Alerta

Cisco Secure Firewall ASA y FTD – CVE-2026-20349

COLCERT AL – 20260819 - 113

TLP:CLEAR

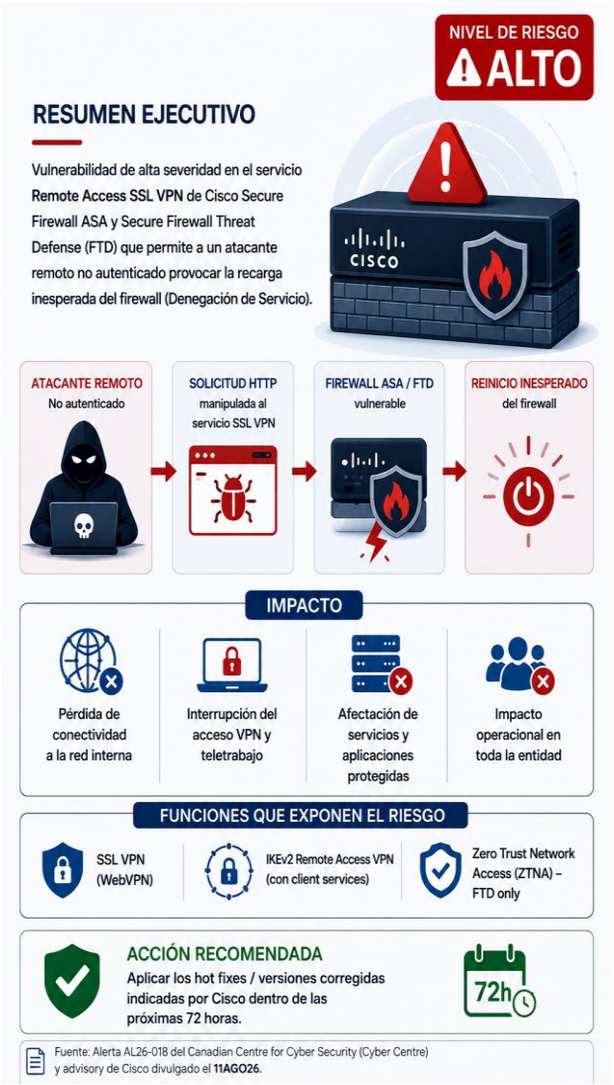
Resumen Ejecutivo

El ColCERT emite la presente alerta en respuesta a la reciente divulgación por parte de Cisco sobre una **vulnerabilidad de alta severidad** que afecta el servicio Remote Access SSL VPN en sus productos Secure Firewall ASA y Secure Firewall Threat Defense (FTD).

La gravedad de esta situación se acentúa dado que el fabricante ha confirmado su explotación activa en entornos reales, lo que motivó su inclusión inmediata en el catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA el mismo día de su publicación.

(Known Exploited Vulnerabilities Catalog | CISA)

Técnicamente, un atacante remoto y no autenticado puede enviar una única solicitud HTTP manipulada al portal VPN y provocar el reinicio inesperado del firewall, sin requerir ninguna interacción del usuario. Dado que este ataque es fácilmente repetible, puede sostenerse en el tiempo para mantener el equipo fuera de servicio. Consecuentemente, el impacto trasciende el dispositivo*, la caída del firewall perimetral interrumpe de forma simultánea el control de acceso a la red y los accesos de teletrabajo de toda la organización.* (Cabe destacar que el Cisco Secure Firewall Management Center - FMC - no se ve afectado).



Frente a este escenario, Cisco ha confirmado que no existen medidas de mitigación alternativas (workarounds) ni configuraciones compensatorias. La única remediación efectiva es la aplicación del hot fix correspondiente, el cual se distribuye a través del Software Center y no se soluciona mediante una actualización ordinaria del tren de versiones.

En virtud de lo anterior, la evaluación SSVC del ColCERT determina la decisión de actuar.

Se insta a las entidades a inventariar de manera urgente sus equipos ASA y FTD expuestos a Internet, verificar las versiones y las funciones VPN habilitadas, y aplicar el hot fix en un plazo no mayor a 72 horas.

