Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-20316: Cisco Secure FMC Skeleton Key Exploited as a Zero-Day

Date of Publication	Admiralty Code	TA Number
July 31, 2026	A1	TA2026218

Summary

First Seen: July 2026
Affected Products: Cisco Secure Firewall Management Center (FMC) Software
Impact: Cisco has disclosed CVE-2026-20316, an actively exploited zero-day flaw in the web interface of Cisco Secure Firewall Management Center (FMC) Software. The root of the problem is a set of static, built-in credentials for a low-privilege account that ships with the software. Because those credentials are hard-coded, an unauthenticated, remote attacker can log in to an exposed device and read sensitive data as that low-privilege user, without needing to steal or guess anything. Cisco's PSIRT became aware of active exploitation in July 2026. Because the flaw is already being actively exploited, prompt patching is necessary.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20316	Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability	Cisco Secure Firewall Management Center (FMC) Software	✓	✓	✓

Vulnerability Details

#1

Cisco has addressed a vulnerability in its Cisco Secure Firewall Management Center (FMC) Software that is actively exploited. The weakness lives in the web interface of Cisco Secure Firewall Management Center Software, and it exists regardless of how the device is configured. The software ships with static user credentials tied to a low-privilege account, and because those credentials are fixed rather than unique per deployment, anyone who knows them can authenticate.

#2

The exploitation mechanism is straightforward, which is part of what makes it dangerous. An unauthenticated, remote attacker uses the built-in account to log in to the FMC web interface over the network. No prior access, phishing, or additional exploit is required for the initial login. Once authenticated, the attacker can access sensitive data within the affected system as the low-privileged user. Cisco has noted that the attack surface is meaningfully reduced when the FMC management interface is not reachable from the public internet, so internet-exposed management interfaces carry the highest risk.

#3

The affected scope spans multiple Cisco Secure FMC Software releases, including builds across the 7.0, 7.2, 7.3, 7.4, 7.6, 7.7, and 10.0 trains before the fixed hot-fix versions. Cisco has confirmed that Cloud-Delivered FMC (cdFMC), Firewall Device Manager (FDM), Secure Firewall ASA Software, Secure Firewall Threat Defense (FTD) Software, and Security Cloud Control (SCC) are not affected. Active exploitation is confirmed. Organizations running affected Cisco Secure FMC Software should upgrade to the latest fixed hot-fix releases without delay.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20316	Cisco Secure Firewall Management Center (FMC) Software (7.0.x through 7.7.x and 10.0.x releases prior to the fixed hot-fix builds)	cpe:2.3:a:cisco:secure_firewall_management_center:*:*:*:*:*:*:*:*	CWE-259

Recommendations

Apply the Cisco Hot Fix Immediately: Cisco has released hot fixes for every affected train, 7.0, 7.2, 7.4, 7.6, 7.7, and 10.0, available from the Software Center on Cisco.com. There are no workarounds, so upgrading to the fixed hot-fix build is the only real remediation. Given confirmed active exploitation and the federal August 1, 2026 deadline, treat patching as urgent.

Check for Signs of Exploitation: In expert mode, run `cat /var/log/messages | grep license` on the FMC device. If the output references `/var/tmp/license.tmp`, the vulnerability may have been exploited. If you see this indicator or otherwise suspect compromise, contact the Cisco Technical Assistance Center (TAC) for recovery guidance.

Rotate Credentials and Keys: Because exploitation has been ongoing, Cisco recommends rotating all user credentials, keys, and certificates on any affected Cisco Secure FMC device, even after patching, to ensure an attacker who already logged in cannot retain access.

Restrict Management Interface Exposure: Ensure the FMC management interface is not reachable from the public internet. Placing it behind a VPN or restricting it to a trusted management network sharply reduces the attack surface for this and similar flaws, and should be standard practice for security appliance consoles.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
Collection	T1005: Data from Local System	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 31, 2026 • 08:30 AM

More at www.hivepro.com