



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in MariaDB
Tracking #:432319086
Date:08-06-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple security vulnerabilities have been identified in the MariaDB Community Server, including a critical flaw.

TECHNICAL DETAILS:

Multiple security vulnerabilities have been identified in the MariaDB Community Server, including a critical flaw tracked as CVE-2026-49261 with a CVSS score of 10.0. The vulnerabilities impact several widely deployed MariaDB versions and could expose organizations to unauthorized access, compromise of sensitive data, and potential database server takeover.

Vulnerability Details:

1. CVE-2026-49261
 - Severity: **Critical**
 - CVSS Score: 10.0
2. CVE-2026-48165
 - Severity: High
 - CVSS Score: 8.0
3. CVE-2026-48163
 - Severity: High
 - CVSS Score: 8.0

Fixed Versions:

- MariaDB 11.8.8 or later
- MariaDB 11.4.12 or later
- MariaDB 10.11.18 or later
- MariaDB 10.6.27 or later

RECOMMENDATIONS:

Immediate Actions:

- Upgrade MariaDB Community Server to the latest patched release immediately.
- Identify all affected MariaDB instances across on-premises and cloud environments.
- Prioritize remediation of internet-facing database servers.

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://mariadb.com/docs/release-notes/community-server/11.8/11.8.8>
- <https://mariadb.com/docs/release-notes/community-server/11.4/11.4.12>
- <https://mariadb.com/docs/release-notes/community-server/10.11/10.11.18>
- <https://mariadb.com/docs/release-notes/community-server/10.6/10.6.27>