CYBER ADVISORY

Thursday, May 07, 2026 **CSIC-ADVISORY-202605-A-003**

SQL Injection Vulnerability Impacting Oracle MCP Server Helper Tool

SQL Injection	Tool Compromise	Data Modification	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high- severity vulnerability that targets the Oracle Model Context Protocol (MCP) Server Helper Tool products of Oracle Open-Source Projects. CVE-2026-35228 carries a CVSS 3.1 score of 8.7.[1] The vulnerability allows unauthenticated attackers network access via HTTP to execute malicious SQL commands against the application. Successful exploitation would grant an unauthenticated attacker access to unauthorized data, data modification, and compromise of the Oracle MCP Server Helper Tool. Additionally, successful exploitation would impact the confidentiality and integrity across the target's interconnected systems.[2]

Oracle customers with a *valid support license* may use the link below for more technical vulnerability details and remediation instructions within Oracle's security alert document. If immediate patching is not feasible, restrict network access to the Oracle MCP Server Helper tool to only trusted networks and monitor logs for suspicious SQL command execution patterns and unusual database activity.

https://www.oracle.com/security-alerts/all-oracle-cves-outside-other-oracle-public-documents.html

Affected Product and Version:

Products	Version
Oracle MCP Server Helper Tool	***1.0.1*** to ***1.0.156***

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-3528"; https://nvd.nist.gov/vuln/detail/CVE-2026-35228; accessed 05 May 2026
[2] Feedly; "CVE-2026-35228"; https://feedly.com/cve/CVE-2026-35228; accessed 05 May 2026