Cisco ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en el software Secure Firewall Management Center (FMC), la cual podría permitir a un atacante ejecutar código arbitrario en los sistemas afectados.

La falla, catalogada con el identificador CVE-2025-20265 (puntaje CVSS: 10.0), impacta la implementación del subsistema RADIUS. Esto abre la posibilidad de que un atacante remoto y no autenticado inyecte comandos arbitrarios en la terminal, los cuales serían ejecutados directamente por el dispositivo.

El fabricante explicó que el origen del problema se debe a la falta de un manejo adecuado de la entrada de datos del usuario durante el proceso de autenticación. Como consecuencia, un atacante podría enviar información especialmente manipulada al introducir credenciales, logrando que se validen en el servidor RADIUS configurado.

"Una explotación exitosa podría permitir al atacante ejecutar comandos con un nivel elevado de privilegios", señaló la compañía en un aviso emitido el jueves. *"Para que esta vulnerabilidad pueda ser aprovechada, el software Cisco Secure FMC debe estar configurado para autenticación RADIUS ya sea en la interfaz de administración web, en la administración mediante SSH, o en ambas"*.

El fallo afecta a las versiones 7.0.7 y 7.7.0 de Cisco Secure FMC Software, siempre que tengan habilitada la autenticación RADIUS. No existen soluciones temporales, salvo aplicar los parches proporcionados por Cisco. El crédito por descubrir el problema corresponde a Brandon Sakai, miembro del equipo de pruebas internas de seguridad de la empresa.

Además del CVE-2025-20265, Cisco solucionó múltiples vulnerabilidades de alta severidad:

- CVE-2025-20217 (CVSS 8.6) – Vulnerabilidad de denegación de servicio en Snort 3 de Cisco Secure Firewall Threat Defense Software
- CVE-2025-20222 (CVSS 8.6) – Vulnerabilidad de denegación de servicio en Cisco Secure Firewall ASA y Threat Defense para Firepower 2100 Series con IPv6 sobre IPsec
- CVE-2025-20224, CVE-2025-20225, CVE-2025-20239 (CVSS 8.6) – Vulnerabilidades de

denegación de servicio en Cisco IOS, IOS XE, Secure Firewall ASA y Threat Defense en IKEv2

- CVE-2025-20133, CVE-2025-20243 (CVSS 8.6) – Vulnerabilidades de denegación de servicio en Cisco Secure Firewall ASA y Threat Defense mediante SSL VPN de acceso remoto
- CVE-2025-20134 (CVSS 8.6) – Vulnerabilidad de denegación de servicio en certificados SSL/TLS en Cisco Secure Firewall ASA y Threat Defense
- CVE-2025-20136 (CVSS 8.6) – Vulnerabilidad de denegación de servicio en inspección DNS con NAT en Cisco Secure Firewall ASA y Threat Defense
- CVE-2025-20263 (CVSS 8.6) – Vulnerabilidad de denegación de servicio en servicios web de Cisco Secure Firewall ASA y Threat Defense
- CVE-2025-20148 (CVSS 8.5) – Vulnerabilidad de inyección HTML en Cisco Secure Firewall Management Center Software
- CVE-2025-20251 (CVSS 8.5) – Vulnerabilidad de denegación de servicio en el servidor web de VPN en Cisco Secure Firewall ASA y Threat Defense
- CVE-2025-20127 (CVSS 7.7) – Vulnerabilidad de denegación de servicio en TLS 1.3 Cipher en Cisco Secure Firewall ASA y Threat Defense para Firepower 3100 y 4200 Series
- CVE-2025-20244 (CVSS 7.7) – Vulnerabilidad de denegación de servicio en el servidor web de VPN de acceso remoto en Cisco Secure Firewall ASA y Threat Defense

Aunque hasta el momento no existen indicios de explotación activa de estas fallas en entornos reales, los dispositivos de red siguen siendo un objetivo recurrente de los atacantes. Por ello, resulta fundamental que los administradores actualicen sus instancias a la versión más reciente lo antes posible.