Fecha de la vulnerabilidad

Atributo	Valor
Identificador	CVE-2026-20349
Advisory del fabricante	cisco-sa-asaftd-vpn-dos-dzv4mQFF (Bug ID CSCwv96220)
Debilidad	CWE-244 — Improper Clearing of Heap Memory Before Release
CVSS v3.1	8.6 (Alta) — AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Causa raíz	Verificación insuficiente de errores al procesar solicitudes HTTP
Vector de ataque	Solicitud HTTP manipulada al servicio Remote Access SSL VPN
Privilegios requeridos	Ninguno — atacante no autenticado
Interacción del usuario	Ninguna
Impacto	Recarga inesperada del dispositivo — denegación de servicio
Workaround	No existe
Explotación en entornos reales	Confirmada por Cisco PSIRT (agosto de 2026)
Exploit público	No identificado a la fecha de este boletín
Producto no afectado	Cisco Secure Firewall Management Center (FMC)
Técnica ATT&CK	T1499.004 — Endpoint Denial of Service: Application or System Exploitation

Lectura correcta de la severidad

Es fundamental precisar la naturaleza del impacto de esta amenaza, no se trata de una vulnerabilidad de ejecución remota de código (RCE). No existe exposición de datos, exfiltración de información sensible ni evidencia de que el atacante pueda tomar el control administrativo del equipo.

De acuerdo con el vector CVSS, el impacto sobre la Confidencialidad y la Integridad de la información es nulo (C:N / I:N). La calificación de alta severidad (8.6) está fundamentada de forma exclusiva en la afectación a la Disponibilidad (A:H) y en el componente de Alcance Modificado (S:C).

El riesgo crítico radica en el efecto cascada: al provocarse el reinicio inesperado del firewall, la interrupción no se limita al dispositivo en sí, sino que arrastra consigo la conectividad, el control de acceso y los servicios de todos los sistemas internos que este protege.

Observación de riesgo del ColCERT

A pesar de la calificación del vector CVSS expuesta anteriormente, el ColCERT advierte que esta amenaza no debe subestimarse, ni tratarse como "solamente una denegación de servicio".

Es importante considerar que la debilidad asignada por el fabricante (CWE-244) corresponde, según la definición de MITRE, a una categoría de exposición de información en la memoria dinámica, no a un simple fallo de disponibilidad. El defecto de fondo radica en un problema de gestión de memoria *heap,* el cual es alcanzable sin ningún tipo de autenticación a través del motor HTTP del portal VPN.

Históricamente, las primitivas de corrupción de *heap* remotas y no autenticadas que afectan este componente han demostrado la capacidad de escalar hacia escenarios de mayor criticidad. Por consiguiente, el ColCERT emite una recomendación enfática: las entidades deben priorizar la remediación de este fallo al mismo nivel de urgencia y criticidad que una vulnerabilidad de Ejecución Remota de Código (RCE) en un dispositivo perimetral.

Alcance de la afectación

Esta vulnerabilidad impacta a toda entidad que opere dispositivos Cisco Secure Firewall ASA o FTD en las versiones comprometidas, siempre y cuando mantengan habilitada al menos una de las funciones que generan sockets SSL en estado de escucha.

Es importante subrayar que este riesgo se maximiza de forma crítica cuando el portal VPN se encuentra expuesto directamente hacia Internet, condición que, por la naturaleza del servicio de acceso remoto, corresponde a su modo de despliegue y operación habitual.

Configuraciones vulnerables

Un dispositivo se considera vulnerable única y exclusivamente si cumple con dos condiciones simultáneas: ejecutar una de las versiones de software afectadas y tener habilitada, al menos, una de las siguientes funcionalidades:

Función	Configuración en show running-config
IKEv2 Remote Access VPN (con client services)	crypto ikev2 enable <interface> client-services port <puertos>
SSL VPN (WebVPN)	webvpn → enable <interface>
Zero Trust Network Access (solo FTD)	zero-trust → enable

Prioridad asignada y evaluación SSVC

Tras el análisis de la amenaza, la evaluación SSVC (Stakeholder-Specific Vulnerability Categorization) realizada por el ColCERT determina la decisión de Actuar (Act).

Esta máxima prioridad se fundamenta técnica y operativamente en tres factores críticos:

- Explotación activa confirmada en entornos reales.
- Exposición inherente a Internet, dictada por el diseño y propósito del servicio VPN.
- Alta facilidad de explotación, la cual es completamente automatizable mediante el envío de una única solicitud HTTP manipulada.

La criticidad y urgencia de este escenario se ven respaldadas por la rápida acción de CISA, que incorporó esta vulnerabilidad a su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV) el mismo día de su divulgación oficial.

Sin solución alternativa (Workarounds)

Cisco ha confirmado oficialmente que **no existen configuraciones compensatorias ni workarounds** para mitigar esta vulnerabilidad. La única remediación técnica y verdaderamente efectiva es la aplicación inmediata del hot fix correspondiente.

