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

CERT-MU Vulnerability Note

FortiWeb Authentication Bypass Vulnerability

Vulnerability Note: VN-2025-17

Date of Issue: 13 August 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 critical security vulnerability has been identified in Fortinet's FortiWeb web application firewall, and this could allow unauthenticated attackers to bypass authentication and impersonate any existing user on affected devices. The vulnerability exploits an out-of-bounds read access issue in FortiWeb's cookie handling code, enabling attackers to force the server to use a predictable, all-zero secret key for session encryption and signing.

CVE Information
CVE-2025-52970

Workaround
Fortinet published the security advisory on August 12, 2025, and has released patches for all affected versions. Organizations running vulnerable FortiWeb installations should prioritize immediate updates to the latest available versions.

More information is available on:
https://www.fortiguard.com/psirt

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,