lo
CVE-2026-34284	Oracle Business Process Management Suite	Human workflow 11g+	HTTP	Yes	6.1	Network	Low	Nor
CVE-2026-34283	Oracle Identity Manager	Identity Console	HTTP	Yes	6.1	Network	Low	Nor
CVE-2026-34288	Oracle Identity Manager Connector	Core	HTTP	Yes	5.9	Network	High	Nor

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2026-34289	Oracle Identity Manager Connector	Core	HTTPS	Yes	5.9	Network	High	Non
CVE-2026-34294	Oracle Identity Manager Connector	Microsoft Active Directory	LDAP	No	5.9	Network	High	Lo
CVE-2025-53864	Oracle Data Integrator	Security (Nimbus JOSE+JWT)	HTTP	Yes	5.8	Network	Low	Non
CVE-2026-35232	Oracle Fusion Middleware	Dynamic Monitoring Service	HTTP	No	5.4	Network	Low	Lo
CVE-2025-48924	Oracle Application Development Framework (ADF)	ADF Faces (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	Non
CVE-2025-31672	Oracle Application Development Framework (ADF)	ADF Faces (Apache POI)	HTTP	Yes	5.3	Network	Low	Non
CVE-2025-48924	Oracle Business Process Management Suite	Composer (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	Non
CVE-2025-48924	Oracle Middleware Common Libraries and Tools	Third Party (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	Non
CVE-2025-8916	Oracle Middleware Common Libraries and Tools	Thirdparty Patch (Bouncy Castle Java Library)	HTTPS	Yes	5.3	Network	Low	Non

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-48924	Oracle Web Services Manager	Third Party (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	Non
CVE-2025-8916	Oracle WebLogic Server	Centralized Thirdparty Jars (Bouncy Castle Java Library)	HTTPS	Yes	5.3	Network	Low	Non
CVE-2025-68161	Oracle Business Process Management Suite	Runtime Engine (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle Data Integrator	Security (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle Identity Manager	Installer (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle Managed File Transfer	MFT Runtime Server (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle Middleware Common Libraries and Tools	Thirdparty Patch (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle WebCenter Sites	Thick Client (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle WebLogic Server	Centralized Third Party Jars (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-41254	Oracle Middleware Common	Third Party (Spring Web Services)	HTTP	Yes	4.3	Network	Low	Non

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Libraries and Tools							
CVE-2024-31573	Oracle SOA Suite	Fabric Layer (xmlunit)	None	No	4.0	Local	High	Non

Notes:

1. This vulnerability applies to Windows only.

Additional CVEs addressed are:

- The patch for CVE-2021-45046 also addresses CVE-2025-48924.
- The patch for CVE-2022-45047 also addresses CVE-2023-48795.
- The patch for CVE-2024-29857 also addresses CVE-2025-8885.
- The patch for CVE-2026-25210 also addresses CVE-2026-24515.
- The patch for CVE-2025-58098 also addresses CVE-2025-54090.
- The patch for CVE-2025-46392 also addresses CVE-2025-48924.

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

- Oracle HTTP Server
  - ModSecurity (curl): CVE-2025-14017, CVE-2025-10148, CVE-2025-13034, CVE-2025-14524, CVE-2025-14819, CVE-2025-15079 and CVE-2025-15224 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Analytics Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle Analytics. 11 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-27727	Oracle Business Intelligence Enterprise Edition	Platform Security (Mchange Commons Java)	LDAP	Yes	9.8	Network	Low	None
CVE-2026-27830	Oracle Business Intelligence Enterprise Edition	Platform Security (c3p0)	LDAP	No	9.0	Adjacent Network	Low	Low
CVE-2025-48734	Oracle Business Intelligence Enterprise Edition	Platform Security (Apache Commons BeanUtils)	HTTP	No	8.8	Network	Low	Low
CVE-2025-15467	Oracle Business Intelligence Enterprise Edition	BI Platform Security (OpenSSL)	TLS	Yes	8.8	Network	Low	None
CVE-2025-46762	Oracle Business Intelligence Enterprise Edition	Platform Security (Apache Parquet Java)	HTTP	Yes	8.1	Network	High	None
CVE-2026-21441	Oracle Business Intelligence Enterprise Edition	Pipeline Test Failures (urllib3)	HTTP	Yes	7.5	Network	Low	None
CVE-2025-58057	Oracle Business Intelligence Enterprise Edition	Platform Security (Netty)	HTTP	Yes	7.5	Network	Low	None
CVE-2023-52428	Oracle Business Intelligence Enterprise Edition	Platform Security (Nimbus JOSE+JWT)	HTTP	Yes	7.5	Network	Low	None

