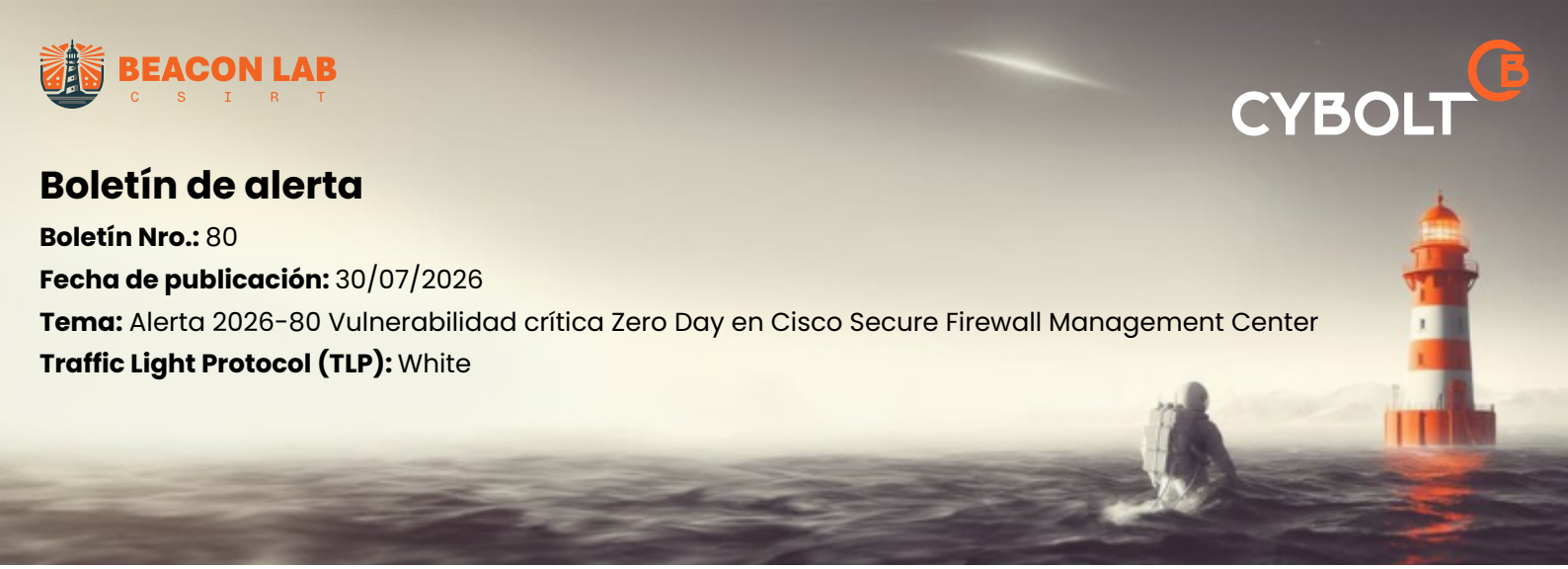

Boletín de alerta

Boletín Nro.: 80
Fecha de publicación: 30/07/2026
Tema: Alerta 2026-80 Vulnerabilidad crítica Zero Day en Cisco Secure Firewall Management Center
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Cisco Secure Firewall Management Center (FMC) Software

- Versiones vulnerables especificadas por Cisco en su aviso de seguridad (consultar el *Software Checker* del fabricante para determinar la versión exacta de cada implementación).

Descripción

Recientemente, el Cisco Product Security Incident Response Team (PSIRT) reveló la vulnerabilidad CVE-2026-20316 en Cisco Secure Firewall Management Center (FMC), la plataforma centralizada utilizada para administrar políticas, eventos, inteligencia de amenazas y configuraciones de los firewalls Cisco Secure Firewall. Aunque la vulnerabilidad posee una puntuación CVSS v3.1 de 5.3 (Media), su riesgo operativo es considerablemente mayor debido a que Cisco confirmó que está siendo explotada activamente como Zero Day desde julio de 2026.

La vulnerabilidad se debe a la presencia de credenciales estáticas (hardcoded/static credentials) asociadas a una cuenta de bajo privilegio incluida en el sistema. Un atacante remoto no autenticado puede utilizar dichas credenciales para iniciar sesión directamente en la interfaz de administración del FMC sin necesidad de conocer credenciales válidas del administrador. Una vez autenticado con esta cuenta, el atacante puede acceder a información sensible almacenada en el dispositivo y obtener una visión detallada de la infraestructura de seguridad administrada por el FMC.

Aunque el acceso inicial corresponde únicamente a un usuario con privilegios limitados, la exposición de información sensible puede facilitar ataques posteriores, reconocimiento interno o el encadenamiento con otras vulnerabilidades. Investigadores y la comunidad de seguridad han señalado que esta vulnerabilidad puede utilizarse como punto de partida para compromisos de mayor impacto cuando se combina con otras fallas presentes en el entorno. Cisco confirmó además la existencia de código de explotación activo y recomienda aplicar los hotfixes de manera inmediata. Reddit

Solución:

Cisco publicó hotfixes de emergencia para las versiones afectadas de Cisco Secure Firewall Management Center y recomienda instalarlos de forma prioritaria. En caso de existir una versión fija para la rama instalada, debe actualizarse inmediatamente a dicha versión. sec.cloudapps.cisco.com

Mientras se implementa la actualización, se recomienda restringir estrictamente el acceso a la interfaz de administración del FMC, evitando su exposición directa a Internet y permitiendo únicamente conexiones desde redes administrativas confiables mediante listas de control de acceso (ACL) o VPN. Asimismo, es recomendable revisar los registros de autenticación para identificar accesos sospechosos y verificar posibles indicadores de compromiso. Reddit

Parche y aviso oficial del fabricante:

Cisco Security Advisory – CVE-2026-20316

Información adicional:

- **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/**