Smarttech
YOUR 24/7 SECURITY PARTNER

# Oracle Critical Security Patches Issued - August 2026

| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 139 |
| **Authors** | Dorin Constantin Banu < constantin.banu@smarttech247.com > |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 2026-08-19 |
| **Issue Date** | 2026-08-19 |

**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 discovered in Oracle products. Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

## RISK

**Government:**

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

**Businesses:**

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

**Home Users: Low**

## Affected Products and Patch Information

This Critical Patch Update contains new security patches across the product families listed below.
It has been reported again 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 security patches without delay.

| Affected Products and Versions |
|---|
| Enterprise Manager for MySQL Database, versions 13.5.1.0.0-13.5.6.0.0 |
| Helidon, versions 1.4.19, 1.4.20, 3.2.18, 3.2.19, 3.2.20, 4.5.0, 4.5.1, 4.5.3 |
| JD Edwards EnterpriseOne Orchestrator, versions 9.2.0.0-9.2.26.4 |
| JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.26.4 |
| JD Edwards EnterpriseOne US Payroll, version 9.2 |
| Management Cloud Engine, version 25.2.0.0.10 |
| MySQL AI, versions 9.4.0-9.7.2, 26.7.0 |
| MySQL Cluster, versions 8.0.0-8.0.48, 8.4.0-8.4.11, 9.7.0-9.7.2 |
| MySQL Connectors, version 26.7.0 |
| MySQL Shell, version 26.7.0 |
| Oracle Access Manager, versions 12.2.1.4.0, 14.1.2.1.0 |
| Oracle Agile Engineering Data Management, version 6.2.1 |
| Oracle Agile PLM, version 9.3.6 |
| Oracle Agile PLM MCAD Connector, version 3.6 |

| |
|---|
| Oracle Application Testing Suite, version 13.3.0.1 |
| Oracle Autonomous Health Framework, versions 26-26.1.0, 26.2.0, 26.3.1, 26.5.0, 26.5.2 |
| 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 Commerce Guided Search / Oracle Commerce Experience Manager, version 11.4.0 |
| Oracle Commerce Platform, version 11.4.0 |
| Oracle Communications ASAP, versions 7.4.1, 8.0.0 |
| Oracle Communications Network Analytics Data Director, versions 24.2.0, 24.3.4, 25.1.200 |
| Oracle Communications Unified Assurance, versions 6.1.1-7.0.0 |
| Oracle Communications Unified Inventory Management, versions 7.5.0-7.5.1, 7.6.0-7.8.0, 8.0.1 |
| 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 Systems Infrastructure, versions 13.5, 24.1 |
| Oracle Essbase, version 21.8.1.0.0 |
| Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.11 |
| Oracle Financial Services Compliance Studio, version 8.1.3.1 |
| Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.2.11 |
| Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8.0 |
| Oracle GraalVM Enterprise Edition, version 21.3.19 |
| Oracle GraalVM for JDK, versions 17.0.20, 21.0.12 |
| Oracle Hospitality OPERA 5 Property Services, versions 5.6.28.0-5.6.28.1 |
| Oracle Hospitality Simphony, versions 19.8-19.8.5, 19.9-19.9.3, 19.10-19.10.1 |
| Oracle Hyperion Calculation Manager, version 11.2.25.0.0 |
| Oracle Hyperion Data Relationship Management, versions 11.2.23.0.0, 11.2.25.0.0 |
| Oracle Hyperion Financial Management, version 11.2.25.0.0 |
| Oracle Hyperion Financial Reporting, version 11.2.25.0.0 |
| Oracle Hyperion Infrastructure Technology, version 11.2.25.0.0 |
| Oracle Hyperion Profitability and Cost Management, version 11.2.25.0.0 |
| 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 Internet Directory, versions 12.2.1.4.0, 14.1.2.1.0 |
| Oracle Java SE, versions 8u501, 11.0.32, 17.0.20, 21.0.12, 25.0.4, 26.0.2 |
| Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0 |
| Oracle Outside In Technology, version 8.5.8 |
| Oracle Product Lifecycle Analytics, version 3.6.1 |
| Oracle Reports Developer, versions 12.2.1.19.0, 14.1.2.0.0 |
| Oracle Retail Advanced Inventory Planning, versions 15.0, 16.0 |
| Oracle Retail Assortment Planning, versions 15.0, 16.0 |
| Oracle Retail Fiscal Management, version 14.2 |
| Oracle Retail Item Planning, versions 15.0, 16.0 |
| Oracle Retail Regular Price Optimization, versions 15.0, 16.0 |
| Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0 |
| Oracle Unified Directory, versions 12.2.1.4.0, 14.1.2.1.0 |
| Oracle Virtual Directory, versions 12.2.1.4.0, 14.1.2.0.0 |
| Oracle VM VirtualBox, version 7.2.14 |
| Oracle Web Services Manager, versions 12.2.1.4.0, 14.1.2.0.0 |
| Oracle WebCenter Content, versions 12.2.1.4.0, 14.1.2.0.0 |
| Oracle WebCenter Enterprise Capture, 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 |
| PeopleSoft Enterprise CC Common Application Objects, version 9.2 |
| PeopleSoft Enterprise FIN Common Objects, version 9.2 |

| |
|---|
| PeopleSoft Enterprise FIN Common Objects Brazil, version 9.1 |
| PeopleSoft Enterprise FIN Lease Administration, version 9.2 |
| PeopleSoft Enterprise PeopleTools, versions 8.61-8.63 |
| Primavera P6 Enterprise Project Portfolio Management, versions 21.12.0.0-21.12.21.8, 22.12.0.0-22.12.21.3, 23.12.0.0-23.12.19.0, 24.12.0.0-24.12.15.0, 25.12.0.0-25.12.6.0 |
| Service Delivery Platform, versions 12.2.1.4.0, 14.1.2.0.0 |
| Siebel Applications, versions 17.0-26.6 |

## 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 Proces**s: 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/cspuaug2026.html

-


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com