

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



SQL Injection Vulnerabilities in SuiteCRM

Tracking #:432317987

Date:11-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SuiteCRM maintainers released a security update to fix two authenticated SQL injection vulnerabilities in SuiteCRM instances.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2025-64492 — CVSS 8.8 (High)**: time-based, authenticated blind SQL injection that can be used to enumerate database schema and extract sensitive data by measuring response delays. Affects SuiteCRM versions $\leq 8.9.0$.
2. **CVE-2025-64493 — CVSS 6.5 (Medium)**: authenticated blind SQL injection in the GraphQL appMetadata operation. Observed in 8.6.0 – 8.8.0 and does not require administrative privileges (any logged-in user could exploit).

Affected software

- SuiteCRM: $\leq 8.9.0$ (CVE-2025-64492)
- SuiteCRM $\geq 8.6.0$, $\leq 8.9.0$ (CVE-2025-64493)
- Patched version: 8.9.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade all SuiteCRM instances to 8.9.1 as soon as feasible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://github.com/SuiteCRM/SuiteCRM-Core/security/advisories/GHSA-5gcj-mfqq-v8f7>
- <https://github.com/SuiteCRM/SuiteCRM-Core/security/advisories/GHSA-54m4-4p54-j8hp>