Boletín informativo
Vulnerabilidad en Cisco Secure (FMC)

CSIRTSALUD-AV-20260319-37

TLP: CLEAR

Incidente ID:	037
Fecha del reporte:	19/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidades en Cisco Secure Firewall Management Center
Herramienta de detección	N/A
Activo involucrado:	CISCO
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema y orientar a los equipos de ciberseguridad, administradores de red y gestores de riesgo sobre la vulnerabilidad crítica CVE-2026-20131, identificada en el software Cisco Secure Firewall Management Center (FMC). Esta vulnerabilidad ha sido clasificada con la puntuación máxima de severidad (CVSS 10.0) y se encuentra siendo explotada activamente por el grupo de ransomware Interlock, habiendo detectado actividad maliciosa desde el 26 de enero de 2026, más de un mes antes de su divulgación pÚblica por parte de Cisco el 4 de marzo de 2026.

Descripción:

CVE-2026-20131 es una vulnerabilidad de ejecución remota de código (RCE) que reside en la interfaz de administración web del software Cisco Secure Firewall Management Center (FMC). La falla esta categorizada bajo CWE-502 (Deserialización de datos no confiables) y tiene origen en el procesamiento inseguro de flujos de bytes Java serializados por parte de la interfaz de gestión web.

La serialización en Java es un mecanismo que convierte objetos en flujos de bytes para su transmisión o almacenamiento. La deserialización es el proceso inverso: reconstruir el objeto a partir de esos bytes. El problema surge cuando una aplicación Java acepta y deserializa

datos provenientes de fuentes no confiables (como peticiones HTTP externas) sin validar la integridad ni la seguridad de esos datos.

En el contexto de Cisco FMC, la interfaz de administración web acepta objetos Java serializados de fuentes remotas no autenticadas. La aplicación no implementa validación look-ahead ni una lista blanca de clases permitidas antes de iniciar el proceso de deserialización. Esto permite a un atacante suministrar un grafo de objetos diseñado, conocido como cadena de gadgets (gadget chain), utilizando clases ya presentes en el classpath de la aplicación, como bibliotecas comunes del ecosistema Java (por ejemplo, Apache Commons Collections o Spring Framework). Al manipular las propiedades de estos objetos, el atacante obliga a la Máquina Virtual Java (JVM) a ejecutar comandos arbitrarios durante la reconstrucción del objeto, eludiendo por completo la lógica de la aplicación.

La vulnerabilidad no requiere autenticación previa ni interacción del usuario. Un atacante remoto con acceso de red a la interfaz de administración puede comprometer totalmente el sistema. No existen soluciones alternativas (workarounds) que mitiguen el riesgo; la única solución es aplicar el parche del fabricante.

La explotación exitosa de CVE-2026-20131 otorga al atacante control total como root sobre el dispositivo FMC comprometido. Dado que FMC es el cerebro centralizado de la infraestructura de seguridad de red, gestionando múltiples firewalls downstream, sus consecuencias tienen efectos en cascada sobre toda la organización:

Acceso root total al sistema	El atacante obtiene los privilegios más altos posibles sobre el sistema operativo Linux subyacente del FMC.
Manipulación de políticas de seguridad	Posibilidad de modificar, deshabilitar o eliminar reglas de firewall, ACLs, IPS/IDS, filtrado de URL y control de aplicaciones en todos los dispositivos gestionados.

Exfiltración de configuraciones criticas	Robo de configuraciones completas de red, credenciales, claves VPN, políticas de seguridad y datos sensibles almacenados en el FMC.
Instalación de backdoors persistentes	Despliegue de implantes maliciosos (RATs) que sobreviven a reinicios, garantizando acceso continuo al entorno comprometido.
Movimiento lateral hacia firewalls	Uso del FMC como pivote para comprometer los dispositivos FTD gestionados, potencialmente deshabilitando controles de seguridad a nivel empresarial.
Despliegue de ransomware	Como lo demostró el grupo Interlock, el acceso root permite desplegar ransomware que cifra sistemas en toda la red, causando interrupción operacional.
Impacto regulatorio y legal	En caso de exfiltración de datos, la organización puede enfrentar sanciones bajo regulaciones de protección de datos como GDPR, CCPA o normativas locales.

Modo de explotación y cadena de infección

A continuación se describe en detalle la cadena de ataque (kill chain) observada en la explotación activa de CVE-2026-20131 por parte del grupo Interlock, basada en la investigación de Amazon MadPot y el análisis del kit de herramientas operacional expuesto inadvertidamente por los atacantes.

- **Reconocimiento**

El atacante realiza reconocimiento para identificar instancias de Cisco Secure FMC expuestas. Herramientas como Shodan, Censys o Fofa son utilizadas para buscar interfaces web del FMC accesibles en Internet (típicamente en los puertos TCP/443 o TCP/8443). El atacante verifica si la versión del sistema es vulnerable antes de proceder.

- **Generación del Payload Malicioso**

Con herramientas como ysoserial (una utilidad especializada en la creación de payloads de deserialización Java), el atacante genera un objeto Java serializado malicioso. Este payload contiene una cadena de gadgets compatible con las bibliotecas presentes en el entorno del FMC (ej. Apache Commons Collections, Spring Framework). La carga maliciosa comienza con los bytes mágicos de serialización Java: 0xAC ED 00 05, identificadores reconocibles en el tráfico de red. El payload incluye dos URLs embebidas: una para entregar datos de configuración del exploit y otra para confirmar la explotación exitosa mediante una petición HTTP PUT saliente del sistema comprometido.

- **Entrega y Explotación**

El atacante envía una petición HTTP POST especialmente diseñada al endpoint vulnerable de la interfaz web del FMC. El cuerpo de la petición contiene el objeto Java serializado malicioso. Al recibir la petición, el servidor FMC intenta deserializar el objeto sin validación previa. La cadena de gadgets se activa durante la reconstrucción del objeto, forzando a la JVM a ejecutar un comando del sistema. El comando ejecutado realiza una petición HTTP PUT hacia el servidor del atacante para confirmar la explotación exitosa (beacon de confirmación).

- **Post-Explotación Inicial**

Una vez confirmada la explotación, el servidor de comando y control (C2) del atacante emite instrucciones para descargar y ejecutar un binario ELF malicioso desde el servidor remoto. Este binario es el primer implante en el sistema comprometido y constituye la puerta de entrada para el despliegue del kit completo de herramientas de Interlock.

- **Despliegue de Herramientas Avanzadas**

Con acceso root establecido, el atacante despliega su kit operacional completo: (a) Un script PowerShell de reconocimiento sistemático que recopila información detallada del entorno Windows, incluyendo sistemas operativos, servicios, software instalado, VMs Hyper-V, artefactos de navegadores web (historial, credenciales almacenadas), conexiones de red activas, tablas ARP y eventos de autenticación RDP. (b) Un RAT en JavaScript ofuscado que establece comunicaciones C2 cifradas mediante WebSocket con claves RC4 aleatorias por mensaje, capaz de ejecutar comandos, transferir archivos y crear túneles SOCKS5. (c) Un RAT

equivalente implementado en Java (basado en GlassFish/Grizzly) para redundancia en caso de que el implante JS sea detectado. (d) Un script Bash que configura servidores Linux como proxies HAProxy para enmascarar el tráfico de C2 y exfiltración, con borrado de logs cada 5 minutos vía cron.

- **Movimiento Lateral y Persistencia**

Desde el FMC comprometido, los atacantes pivotan hacia la red de gestión interna, comprometiendo los firewalls FTD gestionados y otros activos de red críticos. ConnectWise ScreenConnect es instalado como mecanismo de acceso persistente alternativo. Los atacantes mantienen acceso durante semanas antes de activar el payload de ransomware, maximizando el impacto y asegurando la exfiltración de datos sensibles para la doble extorsión.

- **Exfiltración y Cifrado**

Antes del cifrado, los atacantes exfiltran datos sensibles (configuraciones de red, credenciales, políticas de seguridad, datos de clientes) para utilizarlos en la estrategia de doble extorsión. Finalmente, el ransomware Interlock/Slopoly es desplegado, cifrando sistemas en toda la red. La nota de rescate característica de Interlock es distribuida, amenazando con publicar los datos robados y citar violaciones regulatorias para presionar el pago.

VULNERABILIDADES PARCHADAS EN EL MISMO AVISO

El 4 de marzo de 2026, Cisco publico actualizaciones de seguridad que abordaron múltiples vulnerabilidades en los productos Secure FMC, ASA y FTD. A continuación se describen las principales vulnerabilidades incluidas en el mismo ciclo de parchado:

CVE-2026-20131 | CVSS 10.0 | CRITICO

Deserialización insegura de flujo de bytes Java (CWE-502) en la interfaz de administración web de Cisco Secure FMC. Permite a un atacante remoto no autenticado ejecutar código Java

arbitrario como root enviando un objeto Java serializado malicioso. No existen workarounds; requiere actualización inmediata de software.

CVE-2026-20079 | CVSS 10.0 | CRITICO

Omisión de autenticación en la interfaz de administración web de Cisco Secure FMC, ocasionada por un proceso del sistema creado incorrectamente durante el arranque del dispositivo (improper system process at boot). Un atacante remoto no autenticado puede eludir la autenticación y ejecutar scripts con privilegios root enviando peticiones HTTP diseñadas. Esta vulnerabilidad permite al atacante ejecutar una variedad de scripts y comandos que otorgan acceso root al sistema operativo subyacente.

CVE-2026-20001, CVE-2026-20002, CVE-2026-20003 | Inyección SQL en FMC

Tres vulnerabilidades de inyección SQL en diferentes componentes de la interfaz de Cisco Secure FMC. A diferencia de las anteriores, estas requieren autenticación previa. Un usuario autenticado con privilegios bajos podría explotar estas fallas para ejecutar sentencias SQL arbitrarias, comprometiendo la integridad y confidencialidad de la base de datos de gestión del FMC. Se recomienda auditar cuentas de usuario, aplicar el principio de mínimo privilegio y habilitar autenticación multifactor (MFA) para todos los accesos administrativos.

CVE-2026-20062 | CVSS 7.2 | ALTO - Acceso a Archivos en Cisco ASA

Vulnerabilidad de acceso a archivos en Cisco ASA Software en modo de múltiples contextos con la pila SSH de Cisco habilitada. Requiere que el atacante este autenticado y con acceso local. La explotación permite leer o sobrescribir archivos sensibles entre contextos de privilegio mediante SCP, comprometiendo la confidencialidad e integridad de configuraciones críticas de los dispositivos ASA. Aplica específicamente a entornos ASA con múltiple context mode activo.

Multiples CVEs de alta severidad en FMC, ASA/FTD

Adicionalmente, Cisco parcheo 15 vulnerabilidades de alta severidad en Secure FMC, Secure Firewall Adaptive Security Appliance (ASA) y Secure Firewall Threat Defense (FTD), incluyendo fallas de denegación de servicio (DoS) en implementaciones SSL VPN de acceso remoto. Las organizaciones deben revisar el aviso completo de Cisco y usar el Cisco Software Checker para identificar las versiones con parche aplicable a su infraestructura especifica.

Relación con tácticas MITRE ATT&CK

La cadena de ataque asociada a CVE-2026-20131 y la campaña Interlock se mapea con las siguientes tácticas y técnicas del framework MITRE ATT&CK for Enterprise:

ID Técnica	Táctica	Técnica / Sub-Técnica	Descripción en el Contexto del Ataque
T1190	**Acceso Inicial**	Exploit Public-Facing Application	explotación de CVE-2026-20131 en la interfaz web pública del FMC sin autenticación para obtener RCE como root.
T1059.007	**Ejecución**	Command and Scripting Interpreter: JavaScript	Uso del RAT en JavaScript para ejecución de comandos remotos y shell interactivo en sistemas comprometidos.
T1059.001	**Ejecución**	Command and Scripting Interpreter: PowerShell	Script PowerShell para reconocimiento sistemático del entorno Windows de la víctima.

ID Técnica	Táctica	Técnica / Sub-Técnica	Descripción en el Contexto del Ataque
T1053.003	**Persistencia**	Scheduled Task/Job: Cron	Cron job configurado para borrar logs cada 5 minutos y mantener la persistencia del proxy HTTP.
T1133	**Persistencia**	External Remote Services	Instalación de ConnectWise ScreenConnect como canal de acceso remoto persistente.
T1543	**Persistencia**	Create or Modify System Process	Configuración de HAProxy como servicio systemd persistente que sobrevive reinicios.
T1068	**Escalación de Privilegios**	Exploitation for Privilege Escalation	La vulnerabilidad otorga directamente privilegios root; no se requiere escalación adicional.
T1070.002	**Evasión de Defensa**	Indicator Removal: Clear Linux or Mac System Logs	Borrado agresivo de logs del sistema (/var/log/*.log) cada 5 minutos mediante cron para destruir evidencia forense.
T1090.001	**Evasión de Defensa**	Proxy: Internal Proxy	Script Bash que configura HAProxy como relay HTTP para enmascarar el origen real del tráfico malicioso.
T1095	**Comando y Control**	Non-Application Layer Protocol	Comunicación C2 vía WebSocket con mensajes cifrados RC4 con claves aleatorias por mensaje.

