



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Monday, October 06, 2025

CAL-CSIC-202510-A-001

Oracle E-Business Suite Remote Code Execution Vulnerability

Oracle

Concurrent Processing

Unauthentication

Versions 12.2.3-13.2.14

SUMMARY: The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability (CVE-2025-61882) affecting Oracle Concurrent Processing, a core component of the Oracle E-Business Suite (versions 12.2.3-13.2.14).¹ Rated 9.8 (Critical) on the CVSS v3.1 scale, the vulnerability stems from an unauthenticated access flaw exploitable via the Hypertext Transfer Protocol (HTTP). This allows a remote attacker to achieve remote code execution (RCE) and gain full control of the vulnerable application.²

Affected Versions (CVE-2025-61882):

- Oracle E-Business Suite, versions 12.2.3-12.2.14

The Cal-CSIC recommends that organizations immediately apply the security patches released by Oracle to address CVE-2025-61882.

For further information to apply upgrades please refer to the [Oracle Security Alert Advisory - CVE-2025-61882](#)

References

¹ National Vulnerability Database; “CVE-2025-61882 Detail”; <https://nvd.nist.gov/vuln/detail/CVE-2025-61882>; accessed 06 October 2025

² Oracle; “Oracle Security Alert Advisory - CVE-2025-61882 Description”; <https://www.oracle.com/security-alerts/alert-cve-2025-61882.html#AppendixEBS>; accessed 06 October 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR