Boletín de alerta

Boletín Nro.:
Fecha de publicación: 19/03/2026
Tema: Alerta 2026-26 Vulnerabilidad crítica en Cisco bajo explotación activa
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Cisco Secure Firewall Management Center (FMC)
- Cisco Security Cloud Control (SCC)
- Infraestructuras que expongan la interfaz web de administración de FMC

Descripción

Se ha identificado la vulnerabilidad **CVE-2026-20131 (CVSS 10.0 – Crítica)**, actualmente **explotada activamente como 0-day** por el grupo de ransomware Interlock desde finales de enero de 2026.

La falla corresponde a una **ejecución remota de código (RCE)** causada por una **deserialización insegura en Java** dentro de la interfaz web de Cisco FMC. Un atacante remoto no autenticado puede enviar objetos Java manipulados para ejecutar código arbitrario con privilegios de **root**, comprometiendo completamente el dispositivo.

Investigaciones de inteligencia de amenazas revelan que esta vulnerabilidad fue explotada **36 días antes de su divulgación pública**, permitiendo a los atacantes comprometer organizaciones sin ser detectados. La explotación se realiza mediante solicitudes HTTP especialmente diseñadas que activan la ejecución de código y validan el acceso mediante comunicación con servidores externos.

El sistema de inteligencia de amenazas de Amazon ha identificado una campaña activa de ransomware **Interlock** que explota la vulnerabilidad CVE-2026-20131, una vulnerabilidad crítica en el software Cisco Secure Firewall Management Center (FMC) que podría permitir a un atacante remoto no autenticado ejecutar código Java arbitrario como root en un dispositivo afectado.

Una vez dentro, el grupo Interlock despliega múltiples herramientas maliciosas, incluyendo scripts de reconocimiento, troyanos de acceso remoto, webshells en memoria y malware tipo ELF. Estas herramientas permiten mantener persistencia, ejecutar comandos, robar información, moverse lateralmente y evadir controles de seguridad. También utilizan herramientas legítimas como ScreenConnect para acceso remoto encubierto y técnicas de limpieza de logs para ocultar evidencia.

Este grupo, activo desde 2024, ha atacado sectores críticos como salud, educación, industria y gobierno, utilizando tácticas avanzadas de ransomware y exfiltración de datos.

Indicadores de compromiso (IoC)

Los siguientes indicadores respaldan las medidas defensivas que pueden adoptar las organizaciones afectadas. Debido a que Interlock utiliza técnicas de variación de contenido, la mayoría de los hashes de archivos no se consideran indicadores fiables. El atacante modificó la mayoría de los artefactos, como scripts y binarios, descargados a diferentes objetivos. Esto generó hashes de archivos distintos para herramientas funcionalmente idénticas. Esta personalización permitió que cada ataque eludiera la detección basada en firmas, que busca coincidencias exactas de archivos.

206.251.239[.]164	Exploit source IP	Activ Jan
199.217.98[.]153	Exploit source IP	Activ Mar
89.46.237[.]33	Exploit source IP	Activ Mar
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0	Exploit HTTP User-Agent	Obs Jan and 2026
b885946e72ad51dca6c70abc2f773506	Exploit TLS JA3	Obs Jan and 2026
f80d3d09f61892c5846c854dd84ac403	Exploit TLS JA3	Obs Mar
t13i1811h1_85036bcba153_b26ce05bbdd6	Exploit TLS JA4	Obs Jan and 2026
t13i4311h1_c7886603b240_b26ce05bbdd6	Exploit TLS JA4	Obs Mar
144.172.94[.]59	C2 Fallback IP	Activ Mar
199.217.99[.]121	C2 Fallback IP	Activ Mar
188.245.41[.]78	C2 Fallback IP	Activ Mar

144.172.110[.]106	Backend C2 IP	Acti Mar
95.217.22[.]175	Backend C2 IP	Acti Mar
37.27.244[.]222	Staging host IP	Acti Mar
hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion/chat.php	Ransom negotiation portal	Acti Mar
cherryberry[.]click	Exploit Support Domain	Acti Jan
ms-server-default[.]com	Exploit Support Domain	Acti Mar
initialize-configs[.]com	Exploit Support Domain	Acti Mar
ms-global.first-update-server[.]com	Exploit Support Domain	Acti Mar
ms-sql-auth[.]com	Exploit Support Domain	Acti Mar
kolonialeru[.]com	Exploit Support Domain	Acti Mar
sclair.it[.]com	Exploit Support Domain	Acti Mar
browser-updater[.]com	C2 domain	Acti Mar
browser-updater[.]live	C2 domain	Acti Mar
os-update-server[.]com	C2 domain	Acti Mar
os-update-server[.]org	C2 domain	Acti Mar

os-update-server[.]live	C2 domain	Activ Mar
os-update-server[.]top	C2 domain	Activ Mar
d1caa376cb45b6a1eb3a45c5633c5ef75f7466b8601ed72c8022a8b3f6c1f3be	Offensive security tool (Certify)	Obs Mar
6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f	Screen locker	Obs Mar

Solución y mitigaciones:

- Actualizar inmediatamente a la versión corregida proporcionada por Cisco.
- Restringir el acceso a la interfaz de administración (FMC) únicamente a redes internas o direcciones IP confiables.
- Revisar logs y buscar Indicadores de Compromiso (IoCs) asociados a actividad sospechosa

Información adicional:

- https://thehackernews.com/2026/03/interlock-ransomware-exploits-cisco-fmc.html
- https://securityaffairs.com/189636/malware/interlock-group-exploiting-the-cisco-fmc-flaw-cve-2026-20131-36-days-before-disclosure.html
- https://aws.amazon.com/it/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh