Smarttech
YOUR 24/7 SECURITY PARTNER

Oracle Critical Security Patches Issued - October 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	179
Authors	Carp Daniel-Cristian < daniel.carp@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-21
Issue Date	2026-10-21

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple vulnerabilities have been identified in Oracle products. Successful exploitation of the most severe vulnerabilities could result in remote code execution.

RISK

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Home Users: Low

Affected Products and Patch Information

This Critical Patch Update contains 1295 new security patches across the listed product families, including 112 critical-severity and 475 high-severity patches. Oracle has again reported successful exploitation of vulnerabilities by attackers targeting customers who have failed to apply available patches. Oracle strongly recommends that customers use actively supported product versions and apply security patches without delay.

Affected Products and Versions
Helidon, versions 3.0.0-3.2.21, 4.0.0-4.5.5, 27.0.0
JD Edwards EnterpriseOne Configurator, version 9.2
JD Edwards EnterpriseOne General Ledger, version 9.2
JD Edwards EnterpriseOne Homebuilder, version 9.2
JD Edwards EnterpriseOne Human Resources Management, version 9.2
JD Edwards EnterpriseOne Localizations, version 9.2
JD Edwards EnterpriseOne Operational Sourcing, version 9.2
JD Edwards EnterpriseOne Orchestrator, versions 9.2.0.0-9.2.26.5
JD Edwards EnterpriseOne Sales Order Entry, version 9.2
JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.26.5
MySQL Cluster, versions 8.0.0-8.0.37, 9.7.3, 26.7.0-26.7.1, 8.0.0-8.0.49, 8.4.0-8.4.12, 9.7.0-9.7.3, 26.7.0-26.7.1
MySQL Connectors, versions 26.7.0, 26.7.1

MySQL Enterprise Backup, versions 8.0.0-8.0.49, 8.4.0-8.4.12, 9.7.0-9.7.3, 26.7.0
MySQL Router, version 26.7.0
MySQL Server, versions 8.4.0-8.4.12, 9.7.0-9.7.3, 26.7.0-26.7.1
Oracle Access Manager, versions 12.2.1.4.0, 14.1.2.0.0, 14.1.2.1.0
Oracle Agile Engineering Data Management, version 6.2.1
Oracle Agile PLM, versions 2.6, 9.3.6
Oracle Agile PLM MCAD Connector, version 3.6
Oracle Agile Product Lifecycle Management for Process, version 6.2.4
Oracle APEX, versions 24.1.0-24.1.21, 24.2.0-24.2.20, 26.1.0-26.1.4
Oracle Application Testing Suite, version 13.3.0.1
Oracle Autonomous Health Framework, versions 26.3-26.8
Oracle BI Publisher, versions 8.2.0.0.0, 12.2.1.4.0, 26.1.0.0.0
Oracle Business Intelligence Enterprise Edition, versions 8.2.0.0.0, 12.2.1.4.0, 26.1.0.0.0
Oracle Business Process Management Suite, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0
Oracle Commerce Platform, version 11.4.0
Oracle Communications Billing and Revenue Management, versions 15.0.0.0.0, 15.0.1.0.0, 15.1.0.0.0, 15.2.0.0.0
Oracle Communications BRM - Elastic Charging Engine, versions 15.0.0.0.0, 15.0.1.0.0, 15.1.0.0.0, 15.2.0.0.0
Oracle Communications Cloud Native Core Binding Support Function, versions 25.2.200, 25.2.201
Oracle Communications Cloud Native Core Certificate Management, versions 25.2.201, 26.1.200
Oracle Communications Cloud Native Core Console, versions 25.2.202, 26.1.200
Oracle Communications Cloud Native Core Network Repository Function, versions 25.2.202, 26.1.202
Oracle Communications Cloud Native Core Network Slice Selection Function, version 25.2.200
Oracle Communications Cloud Native Core Policy, versions 24.2.4-25.2.0, 25.2.200
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 25.2.200, 25.2.201, 26.1.200
Oracle Communications Cloud Native Core Service Communication Proxy, versions 25.1.100, 25.1.200, 25.2.100, 25.2.200, 26.1.200
Oracle Communications Cloud Native Core Unified Data Repository, versions 25.1.200, 25.2.200, 26.1.200
Oracle Communications EAGLE Element Management System, version 47.0.0.2.0
Oracle Communications EAGLE LNP Application Processor, version 11.0
Oracle Communications LSMS, version 14.0
Oracle Communications Network Analytics Data Director, versions 25.1.200, 25.2.100, 25.2.200
Oracle Communications Operations Monitor, versions 6.0, 6.1
Oracle Communications Policy Management, versions 15.0.0.0.0, 15.1.0.0.0
Oracle Communications Service Catalog and Design, versions 8.0-8.3
Oracle Communications Unified Assurance, versions 6.1.1-7.0.0
Oracle Communications Unified Inventory Management, versions 7.5.0, 7.5.1, 7.6.0, 7.7.0, 7.8.0, 8.0.1
Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Database Server, versions 19.3-19.32, 21.3-21.23, 23.4.0-23.26.3
Oracle Demand Planning, versions 12.1, 12.2
Oracle E-Business Suite, versions 12.2.3-12.2.15