ID Técnica	Táctica	Técnica / Sub-Técnica	Descripción en el Contexto del Ataque
T1219	**Comando y Control**	Remote Access Software	Uso de ScreenConnect para acceso remoto persistente y alternativo al FMC comprometido.
T1057	**Descubrimiento**	Process Discovery	El script de reconocimiento enumera procesos en ejecución, servicios y conexiones de red activas.
T1005	**Recopilación**	Data from Local System	Recopilación de artefactos de navegadores (historial, credenciales), configuraciones de red y datos del sistema.
T1560.001	**Recopilación**	Archive Collected Data: Archive vía Utility	Compresión de datos recopilados en archivos ZIP por hostname antes de la exfiltración.
T1486	**Impacto**	Data Encrypted for Impact	Cifrado de sistemas mediante ransomware Interlock/Slopoly para causar impacto operacional y extorsión.
T1567	**Exfiltración**	Exfiltration Over Web Service	Exfiltración de datos sensibles previo al cifrado para estrategia de doble extorsión.

Boletín informativo
Vulnerabilidad en Cisco Secure (FMC)

CSIRTSALUD-AV-20260319-37 **TLP: CLEAR**

Activos o versiones afectados:

Las siguientes versiones del software Cisco Secure Firewall Management Center (FMC) son vulnerables a CVE-2026-20131. Las organizaciones deben utilizar el Cisco Software Checker disponible en el portal de soporte de Cisco para determinar la primera versión con parche aplicable a su versión actual:

- Cisco Secure FMC 6.4.0
- Cisco Secure FMC 7.0.x
- Cisco Secure FMC 7.1.x
- Cisco Secure FMC 7.2.x
- Cisco Secure FMC 7.3.x
- Cisco Secure FMC 7.4.x
- Cisco Secure FMC 7.6.x
- Cisco Secure FMC 7.7.x
- Cisco Secure FMC 10.0.0

Nota importante sobre Cisco Security Cloud Control (SCC)

CVE-2026-20131 también afecta a Cisco Security Cloud Control (SCC) Firewall Management, la plataforma de gestión de políticas de seguridad basada en nube de Cisco. Cisco ha indicado que ha actualizado el servicio SCC como parte de su mantenimiento rutinario y que no se requiere ninguna acción por parte del usuario para los clientes de SCC.

Indicadores de compromiso:

Los siguientes indicadores de compromiso fueron identificados por el equipo de inteligencia de amenazas de Amazon (MadPot) durante la investigación activa de la campaña del ransomware Interlock. Su presencia en los registros o sistemas puede indicar un compromiso activo o pasado.

- **Indicadores de Red**

Peticiones HTTP sospechosas	Solicitudes POST a rutas específicas de la interfaz web del FMC con cuerpos que contienen bytes mágicos de serialización Java: 0xAC ED 00 05
Peticiones HTTP PUT anómalas	El dispositivo FMC realiza peticiones HTTP PUT salientes hacia servidores externos desconocidos para confirmar la explotación exitosa
Descarga de binario ELF	El FMC descarga y ejecuta un binario ELF (ejecutable Linux) desde un servidor remoto controlado por el atacante
Trafico WebSocket cifrado	comunicación C2 vía conexiones WebSocket persistentes con mensajes cifrados RC4 usando claves aleatorias de 16 bytes por mensaje
Proxies SOCKS5 anómalos	Trafico SOCKS5 que tuneliza comunicaciones TCP a través de sistemas comprometidos para ocultar el origen del ataque
Puertos de escucha	Los atacantes pueden exponer la interfaz en TCP/443 o TCP/8443; verificar conexiones salientes inesperadas desde el FMC

- **Indicadores de Host**

Binarios ELF maliciosos	Presencia de archivos ELF no reconocidos en el sistema de archivos del FMC, especialmente en directorios temporales o de ejecución

Implante JavaScript ofuscado	RAT en JavaScript que sobrescribe métodos de consola del navegador (console.log, console.error) para ocultar su actividad
Implante Java (GlassFish/Grizzly)	RAT en Java utilizando bibliotecas GlassFish/Grizzly para comunicación WebSocket con el servidor C2
Directorio de staging compartido	Presencia del share de red \\JK-DC2\Temp con subdirectorios por hostname con archivos ZIP comprimidos (artefactos de reconocimiento)
Borrado agresivo de logs	Truncamiento sistemático de archivos *.log en /var/log y supresión del historial de shell (HISTFILE no definido) via cron cada 5 minutos
ScreenConnect no autorizado	Instalaciones de ConnectWise ScreenConnect no reconocidas para persistencia de acceso remoto alternativo
Volatility Framework	Presencia del framework de forense de memoria Volatility en sistemas comprometidos
Script PowerShell de reconocimiento	Script PS1 que enumera OS, servicios, software, VMs Hyper-V, artefactos de navegadores (historial, credenciales), conexiones activas y tablas ARP