Si bien las entidades pueden contemplar medidas restrictivas de manera temporal, es fundamental comprender sus limitaciones críticas y sus impactos operativos:

- **Restricción por lista de control de acceso (ACLs):** Limitar el acceso al portal VPN mediante listas de direcciones IP de origen reduce significativamente la superficie de ataque. Sin embargo, esta medida no protege al dispositivo frente a un atacante que logre alcanzar el servicio (por ejemplo, desde un origen permitido o suplantado).
- **Deshabilitación temporal de la VPN:** Apagar el servicio elimina por completo la exposición a la vulnerabilidad, pero interrumpe los canales de acceso remoto y teletrabajo de la organización.

Dado que la suspensión de la VPN afecta directamente la operatividad, el ColCERT enfatiza que esta es una decisión de continuidad del negocio. Como tal, cualquier acción encaminada a deshabilitar el acceso remoto debe escalarse de inmediato al comité directivo o de crisis correspondiente y quedar debidamente documentada.

Paso 1 — Determine si está afectado

Ejecute en el dispositivo:

```
show version | include Version
show running-config webvpn
show running-config crypto ikev2
show running-config zero-trust        ! solo FTD
show asp table socket | include SSL
```

Si el dispositivo ejecuta una versión perteneciente a un tren de software afectado y presenta alguno de los servicios previamente mencionados habilitado sobre una interfaz accesible desde Internet, el equipo se considera vulnerable. En este escenario, se reitera que no existe mitigación técnica posible distinta a la aplicación del *hot fix.*

Para garantizar la precisión de este diagnóstico y descartar falsos negativos, se recomienda complementar la verificación manual utilizando la herramienta oficial Cisco Software Checker.

Paso 2 — Aplicación el hot fix correspondiente

Cisco ha publicado estas correcciones de seguridad exclusivamente en formato de hot fix, los cuales deben descargarse de manera directa desde el Software Center.

Dado que no han sido liberados como versiones de disponibilidad general (GA - General Availability), esta vulnerabilidad no se soluciona mediante una actualización ordinaria del tren de versiones. Se requiere la instalación específica del *hot fix* provisto por el fabricante para la versión que su equipo esté ejecutando.

Producto	Tren afectado	Hot fix
Cisco Secure Firewall ASA	9.16.x	89.16.4.50
Cisco Secure Firewall ASA	9.18.x	89.18.4.50
Cisco Secure Firewall ASA	9.20.x	9.20.4.235
Cisco Secure Firewall ASA	9.22.x	9.22.3.191
Cisco Secure Firewall ASA	9.23.x	9.23.1.211
Cisco Secure Firewall ASA	9.24.x	9.24.1.221
Cisco Secure Firewall FTD	7.0.x	Cisco_FTD_Hotfix_GC-7.0.9.1-1
Cisco Secure Firewall FTD	7.2.x	Cisco_FTD_Hotfix_HM-7.2.11.1-2
Cisco Secure Firewall FTD	7.4.x	Cisco_FTD_Hotfix_HK-7.4.7.1-1
Cisco Secure Firewall FTD	7.6.x	Cisco_FTD_Hotfix_DD-7.6.4.1-2
Cisco Secure Firewall FTD	7.7.x	Cisco_FTD_Hotfix_AN-7.7.11.1-2
Cisco Secure Firewall FTD	10.0.x	Cisco_FTD_Hotfix_S-10.0.0.1-2

Nota: los hot fixes de ASA 9.16 y 9.18 comienzan por 89. No es un error tipográfico.

Cisco advierte que, al aplicar un *hot fix* cuya nomenclatura inicie con "89", es necesario instalar simultáneamente ASDM 7.24.1.374, dado que las versiones anteriores no reconocen este formato de numeración y ocasionarán la pérdida de acceso a la consola de administración.

Para entornos FTD, cada tren de software publica variantes específicas según la plataforma física (SSP, FP1K, FP2K, FP3K, Secure Firewall 1200/4200/6100). Asegúrese de descargar e implementar la variante exacta que corresponda a su hardware, omitiendo estrictamente el uso de paquetes genéricos.

