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

3 August 2026

Advisory 176: Cisco Secure Firewall Management Center (FMC) Static Credential Vulnerability (CVE-2026-20316)

Release Date: 29th July 2026
Impact: HIGH
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 utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-20316 is a vulnerability in Cisco Secure Firewall Management Center (FMC) Software (CWE-259, Use of Hard-coded Password; CVSS v3.1 base score 5.3, Medium) caused by the presence of static user credentials for a low-privileged account in the FMC web-based management interface. Although the CVSS base score is Medium, Cisco has assigned this vulnerability a Security Impact Rating (SIR) of High, because the low-privileged access it grants can be combined with other Cisco Secure Firewall Management Center vulnerabilities to elevate privileges. Cisco has confirmed active exploitation of this vulnerability in the wild.

What are the systems affected?

The following on-premises product is affected:

- **Cisco Secure Firewall Management Center (FMC) Software**

Affected release branches (hot fixes released by Cisco):

- FMC Software 7.0 release branch
- FMC Software 7.2 release branch
- FMC Software 7.4 release branch
- FMC Software 7.6 release branch
- FMC Software 7.7 release branch
- FMC Software 10.0 release branch

Cloud-Delivered FMC, Firewall Device Manager (FDM), Secure Firewall ASA Software, Secure Firewall Threat Defense (FTD) Software, and Security Cloud Control are not affected by this vulnerability.

What does this mean?

Typical exploitation flow:

1. Remote unauthenticated login
    - An attacker uses the static, hard-coded low-privileged account credentials to log in remotely to the FMC web-based management interface without needing any valid credentials of their own.
2. Access to sensitive data
    - A successful login allows the attacker to access sensitive data accessible to that low-privileged account.
3. Potential privilege escalation
    - Cisco advises this access can be combined with other Cisco Secure FMC vulnerabilities, including CVE-2026-20079 (a separate critical authentication bypass updated in the same advisory cycle), to obtain greater control, potentially up to root access.
4. Reduced exposure for internal-only deployments
    - If the FMC management interface does not have public internet access, the attack surface associated with this vulnerability is reduced.

This vulnerability requires:

- No authentication
- No user interaction
- Low attack complexity

Mitigation process

CERTVU recommends the following:

1. **Apply Security Updates Immediately**
2. Install the Cisco-released hot fix appropriate to your FMC release branch (7.0, 7.2, 7.4, 7.6, 7.7, or 10.0) without delay.
3. **Restrict Network Exposure**
    - Restrict access to the FMC web-based management interface to trusted administrative networks only, as an interim defense-in-depth control pending patching.

4. **Review for Prior Compromise**
    - Review FMC logs for the /var/tmp/license.tmp indicator and any unexpected low-privilege logins, and treat any positive finding as a potential compromise requiring incident response.
5. **Monitor Related Advisories**
    - Track Cisco's updated advisory for CVE-2026-20079 given the overlapping forensic indicator and potential for chained exploitation.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-20316
2. https://www.cve.org/CVERecord?id=CVE-2026-20316
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh
4. https://cwe.mitre.org/data/definitions/259.html