Cisco Secure Firewall Management Center RCE Vulnerability

TL;DR

Cisco has updated its security advisory regarding a max-severity remote code execution vulnerability (CVE-2026-20131) in Secure Firewall Management Center (FMC). The vulnerability lets an unauthenticated attacker run code as root.

The issue comes from insecure deserialization in the web interface, and Cisco has already seen attempted exploitation.

Overview

There is an update regarding a critical vulnerability (CVE-2026-20131, CVSS 10) in Cisco Secure Firewall Management Center (FMC). The vulnerability allows remote code execution in FMC without authentication. The issue is in the web-based management interface and comes down to how the system handles serialized Java data.

Affected Products

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

Not Affected

- Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Cisco Secure Firewall Threat Defense (FTD)

An attacker can send a crafted payload to the interface and trigger insecure deserialization. Once that happens, they can run arbitrary code and gain root-level control of the device. At that point, the firewall management system is no longer trustworthy.

If this is exploited, an attacker can take control of the FMC system and change firewall rules or security settings. That kind of access can open a path into the network and weaken the controls that are supposed to keep attackers out. This week, Cisco reported attempted exploitation of this vulnerability. This should be treated as an active threat, and Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Upgrade FMC to a fixed software version immediately. See Cisco's advisory for more information.
- Do not rely on mitigations - there are none that fully address this
- Restrict access to the FMC management interface - keep it off the public internet

- Review logs for unusual access to the web interface
- Segment management interfaces from production networks

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit the exposed FMC web interface by sending a crafted serialized Java payload.

Execution

- Exploitation for Client Execution [T1203] – The attacker may trigger code execution through insecure deserialization in the web application.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may gain root-level access on the device as a result of successful exploitation.

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

Any organization using Cisco Secure Firewall Management Center for centralized firewall management is at risk.

- 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