

# **Oracle Critical Security Patches Issued - September 2026**



|                        |                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Document ID</b>     | SMA-Threat Report                                                                                                |
| <b>Document status</b> | ISSUED                                                                                                           |
| <b>Issue Number</b>    | 164                                                                                                              |
| <b>Authors</b>         | Dorin Constantin Banu < <a href="mailto:constantin.banu@smarttech247.com">constantin.banu@smarttech247.com</a> > |
| <b>Verified by</b>     | Alin Curcan < <a href="mailto:alin.curcan@smarttech247.com">alin.curcan@smarttech247.com</a> >                   |
| <b>Last modified</b>   | 2026-09-16                                                                                                       |
| <b>Issue Date</b>      | 2026-09-16                                                                                                       |

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 discovered in Oracle products. Successful exploitation of the most severe of these vulnerabilities could allow 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 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                                                              |
|---------------------------------------------------------------------------------------------|
| Helidon, versions 3.0.0-3.2.20, 4.0.0-4.5.4                                                 |
| 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, 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 26.2, 26.3.1, 26.5.3, 26.8                     |
| Oracle Banking Branch, versions 14.5.0.0.0-14.9.0.0.0                                       |
| Oracle Banking Corporate Lending, versions 14.5.0.0.0-14.9.0.0.0                            |
| Oracle Banking Corporate Lending Process Management, versions 14.5.0.0.0-14.9.0.0.0         |
| Oracle Banking Origination, versions 14.5.0.0.0-14.9.0.0.0                                  |
| Oracle Banking Treasury Management, versions 14.5.0.0.0-14.9.0.0.0                          |
| 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 Coherence, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0                   |
| Oracle Commerce Guided Search / Oracle Commerce Experience Manager, version 11.4.0          |
| Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 25.2.201,  |

|                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26.1.200                                                                                                                                                             |
| Oracle Communications MetaSolv Solution Module - ASR, version 70.0.0                                                                                                 |
| Oracle Communications Operations Monitor, version 6.1                                                                                                                |
| Oracle Communications Service Catalog and Design, versions 8.0-8.3                                                                                                   |
| Oracle Communications Unified Assurance, versions 6.1.1-7.0.0                                                                                                        |
| 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 E-Business Suite, versions 12.2.3-12.2.15, V16                                                                                                                |
| Oracle Enterprise Manager Base Platform, versions 13.5, 24.1                                                                                                         |
| Oracle Enterprise Manager for Fusion Middleware, versions 13.5, 24.1                                                                                                 |
| Oracle Enterprise Manager for Oracle Database, version 24.1                                                                                                          |
| Oracle Forms, versions 12.2.1.19.0, 14.1.2.0.0                                                                                                                       |
| Oracle Fusion Middleware Control, versions 12.2.1.4.0, 14.1.2.0.0                                                                                                    |
| Oracle GraalVM Enterprise Edition, version 21.3.19.1                                                                                                                 |
| Oracle GraalVM for JDK 17, version 23.0.13.1                                                                                                                         |
| Oracle GraalVM for JDK 21, version 23.1.12.1                                                                                                                         |
| Oracle Hyperion Data Relationship Management, version 11.2.26.0.0                                                                                                    |
| Oracle Hyperion Financial Management, version 11.2.26.0.0                                                                                                            |
| 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 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 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 Platform Security for Java, versions 12.2.1.4.0, 14.1.2.0.0                                                                                                   |
| Oracle Product Lifecycle Analytics, version 3.6.1                                                                                                                    |
| Oracle Utilities Network Management System, versions 2.4.0.1.0-2.4.0.1.33, 2.5.0.1.0-2.5.0.1.19, 2.5.0.2.0-2.5.0.2.13, 2.6.0.1.0-2.6.0.1.2B, 25.12.0.0.0-25.12.0.0.3 |
| Oracle VM VirtualBox, version 7.2.16                                                                                                                                 |
| 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 Engineering Brazil, version 9.1                                                                                                            |
| PeopleSoft Enterprise FIN Inventory Brazil, version 9.1                                                                                                              |
| PeopleSoft Enterprise PeopleTools, versions 8.61-8.63                                                                                                                |
| PeopleSoft Enterprise PRTL Interaction Hub, version 9.1                                                                                                              |
| Service Delivery Platform, versions 12.2.1.4.0, 14.1.2.0.0                                                                                                           |
| Siebel Applications, versions 17.0-26.7                                                                                                                              |

## 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 Process:** 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/cspusep2026.html>

-