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2025-24970	Oracle Business Intelligence Enterprise Edition	Analytics Server (Netty)	TLS	Yes	7.5	Network	Low	None
CVE-2025-33042	Oracle Business Intelligence Enterprise Edition	Platform Security (Apache Avro)	HTTP	Yes	7.3	Network	Low	None
CVE-2021-28168	Oracle Business Intelligence Enterprise Edition	Platform Security (Eclipse Jersey)	None	No	5.5	Local	Low	Low
CVE-2025-48924	Oracle BI Publisher	BI Publisher Microservice (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	None
CVE-2025-59419	Oracle Business Intelligence Enterprise Edition	Platform Security (netty-codec-smtp)	SMTP	Yes	5.3	Network	Low	None
CVE-2025-68161	Oracle Business Intelligence Enterprise Edition	Analytics Server (Apache Log4j)	TLS	Yes	4.8	Network	High	None
CVE-2023-35116	Oracle Business Intelligence Enterprise Edition	Platform Security (jackson-databind)	None	No	4.7	Local	High	Low

Additional CVEs addressed are:

- The patch for CVE-2025-15467 also addresses CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, and CVE-2026-22796.
- The patch for CVE-2025-58057 also addresses CVE-2025-55163 and CVE-2025-58056.

Oracle Life Science Applications Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Life Science 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 ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-21997	Oracle Life Sciences Empirica Signal	Common Core	HTTP	No	8.5	Network	Low	Low
CVE-2026-34324	Oracle Life Sciences InForm	App Server	HTTP	Yes	6.5	Network	Low	None
CVE-2026-34323	Oracle Life Sciences InForm	IDM Authentication	HTTP	Yes	6.3	Network	Low	None
CVE-2025-68161	Oracle Life Sciences Empirica Signal	Common Core (Apache Log4j)	TLS	Yes	4.8	Network	High	None

Oracle Hospitality Applications Risk Matrix

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

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2026-24734	Oracle Hospitality Cruise Shipboard Property Management (SPMS)	Next-Gen SPMS (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	Non

Additional CVEs addressed are:

- The patch for CVE-2026-24734 also addresses CVE-2025-61795.

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 ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2025-64775	Oracle Hyperion Infrastructure Technology	Installation and Configuration (Apache Struts)	HTTP	Yes	7.5	Network	Low	No
CVE-2025-9086	Oracle Hyperion Infrastructure Technology	Installation and Configuration (curl)	HTTP	Yes	7.5	Network	Low	No
CVE-2025-66566	Oracle Hyperion Infrastructure Technology	Installation and Configuration (lz4-java)	HTTP	Yes	7.5	Network	Low	No
CVE-2025-65018	Oracle Hyperion	Installation and	None	No	7.1	Local	Low	No

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Infrastructure Technology	Configuration (libpng)						
CVE-2025-54571	Oracle Hyperion Infrastructure Technology	Installation and Configuration (ModSecurity)	HTTP	Yes	6.1	Network	Low	N
CVE-2026-35244	Oracle Hyperion Infrastructure Technology	Lifecycle Management	HTTP	No	5.2	Network	Low	H

Additional CVEs addressed are:

- The patch for CVE-2025-9086 also addresses CVE-2025-10148.
- The patch for CVE-2025-65018 also addresses CVE-2025-64505, CVE-2025-64506, and CVE-2025-64720.

Oracle Java SE Risk Matrix

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

The CVSS scores below assume that a user running a Java applet or Java Web Start application has administrator privileges (typical on Windows). When the user does not run with administrator privileges (typical on Solaris and Linux), the corresponding CVSS impact scores for Confidentiality, Integrity, and Availability are "Low" instead of "High", lowering the CVSS Base Score. For example, a Base Score of 9.6 becomes 7.1.

