

CVE-2026-20316

Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability

CISA KEV since Jul 29, 2026

Actively exploited

Ransomware use known

A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to log in to an affected device using a low-privileged account to access sensitive data within the impacted systems. This vulnerability is due to the presence of static user credentials for a low-privileged account. An attacker could exploit this vulnerability by using the account to log in to an affected system.

EVRS 75/100 Urgent priority	CVSS V3.1 5.3 Medium · NVD	EPSS 0.351 98.4th percentile · FIRST	CISA DEADLINE Aug 1, 2026 CISA federal deadline · Overdue by 3 months
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.351 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

A successful exploit could allow the attacker to log in to the affected system and access sensitive data as the low-privileged user. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced. Cisco has assigned this security advisory a Security Impact Rating (SIR) of High rather than Medium as the score indicates. The reason is that this vulnerability can be used with other Cisco Secure FMC Software vulnerabilities to elevate privileges.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
secure firewall management center	$\geq 7.0.0 \leq 7.0.9$ $\geq 7.2.0 \leq 7.2.11$ $\geq 7.3.0 \leq 7.3.1.2$ $\geq 7.4.0 \leq 7.4.7$ $\geq 7.6.0 \leq 7.6.5$ $\geq 7.7.0 \leq 7.7.12$ $\geq 10.0.0 \leq 10.0.1$	no fixed version listed	NVD

Sources

Vendor guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-20316
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-50404
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-20316		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.