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