

CVE-2026-20079

Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability

CISA KEV since Sep 9, 2026

Actively exploited

Public exploit module (Metasploit)

A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass authentication and execute script files on an affected device to obtain root access to the underlying operating system. This vulnerability is due to an improper system process that is created at boot time. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device.

EVRS 89/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.885 99.77th percentile · FIRST	CISA DEADLINE Sep 12, 2026 CISA federal deadline · Overdue by 44 days
--	---	---	---

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	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.885 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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 execute a variety of scripts and commands that allow root access to the device.

Affected and fixed versions



secure firewall management	7.0.0	no fixed version listed	NVD
center	7.0.0.1		
	7.0.1		
	7.0.1.1		
	7.0.2		
	7.0.2.1		
	7.0.3		
	7.0.4		
	7.0.5		
	7.0.6		
	7.0.6.1		
	7.0.6.2		
	7.0.6.3		
	7.0.7		
	7.0.8		
	7.0.8.1		
	7.0.9		
	7.1.0		
	7.1.0.1		
	7.1.0.2		
	7.1.0.3		
	7.2.0		
	7.2.0.1		
	7.2.1		
	7.2.2		
	7.2.3		
	7.2.3.1		
	7.2.4		
	7.2.4.1		
	7.2.5		
	7.2.5.1		
	7.2.5.2		
	7.2.6		
	7.2.7		
	7.2.8		
	7.2.8.1		
	7.2.9		
	7.2.10		
	7.2.10.1		
	7.2.10.2		
	7.2.11		
	7.3.0		
	7.3.1		
	7.3.1.1		
	7.3.1.2		
	7.4.0		
	7.4.1		
	7.4.1.1		
	7.4.2		
	7.4.2.1		
	7.4.2.2		
	7.4.2.3		
	7.4.2.4		
	7.4.3		
	7.4.4		
	7.4.5		
	7.4.6		
	7.4.7		
	7.6.0		
	7.6.1		
	7.6.2		
	7.6.2.1		
	7.6.3		



PACKAGE	AFFECTED	FIXED IN	SOURCE
	7.6.4		
	7.6.5		
	7.7.0		
	7.7.10		
	7.7.10.1		
	7.7.11		
	7.7.12		
	10.0.0		
	10.0.1		

Sources

Vendor guidance	github.com/advisories/GHSA-mv8w-c2qv-cgrg	Additional guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5Jp45V2
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-2026-20079	CISA KEY	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-9438	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-20079

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