



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



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

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

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

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