Oracle Enterprise Manager Base Platform, versions 13.5, 24.1
Oracle Enterprise Manager for Oracle Database, versions 13.5, 24.1
Oracle Enterprise Manager for Siebel, versions 13.5, 24.1
Oracle Enterprise Manager for Virtualization, version 13.5
Oracle Essbase, version 21.8.3.0.0
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.9, 8.0.8.7, 8.1.2.5, 8.1.2.6
Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.11, 8.1.2.12
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8.0
Oracle Fusion Middleware, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Fusion Middleware Control, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Global Lifecycle Management NextGen OUI Framework, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 14.1.2.1.0, 15.1.1.0.0
Oracle Global Lifecycle Management OPatch, versions 12.2.0.1.16-12.2.0.1.52
Oracle Global Lifecycle Management OPatchAuto, versions 12.2.0.1.16-12.2.0.1.52
Oracle GoldenGate, versions 19.1.0.0.0-19.32.0.0, 21.3-21.23, 23.4-23.26.3.0.0
Oracle GoldenGate Big Data and Application Adapters, versions 21.3-21.20, 23.4-23.26.1
Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.16, 26.1.0.0.0-26.2.0.0.1
Oracle GraalVM Enterprise Edition, version 21.3.19.1.1
Oracle GraalVM for JDK, versions 17.0.20.1, 21.0.12.1
Oracle Graph Server and Client, versions 25.4.3, 26.2.2
Oracle Health Sciences Information Manager, versions 4.0.0-4.0.3
Oracle Healthcare Data Repository, versions 8.2.0.0-8.2.0.8
Oracle Healthcare Master Person Index, versions 5.0.0.0-5.0.9.7
Oracle Hospitality Cruise Shipboard Property Management (SPMS), versions 23.1, 23.2, 23.3
Oracle Hospitality OPERA 5 Property Services, versions 5.6.28.0, 5.6.28.2
Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Identity Manager, versions 12.2.1.4.0, 14.1.2.1.0
Oracle Identity Manager Connector, versions 12.2.1.4.0, 14.1.2.1.0
Oracle Java SE, versions 8u503, 8u503-perf, 11.0.32.1, 17.0.20.1, 21.0.12.1, 25.0.4.1, 26.0.2, 27
Oracle JavaFX, versions 21.0.12, 25.0.4, 27
Oracle JDeveloper, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Management Pack for Oracle GoldenGate, versions 13.4.1.0.1-13.5.2.0.6
Oracle Middleware Common Libraries and Tools, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0
Oracle NoSQL Database, versions 1.8.0, 23.3.41, 24.4.14, 25.3.24
Oracle Outside In Technology, version 8.5.8
Oracle Product Lifecycle Analytics, version 3.6.1
Oracle REST Data Services, versions 24.2.0-26.2.2
Oracle Retail Merchandise Financial Planning, versions 15.0, 16.0
Oracle Retail Merchandising System, version 19.0.1.44
Oracle Retail Predictive Application Server, versions 15.0.3.190, 16.0.3.350
Oracle Retail Xstore Point of Service, versions 21.0.5, 22.0.3, 23.0.3, 24.0.2, 25.0.1, 26.0.0
Oracle Secure Backup, versions 19.1.0.0.0, 19.1.0.1.0

