



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



**Critical Vulnerabilities in Cisco Secure Firewall Management Center (FMC)
Software**

Tracking #:432318512

Date:04-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two critical vulnerabilities have been identified in Cisco Secure Firewall Management Center (FMC) software.

TECHNICAL DETAILS:

Two critical vulnerabilities have been identified in Cisco Secure Firewall Management Center (FMC) software:

1. **Authentication Bypass Vulnerability (CVE-2026-20079):**
 - Allows an unauthenticated, remote attacker to bypass authentication and execute arbitrary scripts with root privileges on the affected system.
2. **Remote Code Execution Vulnerability (CVE-2026-20131):**
 - Allows an unauthenticated, remote attacker to execute arbitrary Java code as root due to insecure deserialization in the web interface.

Both vulnerabilities have a CVSS score of 10.0, indicating a **critical risk**, and **no workarounds are available**. Immediate action is recommended to mitigate exposure by upgrading to fixed software releases.

Vulnerability Details

1. Cisco Secure FMC Authentication Bypass

- **CVE:** CVE-2026-20079
- **CWE:** CWE-288 (Authentication Bypass)
- **Impact:** Root access to underlying OS via crafted HTTP requests.
- **Attack Vector:** Remote, unauthenticated, network-based.
- **Mechanism:** Improper system process created at boot time allows attackers to bypass authentication and execute scripts.
- **Affected Products:** Cisco Secure FMC Software (on-premises).
- **Not Affected:** Cloud-delivered FMC (cdFMC), ASA Software, FTD Software, Security Cloud Control (SCC).

2. Cisco Secure FMC Remote Code Execution (RCE)

- **CVE:** CVE-2026-20131
- **CWE:** CWE-502 (Insecure Deserialization)
- **Impact:** Remote execution of arbitrary Java code with root privileges.
- **Attack Vector:** Remote, unauthenticated, network-based.
- **Mechanism:** Insecure deserialization of user-supplied Java objects in the web management interface allows privilege escalation and full system compromise.
- **Affected Products:** Cisco Secure FMC Software and Security Cloud Control (SCC) Firewall Management.
- **Not Affected:** ASA Software, FTD Software.
- **Notes:** Limited exposure if FMC web interface is not publicly accessible.

RECOMMENDATIONS:

Immediate Software Upgrade:

- Upgrade affected Cisco FMC instances to the latest fixed versions as provided in the Cisco

advisories.

Restrict Network Access:

- Limit access to the FMC management interface to trusted internal networks only.
- Implement network segmentation and firewall rules to prevent public access

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh>