Boletín de alerta

Boletín Nro.:
Fecha de publicación: 15/08/2025
Tema: Alerta 2025-70 Falla Crítica CISCO FMC
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Cisco Secure Firewall Management Center (FMC)** versiones **7.0.7** y **7.7.0** con autenticación **RADIUS** habilitada

Descripción

Se ha identificado la vulnerabilidad crítica **CVE-2025-20265** con una puntuación **CVSS de 10.0** (máxima gravedad) en **Cisco Secure Firewall Management Center (FMC)**.
El fallo reside en el subsistema **RADIUS**, donde una validación inadecuada de la entrada del usuario permite que un atacante remoto no autenticado envíe credenciales especialmente diseñadas para ejecutar comandos con privilegios elevados en el dispositivo.

La explotación es posible cuando el FMC está configurado para autenticación RADIUS en la interfaz web de administración, en SSH o en ambas. Esto podría comprometer por completo la integridad, disponibilidad y confidencialidad de los sistemas afectados.

Solución:

Actualizar inmediatamente los dispositivos a la version **mas actual**

Información adicional:

- Vulnerabilidad de ejecución remota de código RADIUS del software Cisco Secure Firewall Management Center
- Aviso de seguridad urgente: CVE-2025-20265 – Vulnerabilidad RCE crítica (CVSS 10.0) en Cisco Secure FMC – Seguridad de ruta crítica
- Cisco advierte sobre la falla CVSS 10.0 FMC RADIUS que permite la ejecución remota de código