Java Management Service, available to all users, can help you find vulnerable Java versions in your systems. Java SE Subscribers and customers running in Oracle Cloud can use Java Management Service to update Java Runtimes and to do further security reviews like identifying potentially vulnerable third party libraries used by your Java programs. Existing Java Management Service user click here to log in to your dashboard. The Java Management Service Documentation provides a list of features available to everyone and those available

only to customers. Learn more about using Java Management Service to monitor and secure your Java Installations.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-20652	Oracle Java SE	JavaFX (WebKitGTK)	Multiple	Yes	7.5	Network	Low	None
CVE-2026-22016	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	JAXP	Multiple	Yes	7.5	Network	Low	None
CVE-2026-34282	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	Networking	Multiple	Yes	7.5	Network	Low	None

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-22003	Oracle Java SE, Oracle GraalVM Enterprise Edition	Hotspot	None	No	6.0	Local	High	Low
CVE-2026-22021	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	JSSE	HTTPS	Yes	5.3	Network	Low	None
CVE-2026-22013	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	JGSS	Multiple	Yes	5.3	Network	High	None

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-23865	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	2D (FreeType)	None	No	5.3	Local	Low	None
CVE-2026-22008	Oracle Java SE	Libraries	Multiple	Yes	3.7	Network	High	None
CVE-2026-22018	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	Libraries	Multiple	Yes	3.7	Network	High	None

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-22007	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	Security	None	No	2.9	Local	High	None
CVE-2026-34268	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	Security	None	No	2.9	Local	High	None

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd

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 can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also 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.

Additional CVEs addressed are:

- The patch for CVE-2026-20652 also addresses CVE-2025-43457, CVE-2026-20608, CVE-2026-20635, CVE-2026-20636, CVE-2026-20644, and CVE-2026-20676.

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

- Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition
    - AWT (libpng): CVE-2026-22801, CVE-2025-64505, CVE-2025-64506, CVE-2025-64720, CVE-2025-65018, CVE-2025-66293 and CVE-2026-22695 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].

Oracle JD Edwards Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2025-9230	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure Security (OpenSSL)	HTTPS	Yes	7.5	Network	Low	N
CVE-2023-5388	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure Security (NSS)	HTTPS	Yes	6.5	Network	Low	N
CVE-2025-48924	JD Edwards EnterpriseOne Tools	Web Runtime Security (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	N

Additional CVEs addressed are:

- The patch for CVE-2025-9230 also addresses CVE-2025-9231 and CVE-2025-9232.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 34 new security patches, plus additional third party patches noted below, for Oracle MySQL. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-15467	MySQL Enterprise Backup	Enterprise Backup (OpenSSL)	TLS	Yes	9.8	Network	Low	Nor
CVE-2025-15467	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	Yes	9.8	Network	Low	Nor

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-15467	MySQL Workbench	MySQL Workbench (OpenSSL)	MySQL Workbench	Yes	9.8	Network	Low	Nor
CVE-2026-34270	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-34271	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-34276	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-34308	MySQL Server	Server: JSON	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-22009	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-22017	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-34272	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov
CVE-2026-34303	MySQL Server	Server: Optimizer	MySQL Protocol	No	6.5	Network	Low	Lov

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2025-14017	MySQL Enterprise Backup	Enterprise Backup (curl)	None	No	6.3	Local	High	Nor
CVE-2025-14017	MySQL Server	Server: Packaging (curl)	None	No	6.3	Local	High	Nor
CVE-2026-34318	MySQL Shell	Shell: Core Client	Multiple	No	5.8	Network	High	Hig
CVE-2025-5318	MySQL Cluster	Cluster: General (libssh)	Multiple	No	5.4	Network	Low	Lo
CVE-2026-34317	MySQL Shell	Shell: Core Client	None	No	5.0	Local	Low	Lo
CVE-2026-34319	MySQL Shell	Shell: Core Client	None	No	5.0	Local	Low	Lo
CVE-2026-22004	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-34304	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-35236	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2026-35237	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-35238	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-34293	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-35239	MySQL Server	Server: DML	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-35235	MySQL Server	Server: GIS	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-21998	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-22005	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-22002	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-34267	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2026-34278	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-35240	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-35234	MySQL Server	Server: Partition	MySQL Protocol	No	4.9	Network	Low	Hig
CVE-2026-22015	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.3	Network	Low	Lo
CVE-2026-22001	MySQL Server	Server: Information Schema	MySQL Protocol	No	2.7	Network	Low	Hig

Additional CVEs addressed are:

- The patch for CVE-2025-5318 also addresses CVE-2025-4877, CVE-2025-4878, CVE-2025-5351, CVE-2025-5372, CVE-2025-5449, and CVE-2025-5987.
- The patch for CVE-2025-14017 also addresses CVE-2025-13034, CVE-2025-14524, CVE-2025-14819, CVE-2025-15079, and CVE-2025-15224.

