Alerta

Técnica

Vulnerabilidades Críticas Detectadas

COLCERT AL-20250819 -073

TLP:CLEAR

Durante el monitoreo de fuentes abiertas realizada por ColCERT se detectó la vulnerabilidad CVE-2025-20265, catalogada como crítica (CVSS 10.0) y que afecta a **Cisco Secure Firewall Management Center (FMC)**. Cuando la plataforma está configurada con el sistema de autenticación RADIUS para la consola web o SSH, permite a un ciberdelincuente remoto no autenticado inyectar comandos de shell durante el proceso de autenticación debido a una validación insuficiente de la entrada, logrando **ejecución de comandos con privilegios elevados** y posible **toma de control del plano** de gestión. Aunque no hay evidencia pública de explotación activa en el momento de los avisos, el riesgo es máximo por la posibilidad de acceso completo y desactivación de defensas en un componente central de la administración de firewalls.

NIVEL DE RIESGO

ALTO

Como medida urgente se deben actualizar las instancias FMC a la última versión o alternativamente desactivar la autenticación RADIUS. (Remote Authentication Dial-In User Service) es un protocolo usado para autenticar usuarios en servicios como VPN o acceso web/SSH. Si no se valida correctamente, puede ser vulnerable a ataques como la inyección de comandos).

¿Cómo se explota esta vulnerabilidad?

1. Se requiere que Cisco Secure Firewall Management Center (FMC) esté específicamente en **las versiones 7.0.7** o **7.7.0** con autenticación RADIUS habilitada en la interfaz de gestión web o SSH, ya que es la configuración que permite la explotación.
2. Se inicia un intento de autenticación hacia el FMC para que el dispositivo envíe las credenciales proporcionadas al servidor RADIUS configurado.
3. En lugar de credenciales válidas, se envían entradas especialmente construidas que incluyen metacaracteres o secuencias de inyección de comandos, aprovechando la validación insuficiente de la entrada durante el proceso de autenticación.
4. El FMC procesa esa entrada y, al interactuar con el servidor RADIUS, termina interpretando partes de las credenciales como comandos de sistema, ejecutándolos con privilegios elevados en el plano de gestión del dispositivo.
5. Con la ejecución de comandos conseguida, se pueden crear cuentas administrativas, extraer configuraciones y credenciales, modificar políticas y objetos de red, y preparar accesos persistentes (por ejemplo, claves SSH o tareas programadas).
6. Una vez dentro se puede limitar el acceso legítimo alterando reglas y controles de administración, deshabilitar registros o alertas.

Debido a estas potenciales acciones, el riesgo es máximo y exige aplicar los parches de seguridad de agosto de 2025 de inmediato o alternativamente y de forma temporal, deshabilitar RADIUS y limitar estrictamente el acceso a la administración hasta completar la actualización.

Técnicas MITRE ATT&CK Asociadas

A continuación, se mapean las técnicas MITRE ATT&CK más relevantes para CVE-2025-20265 en Cisco Secure FMC, enfocadas en cómo un actor pasa de la explotación inicial vía RADIUS a la ejecución de comandos, escalamiento de privilegios.

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación de aplicación expuesta	T1190	Se aprovecha la interfaz de gestión web/SSH del FMC expuesta para inyectar comandos durante la autenticación RADIUS.
Interprete de comandos y scripts	T1059	Se ejecutan comandos de shell en el FMC como resultado de la inyección en el flujo de autenticación RADIUS.
Explotación para escalamiento de privilegios	T1068	Tras la inyección de comandos exitosa, se obtiene permisos elevados en el plano de gestión de FMC que permiten controlar las configuraciones y políticas.
Creación de cuentas	T1136	Tras comprometer el FMC, el atacante puede crear usuarios administrativos para mantener acceso persistente.

Mitigaciones MITRE

Para mitigar el riesgo asociado a CVE-2025-20265 en Cisco Secure FMC, se proponen mitigaciones alineadas con MITRE ATT&CK que priorizan el parchado inmediato, la reducción de la superficie de exposición del plano de gestión (en especial RADIUS) y el control de accesos y cuentas.

MITIGACIÓN	CÓDIGO	RELEVANCIA
Actualización de software	M1051	Establecer un proceso de parchado rápido para FMC y componentes relacionados, aplicar de inmediato los parches de seguridad y retirar las versiones 7.0.7/7.7.0 vulnerables.
Segmentación de red	M1030	Aislar la gestión del FMC en redes de administración dedicadas, con listas de control de acceso y VPN administrativas; bloquear acceso desde Internet.
Deshabilitar o remover funciones	M1042	Deshabilitar temporalmente RADIUS en FMC si no es imprescindible y usar cuentas locales/LDAP/SAML.
Autenticación multifactor	M1032	Requerir MFA robusto para todas las cuentas de administración y acceso remoto a la consola del FMC.
Gestión de cuentas de usuario	M1018	Aplicar mínimos privilegios, rotación de credenciales, cuentas separadas para administración y auditoria, revisar y revocar cuentas inactivas.
Políticas de contraseñas	M1027	Implementar políticas de contraseñas fuertes, sin reutilización y con almacenamiento seguro.
Monitor Activity	(M1039)	Implementar en la fase post-explotación mediante revisión de eventos anómalos o creación de cuentas.

