

CVE-2026-20131

Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability

Exigent

CISA KEV since Mar 19, 2026

Actively exploited

Ransomware use known

A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to execute arbitrary Java code as root on an affected device. This vulnerability is due to insecure deserialization of a user-supplied Java byte stream. An attacker could exploit this vulnerability by sending a crafted serialized Java object to the web-based management interface of an affected device.

EVRS 85/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.432 98.7th percentile · FIRST	CISA DEADLINE Mar 22, 2026 CISA federal deadline · Overdue by 7 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 year
☒ EPSS	0.432 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

A successful exploit could allow the attacker to execute arbitrary code on the device and elevate privileges to root. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced.

Affected and fixed versions



secure firewall management	6.4.0.13	no fixed version listed	NVD
center	6.4.0.14		
	6.4.0.15		
	6.4.0.16		
	6.4.0.17		
	6.4.0.18		
	7.0.0		
	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		
	7.1.0		
	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		
	7.3.0		
	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		
	7.6.0		
	7.6.1		
	7.6.2		



PACKAGE	AFFECTED	FIXED IN	SOURCE
	7.6.2.1		
	7.6.3		
	7.6.4		
	7.7.0		
	7.7.10		
	7.7.10.1		
	7.7.11		
	10.0.0		

Sources

Vendor guidance github.com/advisories/GHSA-r229-mj76-g2qx

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

NVD nvd.nist.gov/vuln/detail/CVE-2026-20131

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-9444

Current data evulnable.com/vulnerability-management/cve/CVE-2026-20131

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