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

- MySQL Connectors
  - Connector/C++ (OpenSSL): CVE-2025-15467 and CVE-2025-11187 [VEX Justification: vulnerable_code_not_in_execute_path].
  - Connector/ODBC (OpenSSL): CVE-2025-15467 and CVE-2025-11187 [VEX Justification: vulnerable_code_not_in_execute_path].
- MySQL Workbench
  - MySQL Workbench (libpng): CVE-2026-25646 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle PeopleSoft Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2025-15467	PeopleSoft Enterprise PeopleTools	Security (OpenSSL)	HTTPS	Yes	8.8	Network	Low	Nc
CVE-2026-34309	PeopleSoft Enterprise PeopleTools	Security	HTTP	No	8.1	Network	Low	Lc
CVE-2025-58754	PeopleSoft Enterprise CC Common Application Objects	Common Application Objects (Axios)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2025-8194	PeopleSoft Enterprise PeopleTools	Porting (Python)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2025-66418	PeopleSoft Enterprise PeopleTools	Porting (urllib3)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2025-43967	PeopleSoft Enterprise PeopleTools	XMLPublisher (libheif)	HTTP	Yes	7.5	Network	Low	Nc
CVE-2026-34277	PeopleSoft Enterprise PeopleTools	Fluid Core	HTTP	No	6.6	Network	Low	Hi
CVE-2026-34300	PeopleSoft Enterprise FIN Contracts	Contracts	HTTP	No	6.5	Network	Low	Lc
CVE-2026-34299	PeopleSoft Enterprise FIN	Work Order Management	HTTP	No	6.5	Network	Low	Lc

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
	Maintenance Management							
CVE-2026-34301	PeopleSoft Enterprise FIN Maintenance Management	Work Order Management	HTTP	No	6.5	Network	Low	Lo
CVE-2026-34306	PeopleSoft Enterprise FIN Project Costing	Projects	HTTP	No	6.5	Network	Low	Lo
CVE-2026-34266	PeopleSoft Enterprise HCM Absence Management	Absence Management	HTTP	No	6.5	Network	Low	Hi
CVE-2026-34280	PeopleSoft Enterprise HCM Human Resources	Job Profile Manager	HTTP	No	6.5	Network	Low	Hi
CVE-2026-34295	PeopleSoft Enterprise SCM Purchasing	Purchasing	HTTP	No	6.5	Network	Low	Lo
CVE-2025-14017	PeopleSoft Enterprise PeopleTools	File Processing (libcurl)	None	No	6.3	Local	High	No
CVE-2026-34269	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	No
CVE-2026-35241	PeopleSoft Enterprise CS Student Records	Research Tracking	HTTP	No	5.7	Network	Low	Lo
CVE-2026-22006	PeopleSoft Enterprise HCM Human Resources	Employee Snapshot	HTTP	No	5.4	Network	Low	Lo
CVE-2026-22019	PeopleSoft Enterprise	Person Search	HTTP	No	5.4	Network	Low	Lo

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.			
					Base Score	Attack Vector	Attack Complex	Pr Re
	HCM Shared Components							
CVE-2026-34307	PeopleSoft Enterprise PeopleTools	Workflow	HTTP	No	5.4	Network	Low	Lo
CVE-2025-68161	PeopleSoft Enterprise PeopleTools	OpenSearch (Apache Log4j)	TLS	Yes	4.8	Network	High	No

Additional CVEs addressed are:

- The patch for CVE-2025-15467 also addresses CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, and CVE-2026-22796.
- The patch for CVE-2025-66418 also addresses CVE-2025-66471.
- The patch for CVE-2025-8194 also addresses CVE-2025-6069.
- The patch for CVE-2025-14017 also addresses CVE-2025-13034, CVE-2025-14524, CVE-2025-14819, CVE-2025-15079, and CVE-2025-15224.
- The patch for CVE-2025-43967 also addresses CVE-2025-29482 and CVE-2025-43966.

