CYBER ADVISORY

Tuesday, November 25, 2025 **CAL-CSIC-202511-A-010**

Cyber Advisory Oracle Fusion Middleware Vulnerability

Multiple Sectors impacted	Oracle Identity Manager	RCE	Exploited in the Wild

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability affecting Oracle Identity Manager, part of the Oracle Fusion Middleware suite. CVE-2025-61757, which carries a CVSS 3.1 score of 9.8, stems from a missing authentication check within the product's Representational State Transfer(REST) WebServices component. This flaw allows an unauthenticated attacker with network access over HTTP to fully compromise an Identity Manager instance, resulting in remote code execution (RCE).

Successful exploitation grants attackers the ability to pivot within an organization's environment, escalate privileges, and freely create or modify user accounts. Exploitation has been confirmed in the wild[1] and may have been as a zero-day.[2] A public Proof-of-Concept is available[3]. Oracle has released a patch as part of its October 2025 Critical Patch Update and organizations using affected versions should prioritize applying these updates immediately.

Product	Affected versions:
Oracle Identity Manager	12.2.1.4.0
	14.1.2.1.0

The Cal-CSIC recommends immediately applying the patches released by Oracle as part of their Oracle Critical Patch Update for the month of October 2025.

For further information on this vulnerability, please see the Oracle Critical Patch Update Advisory.

References

[1] CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2025-61757&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 24 November 2025

[2] SANS; "Oracle Identity Manager Exploit Observation from September (CVE-2025-61757)" https://isc.sans.edu/diary/Oracle+Identity+Manager+Exploit+Observation+from+September+CVE202561757/32506/; accessed 24 November 24, 2025

[3] Searchlight Cyber; "Breaking Oracle's Identity Manager: Pre-Auth RCE (CVE-2025-61757)"; https://slcyber.io/research-center/breaking-oracles-identity-manager-pre-auth-rce/; accessed 24 November 2025