Paso 3 – Busqueda de señales de explotación

Dado que el fabricante no ha emitido indicadores de compromiso (IoCs) atómicos, tales como hashes, direcciones IP o dominios asociados, las labores de detección deben enfocarse estrictamente en el análisis conductual del dispositivo:

- **Recargas inesperadas:** Monitoree cualquier reinicio del ASA/FTD que ocurra sin cambios de configuración previos o fallas de energía documentadas. Verifique el motivo del último reload y examine detalladamente el archivo crashinfo.
- **Reinicios repetidos:** La ocurrencia de reinicios repetidos o en bucle sobre el mismo equipo sugiere un patrón de ataque sostenido, descartando fallas fortuitas de hardware.
- **Caida masiva de sesiones:** Identifique en el syslog del dispositivo cualquier evento que evidencie la desconexión masiva y simultánea de sesiones VPN.
- **Tráfico HTTP anómalo:** Analice picos inusuales de solicitudes HTTP, especialmente si están malformadas, dirigidas al puerto 443 de la interfaz externa y provenientes de un número reducido de orígenes.

Preservar una copia del archivo crashinfo antes de efectuar cualquier reinicio manual o actualización. Esta es la única evidencia forense que documenta el evento y se sobrescribirá irreversiblemente durante el procedimiento.

Recomendaciones del ColCERT

Fase inmediata 0 – 24 horas

- Inventariar de manera exhaustiva todos los dispositivos Cisco ASA y FTD de la entidad, identificando puntualmente aquellos que exponen el portal SSL VPN hacia Internet.
- Verificar las versiones en ejecución y las funciones VPN habilitadas (conforme a los criterios de diagnóstico previamente detallados).
- Programar de forma urgente la ventana de mantenimiento para la aplicación del *hot fix*, contemplando obligatoriamente el tiempo de reinicio del equipo dentro de la planeación operativa.

Fase de ejecución y análisis 24 – 72 horas

- Aplicar el *hot fix* priorizando de manera estricta a los dispositivos expuestos a Internet por encima de los de uso interno.
- Revisar de forma retroactiva los registros (logs) de los últimos 30 días en busca de reinicios inexplicables, asegurando la preservación del archivo crashinfo ante cualquier hallazgo anómalo.
- Reportar de inmediato al ColCERT cualquier evidencia de explotación detectada. Es vital subrayar que un hallazgo positivo se gestionará formalmente como un incidente de seguridad, trascendiendo el proceso de gestión de vulnerabilidades.

Recomendaciones del ColCERT – Acciones de seguimiento y mejora continua

Validar la activación de las reglas Snort 46897 y 59654 en entornos que operen con Snort o FirePOWER. Tenga en cuenta que estas actúan como un control compensatorio parcial y, en ningún caso, sustituyen la aplicación del *hot fix.*

Incorporar de manera permanente los dispositivos perimetrales y concentradores VPN al alcance del programa de gestión de vulnerabilidades de la entidad, dado que históricamente representan el punto ciego más frecuente en las auditorías de infraestructura.

Monitorear constantemente las actualizaciones del advisory oficial de Cisco y mantenerse alerta ante la eventual publicación de un exploit de prueba de concepto (PoC) público, factor que acortaría drásticamente la ventana de riesgo actual.

Referencias

- Cisco PSIRT — advisory cisco-sa-asaftd-vpn-dos-dzv4mQFF (sec.cloudapps.cisco.com/security/center/publicationListing.x)
- Canadian Centre for Cyber Security — Alerta AL26-018, 13 de agosto de 2026.
- CISA — Known Exploited Vulnerabilities Catalog, adición del 11 de agosto de 2026.
- MITRE — CVE-2026-20349 y CWE-244.
- Cisco Software Checker — sec.cloudapps.cisco.com/security/center/softwarechecker.

Vigencia y revisión

La presente alerta mantiene su vigencia y será objeto de actualización inmediata en caso de presentarse alguno de los siguientes escenarios: la publicación de un exploit funcional en fuentes abiertas, la emisión de revisiones críticas al advisory de Cisco, o la identificación de actividad de explotación dirigida específicamente contra entidades del Estado colombiano.

Se aclara que este documento es específico y no sustituye ni invalida el boletín de seguimiento BS-2026-0019 (referente a las vulnerabilidades en equipos SonicWall, Fortinet y Rapid7, reportadas en el mismo ciclo semanal del CCCS). Dichas vulnerabilidades continúan su respectivo trámite y monitoreo por separado bajo la clasificación SSVC Track.

Fuentes

Canadian Centre for Cyber Security (Cyber Centre) — Alert AL26-018: Vulnerability affecting Cisco ASA and Secure Firewall Threat Defense Software Remote Access SSL VPN – CVE-2026-20349, 13 de agosto de 2026.

Cisco Security Advisory — Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability. Referenciado en la alerta canadiense.

CVE.org — CVE-2026-20349.MITRE CWE — CWE-244: Improper Clearing of Heap Memory Before Release (“Heap Inspection”).