

Alert Bulletin

Bulletin N.: 100

Publication Date: 11/09/2026

Subject: Alert 2026-100 Active exploitation of critical vulnerabilities in Cisco Secure FMC

Traffic Light Protocol (TLP): White

Affected product(s):

Product / service	Vulnerability	Impact	Status
Cisco Secure Firewall Management Center (FMC) Software	CVE 2026 20079	Authentication bypass and remote execution of scripts/commands as root	Confirmed active exploitation
Cisco Secure Firewall Management Center (FMC) Software	CVE 2026 20316	Unauthenticated remote login with a static low-privilege account; possible escalation through chaining with other flaws	Confirmed active exploitation
Cisco Security Cloud Control Firewall Management	CVE 2026 20079	Cloud service	Cisco indicates it has already been fixed by the vendor

Description

Active exploitation of two vulnerabilities in **Cisco Secure Firewall Management Center (FMC)** has been reported: **CVE~~2026~~20079** (CVSS 10.0), an authentication bypass that allows execution of commands as root, and **CVE~~2026~~20316** (CVSS 5.3), associated with the use of static credentials for a low-privilege account. Both flaws have been used by different threat clusters to steal credentials, deploy webshells, and, in at least one case, facilitate the deployment of **Qilin** ransomware.

Both vulnerabilities are detailed below:

- **CVE~~2026~~20079 — Authentication Bypass / RCE as root:** It has **critical** severity and CVSS **10.0**. The vulnerability originates in a system process incorrectly created during FMC startup. An unauthenticated remote attacker can send crafted HTTP requests to the web interface of a vulnerable FMC, bypass authentication, and execute scripts or commands with root privileges on the underlying operating system.

- **CVE-2026-20316 — Static credentials:** It has a CVSS score of **5.3** and is due to the presence of static credentials for a low-privilege account in FMC. An unauthenticated remote attacker can authenticate with that account and access sensitive information on the affected system. Cisco warned that this flaw can be combined with other Secure FMC vulnerabilities to elevate privileges and increase the impact.

Indicators of possible compromise

Cisco recommends examining `/var/log/messages` in FMC for references to `/var/tmp/license.tmp`. The following event indicates that the vulnerability **may have been exploited** and requires immediate investigation:

Jul 23 16:16:33 firepower sudo: www : PWD=/ ; USER=root ; COMMAND=/usr/local/sf/bin/package_info.pl /var/tmp/license.tmp -lsm

The following should also be investigated as potential indicators:

- Unrecognized or recently modified JSP files on the FMC system.
- Unusual JAR files used to execute commands.
- Processes or network connections associated with nc/Netcat, especially persistent outbound connections.
- Unauthorized Bash scripts and suspicious scheduled tasks.
- Unknown ELF files, binaries, or processes that could be linked to Cyclops Blink.
- Unauthorized queries to internal databases, anomalous accesses to authentication data, or credential modifications.
- Unusual use of built-in FMC tools for network discovery, configuration collection, or device management.

Solution

Cisco released specific *hotfixes* for the affected versions of Secure FMC, for both **CVE-2026-20079** and **CVE-2026-20316**. The organization should apply both fixes, not just the one corresponding to CVE-2026-20079, given that individual and combined use of both vulnerabilities has been observed in real intrusions.

- <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-fmc-static-cred-BET3Cjh.html>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2>

Additional information:

- [BleepingComputer — Cisco confirms CVE-2026-20079 Secure FMC flaw exploited in attacks](#)
- [The Hacker News — Cisco FMC Flaws Exploited to Steal Credentials and Deploy Qilin Ransomware](#)
- <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-fmc-static-cred-BET3Cjh.html>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2>