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

CERT-MU Vulnerability Note

Cisco Secure Firewall Management Center Software RADIUS Remote Code Execution Vulnerability

Vulnerability Note: VN-2025-18

Date of Issue: 15 August 2025

Severity Rating: High

Systems Affected:

- Cisco Secure FMC Software releases 7.0.7 and 7.7.0

Description

A vulnerability has been identified in the RADIUS subsystem implementation of Cisco Secure Firewall Management Center (FMC) Software and this could allow an unauthenticated, remote attacker to inject arbitrary shell commands that are executed by the device.

This vulnerability is caused due to a lack of proper handling of user input during the authentication phase. An attacker could exploit this vulnerability by sending crafted input when entering credentials that will be authenticated at the configured RADIUS server. A successful exploit could allow the attacker to execute commands at a high privilege level.

CVE Information
CVE-2025-20265

Workaround
Cisco has released free software updates that address the vulnerability described in this advisory. Users are recommended to apply the updates.
More information is available on:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79

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