Oracle Retail Applications Risk Matrix

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

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2025-7962	Oracle Retail Xstore Point of Service	Point of Sale (Jakarta Mail)	SMTP	Yes	7.5	Network	Low	N
CVE-2025-48924	Oracle Retail Assortment Planning	Application Core (Apache Commons Lang)	TCP	Yes	5.3	Network	Low	N

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2025-48924	Oracle Retail Warehouse Management System	Security (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	N
CVE-2025-68161	Oracle Retail Assortment Planning	Application Core (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Bulk Data Integration	BDI Job Scheduler (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail EFTLink	Core/Plugin (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Extract Tranform and Load	Mathematical Operators (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Financial Integration	PeopleSoft Integration (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Fiscal Management	NF Issuing (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Integration Bus	RIB Kernal (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Merchandise Financial Planning	Application Core (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Merchandising System	Security (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Predictive Application Server	RPAS Fusion Client (Apache Log4j)	TLS	Yes	4.8	Network	High	N

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2025-68161	Oracle Retail Price Management	Security (Apache Log4j)	TLS	Yes	4.8	Network	High	N
CVE-2025-68161	Oracle Retail Service Backbone	RSB Installation (Apache Log4j)	TLS	Yes	4.8	Network	High	N

Oracle Siebel CRM Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2025-13601	Siebel CRM Cloud Applications	Siebel Cloud Manager (glib)	None	No	7.7	Local	Low
CVE-2022-45688	Siebel CRM Administration	Data Archival (Quartz)	HTTP	Yes	7.5	Network	Low
CVE-2025-69223	Siebel CRM Cloud Applications	Siebel Cloud Manager (AIOHTTP)	HTTP	Yes	7.5	Network	Low
CVE-2025-8869	Siebel CRM Cloud Applications	Siebel Cloud Manager (pip)	HTTP	Yes	7.5	Network	Low
CVE-2025-58057	Siebel CRM Deployment	Keyword Automation (Netty)	HTTP	Yes	7.5	Network	Low
CVE-2023-26464	Siebel CRM Deployment	Server Infrastructure (Apache Log4j)	TLS	Yes	7.5	Network	Low

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSIC		
					Base Score	Attack Vector	Attack Complex
CVE-2025-7962	Siebel CRM End User	Communications Panel/Dashboard (Jakarta Mail)	SMTP	Yes	7.5	Network	Low
CVE-2024-29371	Siebel CRM Integration	Event Publish and Subscribe (jose4j)	HTTP	Yes	7.5	Network	Low
CVE-2023-1436	Siebel CRM Integration	REST (Jettison)	HTTP	Yes	7.5	Network	Low
CVE-2025-27817	Siebel CRM Integration	Event Publish and Subscribe (Apache Kafka)	TCP	Yes	7.5	Network	Low
CVE-2025-48924	Siebel CRM Deployment	Keyword Automation (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low
CVE-2024-36124	Siebel CRM Integration	Open Integration (Snappy)	HTTP	Yes	5.3	Network	Low
CVE-2025-68161	Siebel CRM Development	Siebel Approval Manager (Apache Log4j)	TLS	Yes	4.8	Network	High
CVE-2025-68161	Siebel CRM Integration	EAI (Apache Log4j)	TLS	Yes	4.8	Network	High

Additional CVEs addressed are:

- The patch for CVE-2023-26464 also addresses CVE-2022-23302, CVE-2022-23305, and CVE-2022-23307.
- The patch for CVE-2025-58057 also addresses CVE-2025-55163 and CVE-2025-58056.
- The patch for CVE-2025-69223 also addresses CVE-2025-69224, CVE-2025-69225, CVE-2025-69226, CVE-2025-69227, CVE-2025-69228, CVE-2025-69229, and CVE-2025-69230.
- The patch for CVE-2024-29371 also addresses CVE-2023-51775.
- The patch for CVE-2023-1436 also addresses CVE-2022-40149, CVE-2022-40150, CVE-2022-45685, CVE-2022-45693, CVE-2026-28493, CVE-2026-28494, CVE-2026-28686, CVE-2026-28687, CVE-2026-28688, CVE-2026-28689, CVE-2026-28690, CVE-2026-28691, CVE-2026-28692, CVE-2026-28693, CVE-2026-30883, CVE-2026-30929, CVE-2026-30931, CVE-2026-30935, and CVE-2026-30936.
- The patch for CVE-2025-27817 also addresses CVE-2025-27818.

