Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Fortinet FortiWeb Fabric Connector Flaw Enables Remote Code Execution

Vulnerability Note: VN-2025-10

Date of Issue: 14 July 2025

Severity Rating: High

Systems Affected:

- FortiWeb version 7.6.0 through 7.6.3
- FortiWeb version 7.4.0 through 7.4.7
- FortiWeb version 7.2.0 through 7.2.10
- FortiWeb version 7.0.0 through 7.0.10

Description

A severe pre-authentication SQL injection vulnerability has been identified in Fortinet's FortiWeb Fabric Connector and this vulnerability can allow unauthenticated attackers to execute unauthorized SQL commands and potentially achieve remote code execution. The vulnerability stems from improper input sanitization in the get_fabric_user_by_token function within FortiWeb's authentication mechanism.

CVE Information
CVE-2025-25257

Workaround
Fortinet has released updates to address this vulnerability.
More information is available on:
https://labs.watchtowr.com/pre-auth-sql-injection-to-rce-fortinet-fortiweb-fabric-connector-cve-2025-25257/

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,