

Alert Bulletin

Bulletin N.: 80

Publication Date: 30/07/2026

Subject: Alert 2026-80 Critical Zero Day Vulnerability in Cisco Secure Firewall Management Center

Traffic Light Protocol (TLP): White

Affected Product(s):

Cisco Secure Firewall Management Center (FMC) Software

- Vulnerable versions specified by Cisco in its security advisory (consult the manufacturer's *Software Checker* to determine the exact version for each implementation).

Description

Recently, the Cisco Product Security Incident Response Team (PSIRT) disclosed vulnerability CVE-2026-20316 in Cisco Secure Firewall Management Center (FMC), the centralized platform used to manage policies, events, threat intelligence, and configurations of Cisco Secure Firewalls. Although the vulnerability has a CVSS v3.1 score of 5.3 (Medium), its operational risk is considerably higher because Cisco confirmed it is being actively exploited as a Zero Day since July 2026.

The vulnerability is due to the presence of static credentials (hardcoded/static credentials) associated with a low-privilege account included in the system. A remote unauthenticated attacker can use these credentials to log in directly to the FMC management interface without needing to know valid administrator credentials. Once authenticated with this account, the attacker can access sensitive information stored on the device and obtain a detailed view of the security infrastructure managed by the FMC.

Although the initial access corresponds only to a user with limited privileges, the exposure of sensitive information can facilitate subsequent attacks, internal reconnaissance, or chaining with other vulnerabilities. Researchers and the security community have pointed out that this vulnerability can be used as a starting point for higher-impact compromises when combined with other flaws present in the environment. Cisco also confirmed the existence of active exploit code and recommends applying the hotfixes immediately. [Reddit](#)

Solution:

Cisco released emergency hotfixes for the affected versions of Cisco Secure Firewall Management Center and recommends installing them as a priority. If a fixed version exists for the installed branch, you must immediately update to that version. sec.cloudapps.cisco.com

While the update is being implemented, it is recommended to strictly restrict access to the FMC management interface, avoiding its direct exposure to the Internet and allowing only connections from trusted administrative networks through access control lists (ACLs) or VPN. Likewise, it is advisable to review authentication logs to identify suspicious access and verify possible indicators of compromise. Reddit

Patch and official manufacturer advisory:

[Cisco Security Advisory – CVE-2026-20316](#)

Additional Information:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2>
- <https://thehackernews.com/2026/07/cisco-fmc-zero-day-actively-exploited.html>
- <https://unaaldia.hispasec.com/un-zero-day-en-cisco-secure-fmc-abre-la-puerta-a-accesos-con-credenciales-estaticas/>