- **Indicadores de Ransomware Interlock**

Nota de rescate	Archivos de nota de rescate con el formato de extorsión característico de Interlock, citando regulaciones de protección de datos (GDPR, CCPA)

Boletín informativo
Vulnerabilidad en Cisco Secure (FMC)

CSIRTSALUD-AV-20260319-37 **TLP: CLEAR**

Portal TOR de negociación	Presencia de un identificador de organización único vinculado al portal de negociación .onion de Interlock
Malware Slopoly	Nueva cepa de malware creada por Interlock con asistencia de IA generativa, identificada por investigadores de IBM X-Force
NodeSnake RAT	Troyano de acceso remoto históricamente asociado con el grupo Interlock
Actividad UTC+3	Actividad concentrada entre las 08:30 y 18:00 UTC+3 (probablemente Europa del Este o Medio Oriente)

Recomendaciones de mitigación:

No existen workarounds ni mitigaciones alternativas para CVE-2026-20131 y CVE-2026-20079. La aplicación del parche de Cisco es la UNICA solución efectiva. Dado que Interlock explota activamente esta vulnerabilidad, las organizaciones deben tratar la aplicación del parche como una emergencia de seguridad con ventana de tiempo de 24-48 horas máximo.

Pasos para la remediación:

1. Acceder al Cisco Software Checker en: sec.cloudapps.cisco.com/security/center/softwarechecker.x para identificar la primera versión con parche aplicable a su versión de FMC.
2. Planificar una ventana de mantenimiento de emergencia
3. Descargar la imagen de software actualizada desde el portal oficial de Cisco (requiere contrato de soporte activo).
4. Realizar backup completo de la configuración del FMC antes de aplicar la actualización.
5. Aplicar la actualización de software siguiendo el procedimiento documentado de Cisco para actualizaciones de FMC.

6. Verificar la versión instalada post-actualización y validar el funcionamiento de todas las políticas de seguridad gestionadas.

Medidas de contención si el Parche No Es Inmediato

Si la aplicación inmediata del parche no es posible (por restricciones operacionales), implementar las siguientes medidas de contención de forma urgente:

- Aislar la interfaz de administración del FMC: implementar reglas de firewall o ACLs que restrinjan el acceso a la interfaz de administración web (puertos 443 y 8443) exclusivamente a direcciones IP de administración conocidas y confiables.
- Nunca exponer la interfaz de gestión a Internet: verificar que la interfaz web del FMC no tenga conectividad directa a Internet. Cisco explícitamente indica que la reducción de la exposición publica reduce la superficie de ataque.
- Implementar segmentación de red para la red de gestión: aislar el FMC en una VLAN o segmento de red dedicado con controles de acceso estrictos.

Fuentes:

- **The Hacker News - Google Fixes Two Chrome Zero-Days Exploited in the Wild Affecting Skia and V8 (Mar. 13, 2026)**

https://thehackernews.com/2026/03/google-fixes-two-chrome-zero-days.html

- **SOC Prime - CVE-2026-3910: Chrome V8 Zero-Day Used for In-the-Wild Attacks**

https://socprime.com/blog/cve-2026-3910-vulnerability/

- **CVE Reports - CVE-2026-3909: Remote Code Execution via Out-of-Bounds Write in Google Skia**

https://cvereports.com/reports/CVE-2026-3909

- **Purple-Ops - CVE-2026-3909 and CVE-2026-3910 Chrome Fixes (CVSS 8.8)**

https://www.purple-ops.io/resources-hottest-cves/cve-2026-3909-3910-chrome/

- **Qualys ThreatPROTECT - Google Patches Two Chrome Vulnerabilities Exploited in the Wild (Mar. 16, 2026)**

https://threatprotect.qualys.com/2026/03/16/google-patches-two-chrome-vulnerabilities-exploited-in-the-wild-cve-2026-3909-cve-2026-3910/

- **Vulert Blog - Google Chrome Zero-Days CVE-2026-3909 & CVE-2026-3910 (Análisis técnico Skia y V8)**

https://vulert.com/blog/google-chrome-zero-days-cve-2026-3909-2026-3910/

- **CISA - Catálogo de Vulnerabilidades Conocidas Explotadas (KEV)**

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **CISA - Alerta oficial: CISA Adds Two Known Exploited Vulnerabilities to Catalog (Mar. 2026)**

https://www.cisa.gov/news-events/alerts/2026/03/13/cisa-adds-two-known-exploited-vulnerabilities-catalog

- **MITRE ATT&CK Framework v18.1 (Marco de tácticas y técnicas adversariales)**

https://attack.mitre.org/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.