مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in MariaDB Server

Tracking #:432319182

Date:23-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in MariaDB that could allow attackers to execute arbitrary shell commands on affected database servers. Successful exploitation could lead to complete system compromise and unauthorized access to sensitive data stored within affected environments.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-49261**
  - **Severity:** Critical | **CVSS:** 10.0
  - Improper handling of the wsrep_notify_cmd parameter may allow command injection through a malicious joiner node name, resulting in arbitrary command execution on vulnerable servers.
- **CVE-2026-48163**
  - **Severity:** High | **CVSS:** 8.0
  - A command injection vulnerability in the SST rsync process allows a malicious joiner node to execute arbitrary shell commands on the donor node.
- **CVE-2026-48165**
  - **Severity:** High | **CVSS:** 8.0
  - A privileged user can manipulate specific global variables to execute arbitrary commands with the privileges of the MariaDB database process.

Affected Versions:

- MariaDB Server 10.6.1-10.6.26, 10.11.1-10.11.17, 11.4.1-11.4.11, 11.8.1-11.8.7, 12.3.1

Fixed Versions

- MariaDB Server 10.6.27, 10.11.18, 11.4.12, 11.8.8, 12.3.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by MariaDB.

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/MariaDB/server/security/advisories/GHSA-3p3m-4x7c-p4pw
- https://github.com/MariaDB/server/security/advisories/GHSA-rpgv-q6gv-684r
- https://github.com/MariaDB/server/security/advisories/GHSA-7v3p-h23x-8hwv