CYBER ADVISORY

TLP:CLEAR

23 January 2025

Oracle Releases Critical Patch Update Advisory

Agile PLM | Oracle | 318 New Patches | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of Oracle's January 2025 Critical Patch Update release.[1] The update introduces 318 new security patches, addressing vulnerabilities across major products.[2] These patches target issues in both Oracle's code and third party components.

The most significant vulnerabilities, CVE-2025-21556 (CVSS 3.1 score of 9.9), affects Oracle Agile Product Lifecycle Management (PLM) Framework version 9.3.6.[3] The exploitation of this vulnerability enables a low-privilege user with network access to compromise Oracle Agile PLM Framework. Successful exploitation could allow the low-privilege user to take control of vulnerable instances. While there have been no reports of widespread exploitation of CVE-2025-21556, researchers cautioned that the vulnerability is highly exploitable, with proofs of concept likely to surface soon. Oracle Agile PLM instances exposed to the internet face a significant risk of being targeted.

The Cal-CSIC recommends immediately applying the appropriate updates to the affected Oracle products.

For more information on applying the security updates please refer to the Oracle Critical Patch Update Advisory.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] Oracle; "Oracle Critical Patch Update Advisory - January 2025"; https://www.oracle.com/security-alerts/cpujan2025.html; accessed 22 January 2025.
[2] The Hacker News; "Oracle Releases January 2025 Patch to Address 318 Flaws Across Major Products"; https://thehackernews.com/2025/01/oracle-releases-january-2025-patch-to.html; accessed 22 January 2025.
[3] National Vulnerability Database; "CVE-2025-21556 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-21556; accessed 22 January 2025.