

Boletín de alerta

Boletín Nro.: 100

Fecha de publicación: 11/09/2026

Tema: Alerta 2026-100 Explotación activa de vulnerabilidades críticas en Cisco Secure FMC

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto / servicio	Vulnerabilidad	Impacto	Estado
Cisco Secure Firewall Management Center (FMC) Software	CVE-2026-20079	Bypass de autenticación y ejecución remota de scripts/comandos como root	Explotación activa confirmada
Cisco Secure Firewall Management Center (FMC) Software	CVE-2026-20316	Inicio de sesión remoto no autenticado con cuenta estática de bajos privilegios; posible escalada mediante encadenamiento con otras fallas	Explotación activa confirmada
Cisco Security Cloud Control Firewall Management	CVE-2026-20079	Servicio cloud	Cisco indica que ya fue corregido por el proveedor

Descripción

Se ha reportado la explotación activa de dos vulnerabilidades en **Cisco Secure Firewall Management Center (FMC)**: ~~CVE-2026-20079~~ (CVSS 10.0), un bypass de autenticación que permite ejecución de comandos como root, y ~~CVE-2026-20316~~ (CVSS 5.3), asociada al uso de credenciales estáticas para una cuenta de bajos privilegios. Ambas fallas han sido empleadas por distintos clusters de amenaza para robar credenciales, desplegar webshells y, en al menos un caso, facilitar el despliegue de ransomware **Qilin**.

A continuación se detallan ambas vulnerabilidades:

- ~~CVE-2026-20079~~ — **Authentication Bypass / RCE como root:** Tiene severidad **crítica** y CVSS **10.0**. La vulnerabilidad se origina en un proceso del sistema creado incorrectamente durante el arranque de FMC. Un atacante remoto no autenticado puede enviar solicitudes HTTP manipuladas a la interfaz

web de un FMC vulnerable, evadir la autenticación y ejecutar scripts o comandos con privilegios root en el sistema operativo subyacente.

- **CVE~~2026~~20316 — Credenciales estáticas:** Tiene puntuación CVSS **5.3** y se debe a la presencia de credenciales estáticas para una cuenta de bajos privilegios en FMC. Un atacante remoto no autenticado puede autenticarse con esa cuenta y acceder a información sensible en el sistema afectado. Cisco advirtió que esta falla puede combinarse con otras vulnerabilidades de Secure FMC para elevar privilegios y aumentar el impacto.

Indicadores de posible compromiso

Cisco recomienda examinar `/var/log/messages` en FMC en busca de referencias a `/var/tmp/license.tmp`. El siguiente evento indica que la vulnerabilidad **podría haber sido explotada** y requiere investigación inmediata:

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

También deben investigarse como potenciales indicadores:

- Archivos JSP no reconocidos o modificados recientemente en el sistema FMC.
- Archivos JAR inusuales usados para ejecutar comandos.
- Procesos o conexiones de red asociados a nc/Netcat, especialmente conexiones salientes persistentes.
- Scripts Bash no autorizados y tareas programadas sospechosas.
- Archivos, binarios o procesos ELF desconocidos que pudieran estar vinculados a Cyclops Blink.
- Consultas no autorizadas a bases de datos internas, accesos anómalos a datos de autenticación o modificaciones de credenciales.
- Uso inusual de herramientas integradas de FMC para descubrimiento de red, recolección de configuraciones o administración de dispositivos.

Solución

Cisco publicó *hotfixes* específicos para las versiones afectadas de Secure FMC, tanto para **CVE~~2026~~20079** como para **CVE~~2026~~20316**. La organización debe aplicar ambos fixes, no solo el correspondiente a CVE~~2026~~20079, dado que se ha observado uso individual y combinado de las dos vulnerabilidades en intrusiones reales.

- <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>

Información adicional:

- [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>