Impacto para Colombia y la región

Sectores afectados: Gobierno, salud, financiero, educación e infraestructura crítica, así como empresas privadas que utilicen Cisco Secure Firewall Management Center (FMC) que estén configurados con el sistema de autenticación RADIUS.

Riesgo alto de ciberataques: La vulnerabilidad crítica CVE-2025-20265 permite a ciberdelincuentes remotos ejecutar comandos con privilegios sin autenticación previa, afectando gravemente a sistemas que usan RADIUS para gestión web o SSH. Aunque no hay reportes públicos de explotación, su alcance y severidad requieren atención inmediata, siendo el parche oficial la única solución efectiva.

Consecuencias: la explotación de esta falla en Cisco FMC puede dar a un atacante control total del sistema, permitir ataques en cadena contra redes protegidas, provocar la caída de servicios críticos y causar graves daños reputacionales y sanciones regulatorias, especialmente en sectores sensibles como gobierno, salud y financiero.

Implicaciones en seguridad digital: Su explotación pondría en riesgo la continuidad de servicios esenciales, la protección de datos sensibles y la confianza en los sistemas nacionales, lo que destaca la necesidad de reforzar la gestión de parches, el control de accesos, la segmentación de redes y la cooperación interinstitucional para prevenir y responder de forma coordinada a incidentes de este tipo.

Otras vulnerabilidades

Adicionalmente, en el mismo parche de seguridad enfocado para resolver CVE-2025-20265, Cisco resolvió múltiples vulnerabilidades. Si bien ninguna de estas vulnerabilidades ha tenido reportes de estar siendo explotadas, es importante realizar las actualizaciones de seguridad lo antes posible.

CVE	Productos afectados	CVSS
CVE-2025-20217	Cisco Secure Firewall Threat Defense Software Snort 3 Denial-of-Service Vulnerability	8.6
CVE-2025-20222	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Firepower 2100 Series IPv6 over IPsec Denial-of-Service Vulnerability	8.6
CVE-2025-20224, CVE-2025-20225, CVE-2025-20239	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial-of-Service Vulnerabilities	8.6
CVE-2025-20133, CVE-2025-20243	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial-of-Service Vulnerabilities	8.6
CVE-2025-20134	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SSL/TLS Certificate Denial-of-Service Vulnerability	8.6

CVE	Productos afectados	CVSS
CVE-2025-20136	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial-of-Service Vulnerability	8.6
CVE-2025-20263	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Web Services Denial-of-Service Vulnerability	8.6
CVE-2025-20148	Cisco Secure Firewall Management Center Software HTML Injection Vulnerability	8.5
CVE-2025-20251	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Server Denial-of-Service Vulnerability	8.5
CVE-2025-20127	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Firepower 3100 and 4200 Series TLS 1.3 Cipher Denial-of-Service Vulnerability	7.7
CVE-2025-20244	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access VPN Web Server Denial-of-Service Vulnerability	7.7

Comunicado Cisco

Por su parte Cisco emitió un aviso oficial en su portal de seguridad sobre CVE-2025-20265, donde detalla que el fallo reside en el subsistema RADIUS de Secure Firewall Management Center, afecta a FMC 7.0.7 y 7.7.0 cuando RADIUS está habilitado en la gestión web o SSH, permite inyección de comandos con ejecución a alto privilegio, no cuenta con "workarounds" efectivos y requiere actualizar de inmediato como medida principal; además, lo incluyó dentro de un paquete de comunicados de agosto de 2025 que también corrige otras vulnerabilidades de alta severidad en sus productos.

Recomendaciones

- Aplicar de inmediato los parches oficiales de seguridad de agosto de 2025 para las versiones FMC 7.0.7 y 7.7.0; planificar mantenimiento prioritario y validar la versión posterior a la actualización.
- Si el parche no es posible de forma inmediata, deshabilitar RADIUS en FMC temporalmente y migrar a cuentas locales.
- Restringir el acceso a la gestión del FMC (HTTPS/SSH) solo desde redes de administración dedicadas mediante listas de permitidos, VPN administrativa y segmentación.
- Auditar configuraciones y objetos del FMC tras el parchado para detectar cambios no autorizados, usuarios añadidos y claves/credenciales almacenadas.
- Implementar reglas de monitoreo para detectar eventos anómalos en el FMC (por ejemplo, nuevos usuarios, cambios no autorizados, o ejecuciones inusuales), que sirvan como señal temprana de actividad maliciosa tras una intrusión.
- Revisar los logs del FMC antes de aplicar el parche para identificar posibles intentos de explotación anteriores, especialmente si el sistema ha estado expuesto con RADIUS activo.

COLCERT

Fuentes

Cisco, 14 de agosto de 2025, "Cisco Secure Firewall Management Center Software RADIUS Remote Code Execution Vulnerability", Fuente oficial.
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79

Cisco, 14 de agosto de 2025, "Cisco Event Response: August 2025 Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication", Fuente oficial.
https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75415

The Hacker News, 15 de agosto de 2025, "Cisco Warns of CVSS 10.0 FMC RADIUS Flaw Allowing Remote Code Execution" Web de noticias de ciberseguridad.
https://thehackernews.com/2025/08/cisco-warns-of-cvss-100-fmc-radius-flaw.html