Critical Cisco Firewall Management Center RCE Vulnerability

TL;DR

CVE-2026-20131 (CVSS 10.0) affects Cisco's Secure Firewall Management Center (FMC) and allows remote code execution without authentication.

An attacker could gain full control of firewall management systems and operate as root. Cisco has reported attempted exploitation.

Overview

There is a vulnerability (CVE-2026-20131, CVSS 10.0) in Cisco's Secure Firewall Management Center (FMC) software that could allow an unauthenticated attacker to execute arbitrary code on affected systems.

This issue is caused by insecure deserialization in the web-based management interface. An attacker can send a crafted request to the interface and execute Java code as root on the device.

Affected Products

- Cisco Secure Firewall Management Center (FMC) Software
- Cisco Security Cloud Control (SCC) Firewall Management

Because FMC is used to manage Cisco firewalls, successful exploitation gives the attacker control over the firewall environment itself. Once inside, they can change firewall rules or turn protections off. From there, they can move through the network and access other systems. That kind of access can lead to data theft or a full network compromise. Due to Cisco confirming attempted exploitation, Aspire recommends organizations treat this as an active risk and patch immediately.

Aspire Protects

- **Patch** - Apply Cisco's patched software immediately. See Cisco's advisory for more information.
- Restrict access to the FMC management interface (do not expose it to the internet).
- Monitor for unusual activity on firewall management systems.
- Review firewall configurations for unauthorized changes.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit the exposed FMC web interface to gain access

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute arbitrary code on the affected system

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

Organizations using Cisco firewall management systems are at risk if FMC is exposed or accessible.

- 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 Remote Code Execution Vulnerability