Oracle Service Bus, versions 12.2.1.4.0, 14.1.2.0.0
Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0
Oracle Solaris, versions 11.3, 11.4
Oracle SQL Developer, versions 23.1.1-26.1.0
Oracle TimesTen In-Memory Database, versions 22.1-22.1.40.0, 26.1-26.1.1.3.0
Oracle Trusted Answer Search, version 26.1
Oracle Utilities Application Framework, versions 4.4.0.2.0, 4.4.0.3.0, 4.4.0.4.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4, 25.10, 26.4, 26.10
Oracle Utilities Network Management System, versions 2.4.0.1.0-2.4.0.1.33, 2.5.0.1.0-2.5.0.1.18, 2.5.0.2.0-2.5.0.2.11, 2.6.0.1.0-2.6.0.1.12, 2.6.0.2.0-2.6.0.2.10, 25.12.0.0.0-25.12.0.0.2
Oracle VM VirtualBox, versions 7.2.16, 7.2.20
Oracle Web Services Manager, version 14.1.2.0.0
Oracle WebCenter Content, versions 12.2.1.4.0, 14.1.2.0.0
Oracle WebCenter Portal, versions 12.2.1.4.0, 14.1.2.0.0
Oracle WebCenter Sites, versions 12.2.1.4.0, 14.1.2.0.0
Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0
Oracle Weblogic Server Proxy Plug-in, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
Oracle ZFS Storage Appliance Kit, version 8.8
PeopleSoft Enterprise CC Common Application Objects, version 9.2
PeopleSoft Enterprise FIN Cash Management, version 9.2
PeopleSoft Enterprise FIN Common Objects Argentina, version 9.1
PeopleSoft Enterprise FIN Common Objects Brazil, version 9.1
PeopleSoft Enterprise FIN General Ledger Brazil, version 9.1
PeopleSoft Enterprise FIN Inventory Brazil, version 9.1
PeopleSoft Enterprise FIN Manufacturing Brazil, version 9.1
PeopleSoft Enterprise FIN Product Configurator Brazil, version 9.1
PeopleSoft Enterprise HCM Global Payroll Switzerland, version 9.2
PeopleSoft Enterprise HCM Human Resources, version 9.2
PeopleSoft Enterprise PeopleTools, versions 8.61-8.63
PeopleSoft Enterprise SCM Manufacturing, version 9.2
PeopleSoft Enterprise SCM Purchasing, version 9.2
PeopleSoft Enterprise SCM Strategic Sourcing, version 9.2
Primavera Gateway, versions 21.12.0-21.12.18
Primavera P6 Enterprise Project Portfolio Management, versions 21.12.0.0-21.12.21.9, 22.12.0.0-22.12.21.4, 23.12.0-23.12.20, 24.12.0-24.12.16, 25.12.0-25.12.8
Primavera Unifier, versions 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.16, 24.12.0-24.12.16, 25.12.0-25.12.9
Siebel Applications, versions 17.0-26.9
WebCenter Content: Imaging, versions 12.2.1.4.0, 14.1.2.0.0

Recommendations

Smarttech247 team recommendations:

- Apply appropriate patches or appropriate mitigations provided by Oracle to vulnerable systems immediately after appropriate testing. (M1051: Update Software)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Proce**ss: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management**: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets**: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities**: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date**: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program**: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests**: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings**: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (M1026: Privileged Account Management):
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software**: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

  - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts**: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
  - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts**: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (M1050: Exploit Protection):
  - **Safeguard 10.5: Enable Anti-Exploitation Features**: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- Block execution of code on a system through application control, and/or script blocking. (M1038: Execution Prevention)
  - **Safeguard 2.5: Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
  - **Safeguard 2.6: Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
  - **Safeguard 2.7: Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (M1040: Behavior Prevention on Endpoint)
  - **Safeguard 13.2: Deploy a Host-Based Intrusion Detection Solution:** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
  - **Safeguard 13.7: Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. (M1017: User Training)
  - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and,

at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

- **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

References

https://www.oracle.com/security-alerts/cpuoct2026.html

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com