Cisco Patches Two Critical Firewall Management Vulnerabilities Allowing Remote Root Access

TL;DR

Cisco patched two critical vulnerabilities in Cisco Secure Firewall Management Center (FMC) that could allow unauthenticated attackers to gain root-level access to firewall management systems.

The vulnerabilities include an authentication bypass vulnerability (CVE-2026-20079) and a remote code execution vulnerability (CVE-2026-20131). Both issues can be exploited remotely through the FMC web interface.

Cisco issued the patches as part of a broader firewall advisory bundle that also addresses multiple additional high-severity vulnerabilities across Secure FMC, Secure Firewall ASA, and Secure Firewall Threat Defense software.

Overview

There are two critical vulnerabilities (CVE-2026-20079 and CVE-2026-20131) affecting Cisco Secure Firewall Management Center (FMC), the centralized platform used to configure and manage Cisco firewall infrastructure.

Affected Products

- Cisco Secure Firewall Management Center (FMC) Software
- Cisco Security Cloud Control (SCC) Firewall Management (affected by CVE-2026-20131)

FMC allows administrators to control firewall policies, intrusion prevention settings, application filtering, and other security services across Cisco firewall deployments such as Secure Firewall Threat Defense devices. Because the platform acts as the central management layer for firewall operations, compromise of FMC can allow attackers to manipulate security policies or gain visibility into network security controls.

CVE-2026-20079 (CVSS 10)

- This is an authentication bypass vulnerability in the FMC web interface. The issue stems from an improper system process created during device boot. An attacker could exploit the vulnerability by sending crafted HTTP requests to the management interface. Successful exploitation would allow the attacker to bypass authentication and execute scripts on the device, resulting in root access to the underlying operating system.

CVE-2026-20131 (CVSS 10)

- This is a remote code execution vulnerability caused by insecure deserialization of a user-supplied Java object. An attacker could exploit it by sending a crafted

serialized Java object to the FMC web interface. If successful, the attacker could execute arbitrary Java code and escalate privileges to root on the affected system.

Both vulnerabilities can be exploited remotely by unauthenticated attackers, increasing the risk in environments where firewall management interfaces are exposed or accessible from untrusted networks.

Cisco released the fixes as part of a larger March 2026 firewall advisory bundle that also addressed multiple additional vulnerabilities across Secure FMC, Secure Firewall Adaptive Security Appliance (ASA), and Secure Firewall Threat Defense (FTD).

Vulnerability Type	CVE(s)	CVSS	Description
SSL VPN Denial of Service	Multiple CVEs	8.6	Multiple vulnerabilities that could allow attackers to disrupt Remote Access SSL VPN services in Cisco ASA and Secure Firewall Threat Defense.
VPN Web Server DoS	CVE-2026-20039	8.6	Vulnerability that could allow attackers to crash the VPN web server component.
TCP Flood DoS	CVE-2026-20082	8.6	Resource exhaustion vulnerability affecting Cisco ASA firewall processing.
SQL Injection	CVE-2026-20001 – CVE-2026-20003	8.1	SQL injection vulnerabilities affecting Cisco Secure Firewall Management Center.
IKEv2 DoS	CVE-2026-20013 – CVE-2026-20015	7.7	Vulnerabilities that could allow attackers to disrupt IKEv2 VPN negotiations.
IPsec DoS	CVE-2026-20049	7.7	Vulnerability that could disrupt IPsec tunnel operations.
Unauthorized File Access	CVE-2026-20062	7.2	Allows unauthorized file retrieval in ASA multiple-context mode via SCP.
OSPF Routing Vulnerabilities	Multiple CVEs	6.8	Multiple issues affecting OSPF routing operations.
SSL Decryption Policy DoS	CVE-2026-20050	6.8	Vulnerability affecting SSL inspection processing in Secure Firewall Threat Defense.
Command Injection	Multiple CVEs	6.5	Authenticated command injection vulnerabilities affecting firewall software.

Vulnerability Type	CVE(s)	CVSS	Description
Cross-Site Scripting	CVE-2026-20102, CVE-2026-20070	6.1	XSS vulnerabilities affecting SAML authentication and VPN web services.
Code Injection	CVE-2026-20008	6.0	Lua code injection vulnerability affecting firewall processing logic.
FMC Command Injection	CVE-2026-20044	6.0	Command injection vulnerability affecting Cisco Secure Firewall Management Center.
Path Traversal	CVE-2026-20018	5.9	Path traversal vulnerability affecting FMC and FTD software.
Access Control Bypass	CVE-2026-20073	5.8	ACL bypass vulnerability that could weaken firewall rule enforcement.
Snort 3 Vulnerabilities	Multiple CVEs	5.8	Multiple vulnerabilities affecting the Snort 3 detection engine that could cause denial-of-service or inspection bypass.
SSH Authentication Bypass	CVE-2026-20009	5.3	SSH partial private key authentication bypass vulnerability.
Request Smuggling	CVE-2026-20069	4.3	Client-side request smuggling vulnerability affecting VPN web services.

***Multiple CVEs referenced above include**: CVE-2026-20100, CVE-2026-20101, CVE-2026-20103, CVE-2026-20105, CVE-2026-20106, CVE-2026-20020 through CVE-2026-20025, CVE-2026-20016, CVE-2026-20017, CVE-2026-20063, CVE-2026-20064, CVE-2026-20005, CVE-2026-20006, CVE-2026-20007, CVE-2026-20052, CVE-2026-20053, CVE-2026-20054, CVE-2026-20057, CVE-2026-20058, CVE-2026-20065 through CVE-2026-20068.*

Cisco reports no active exploitation has been observed at the time of publication. Aspire recommends reading the advisories and patching immediately.

***Note**: While these vulnerabilities vary in severity, the two critical flaws affecting Cisco Secure Firewall Management Center present the greatest risk because successful exploitation could provide attackers with root-level access to the firewall management platform.*

Aspire Protects

- **Patch** - Upgrade Cisco Secure FMC Software to the fixed release found in Cisco's advisories.
  - CVE-2026-20079
  - CVE-2026-20131
- Apply updates to Cisco Security Cloud Control where applicable
- Restrict access to firewall management interfaces so they are not exposed directly to the internet
- Limit management access to trusted administrative networks or VPN connections
- Monitor firewall management logs for unusual authentication activity or unknown administrative actions

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may send crafted requests to the FMC web interface to bypass authentication or trigger remote code execution.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Cisco Secure Firewall Management Center is widely used to manage enterprise firewall deployments. Any organization operating Cisco firewall infrastructure may be affected.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability

Cisco Event Response: March 2026 Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication

Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability