

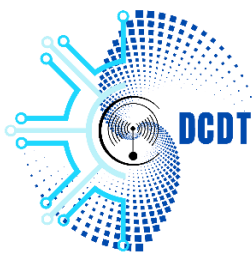
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

10 September 2026

**Advisory 287: Cisco Secure Firewall Management Center Authentication Bypass
Leading to Root Remote Code Execution (CVE-2026-20079).**

Release Date: 9th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate an on-premises Cisco Secure Firewall Management Center (FMC) appliance. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-20079 is a critical authentication bypass vulnerability in Cisco Secure Firewall Management Center (FMC), the centralized management platform used to configure, monitor, and administer Cisco Secure Firewall (Firepower) devices across an organization's network. Cisco is one of the world's most widely-deployed networking and security vendors, and FMC is a standard component of any Cisco Firepower-based firewall deployment. Cisco disclosed this vulnerability on 4 March 2026 via Cisco Security Advisory cisco-sa-onprem-fmc-authbypass-5JPp45V2. Cisco disclosed a second, technically distinct maximum-severity vulnerability in the same product on the same day, CVE-2026-20131 (insecure deserialization of a user-supplied Java byte stream, also enabling unauthenticated root remote code execution).

What are the systems affected?

The following version(s) are affected:

- All on-premises Cisco Secure Firewall Management Center (FMC) software releases - (Affected)

Cloud-Delivered FMC (cdFMC) is not affected. Cisco has not published a single unified “fixed version” number in third-party reporting - administrators should consult the fixed-release table in Cisco Security Advisory [cisco-sa-onprem-fmc-authbypass-5Jp45V2](#) directly, or use Cisco’s Software Checker tool, to determine the correct fixed release for the specific train their appliance is running.

What does this mean?

Typical attack flow:

1. **Reach the FMC web management interface**
 - An unauthenticated remote attacker sends specially crafted HTTP requests to a Cisco FMC appliance’s web management interface, targeting a flaw in a system process that was improperly created at boot time.
2. **Bypass authentication and execute commands as root**
 - The crafted requests exploit the improperly-created boot-time process to bypass authentication entirely, allowing the attacker to execute a variety of scripts and commands with root privileges on the underlying operating system - full administrative control of the management platform itself.

Attack vectors:

- A network-based, unauthenticated attack against any reachable Cisco FMC appliance’s web management interface, most critically if that interface is exposed to the internet or an untrusted network segment.
- No user interaction or privileges are required (CVSS AV:N/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Gain complete, unauthenticated root-level control of the Cisco FMC management appliance itself.
- Use root access to the management platform to view, alter, or disable the configuration of every Cisco Firepower firewall it manages - potentially disabling security policy across an organization’s entire firewall fleet, or using the platform as a pivot point into the wider network.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Identify the exact fixed release for your FMC software train using Cisco’s Software Checker tool or the fixed-release table in Cisco Security Advisory [cisco-sa-onprem-fmc-authbypass-5Jp45V2](#), and apply it. No workaround exists, so upgrading is the only remediation.

2. Restrict access to the FMC management interface
3. Do not expose FMC to the internet
4. Monitor for unauthorized configuration changes

Report any suspected compromise of a Cisco Secure Firewall Management Center appliance to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-20079>
2. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2>