Oracle Supply Chain Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1			
					Base Score	Attack Vector	Attack Complex	Pri Req
CVE-2025-9900	Oracle AutoVue	Security (LibTIFF)	HTTP	Yes	8.8	Network	Low	Non
CVE-2026-22801	Oracle AutoVue	Security (libpng)	None	No	7.8	Local	Low	Lo
CVE-2025-68161	Oracle Product Lifecycle Analytics	Installation Issues (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2026-34296	Oracle Agile Product Lifecycle Management for Process	Product Quality Management	HTTP	No	4.3	Network	Low	Lo

Notes:

1. This vulnerability applies to Oracle AutoVue Office, Oracle AutoVue 2D Professional, Oracle AutoVue 3D Professional Advanced, Oracle AutoVue EDA Professional and Oracle AutoVue Electro-Mechanical Professional. Please refer to Patch Availability Document for more details.

Additional CVEs addressed are:

- The patch for CVE-2025-9900 also addresses CVE-2025-8176, CVE-2025-8177, and CVE-2025-8961.
- The patch for CVE-2026-22801 also addresses CVE-2026-22695.
- The patch for CVE-2026-34296 also addresses CVE-2026-21969.

Oracle Systems Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2024-6387	Sun ZFS Storage Appliance Kit	Firmware subsystem (OpenSSH)	HTTPS	Yes	9.0	Network	High	None	
CVE-2026-34281	Oracle Solaris	Kernel	None	No	6.5	Local	Low	Low	

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 7 new security patches, plus additional third party patches noted below, 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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 F			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2025-53643	Oracle Utilities Live Energy Connect	Python Scripting (AIOHTTP)	HTTP	Yes	7.5	Network	Low	Non
CVE-2025-66418	Oracle Utilities Network Management System	System Wide (urllib3)	HTTP	Yes	7.5	Network	Low	Non
CVE-2026-24734	Oracle Utilities Testing Accelerator	Tools (Apache Tomcat)	HTTP	Yes	7.5	Network	Low	Non
CVE-2020-17521	Oracle Utilities	Security (Apache	None	No	5.5	Local	Low	Lov

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 R			
					Base Score	Attack Vector	Attack Complex	Priv Req
	Application Framework	Groovy)						
CVE-2025-48924	Oracle Utilities Testing Accelerator	Tools (Apache Commons Lang)	HTTP	Yes	5.3	Network	Low	Non
CVE-2025-68161	Oracle Utilities Application Framework	Security (Apache Log4j)	TLS	Yes	4.8	Network	High	Non
CVE-2025-68161	Oracle Utilities Testing Accelerator	Tools (Apache Log4j)	TLS	Yes	4.8	Network	High	Non

Additional CVEs addressed are:

- The patch for CVE-2025-66418 also addresses CVE-2025-66471.
- The patch for CVE-2026-24734 also addresses CVE-2025-61795.

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

- Oracle Utilities Network Management System
  - SW- System Wide (Apache Commons Lang): CVE-2025-48924 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Virtualization Risk Matrix

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 English text form of this Risk Matrix can be found here.

CVE ID	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2026-35242	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High
CVE-2026-35246	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High
CVE-2026-35251	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High
CVE-2026-35230	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High
CVE-2026-35245	Oracle VM VirtualBox	Core	RDP	Yes	7.5	Network	Low	None
CVE-2026-35247	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High
CVE-2026-35248	Oracle VM VirtualBox	Core	None	No	5.0	Local	High	High
CVE-2026-35249	Oracle VM VirtualBox	Core	None	No	3.2	Local	Low	High
CVE-2026-35250	Oracle VM VirtualBox	Core	None	No	2.3	Local	Low	High

© 2026 Oracle | Privacy / Do Not Sell My Info Cookie Preferences Ad Choices Careers
Subscribe to emails Integrity Helpline Contact Us