MariaDB Connector Vulnerability CVE-2020-13249

322 Manu Chacko July 24, 2024 General 3538

How to fix MariaDB Connector Vulnerability CVE-2020-13249?

Overview: This article provides information about a vulnerability identified in the MariaDB connector and the recommended mitigation actions. This vulnerability could potentially allow an unauthenticated remote attacker to execute arbitrary code on affected installations.

NOTE: This does not affect any of the ezeelogin installation as we don't use this connector in ezeelogin.

Recently a very critical vulnerability was identified in MariaDB Connector up to 3.1.7 (Database Software). It's vulnerable to a Remote Code Execution (RCE) tagged as ***CVE-2020-13249**.
This vulnerability potentially allows an unauthenticated remote attacker to execute arbitrary code on vulnerable installations. This vulnerability has been rated with a CVSS score of **9.8** (CRITICAL). This issue is reported to **not affect** any **MySQL** components supported by **Oracle**. The weakness was shared 05/20/2020. This vulnerability is handled as CVE-2020-13249 since 05/20/2020. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Technical details are known, but there is no available exploit.

Recommended Mitigation actions:

It is recommended to **update/patch** all installations of MariaDB Connector/C* to version **3.1.8** immediately since upgrading to version 3.1.8 eliminates this vulnerability.

References:

https://mariadb.com/kb/en/security