La Cybersecurity and Infrastructure Security Agency (CISA) de Estados Unidos ha informado que un organismo civil federal —no identificado— sufrió la intrusión de un dispositivo Cisco Firepower que ejecutaba el software Adaptive Security Appliance (ASA) en septiembre de 2025, mediante un malware denominado FIRESTARTER.

FIRESTARTER, según la CISA y el National Cyber Security Centre (NCSC) del Reino Unido, se considera una puerta trasera diseñada para acceso y control remoto. Se estima que forma parte de una campaña "a gran escala" llevada a cabo por un actor de amenaza persistente avanzada (APT), cuyo objetivo era infiltrarse en el firmware de Cisco Adaptive Security Appliance (ASA) explotando vulnerabilidades de seguridad ya corregidas, tales como:

- CVE-2025-20333 (puntuación CVSS: 9.9) – Una falla de validación incorrecta de entradas proporcionadas por el usuario que podría permitir que un atacante remoto autenticado, con credenciales válidas de VPN, ejecute código arbitrario como root en un dispositivo afectado mediante solicitudes HTTP manipuladas.
- CVE-2025-20362 (puntuación CVSS: 6.5) – Otra vulnerabilidad de validación deficiente que posibilita a un atacante remoto no autenticado acceder a endpoints URL restringidos sin autenticación, también mediante solicitudes HTTP diseñadas.

"FIRESTARTER puede mantenerse como una amenaza activa en dispositivos Cisco que ejecutan ASA o Firepower Threat Defense (FTD), conservando persistencia incluso después de aplicar parches y permitiendo a los atacantes volver a acceder sin necesidad de explotar nuevamente las vulnerabilidades", indicaron las agencias.

En el incidente analizado, se detectó que los atacantes desplegaron una herramienta posterior a la explotación llamada LINE VIPER, capaz de ejecutar comandos CLI, capturar paquetes de red, eludir los mecanismos de autenticación, autorización y contabilidad (AAA) de VPN, suprimir registros syslog, recolectar comandos de usuarios y forzar reinicios retrasados.

El acceso privilegiado que proporciona LINE VIPER facilitó la implementación de FIRESTARTER, instalado en el dispositivo Firepower antes del 25 de septiembre de 2025, lo

que permitió a los atacantes mantener acceso continuo y regresar al sistema comprometido incluso el mes pasado.

Como binario ELF de Linux, FIRESTARTER puede establecer persistencia en el dispositivo y sobrevivir a actualizaciones de firmware y reinicios, salvo que se realice un apagado completo de energía. El malware se integra en la secuencia de arranque del sistema modificando una lista de montaje inicial, asegurando su reactivación automática tras cada reinicio normal. Además de su resistencia, presenta similitudes parciales con un bootkit previamente documentado conocido como RayInitiator.

"FIRESTARTER intenta instalar un 'hook' —un mecanismo para interceptar y modificar operaciones normales— dentro de LINA, el motor principal del dispositivo para el procesamiento de red y funciones de seguridad", detalla el aviso. *"Este 'hook' permite ejecutar código de shell arbitrario proporcionado por los actores APT, incluida la implementación de LINE VIPER."*

"Aunque los parches de Cisco solucionaron CVE-2025-20333 y CVE-2025-20362, los dispositivos comprometidos antes de la actualización pueden seguir siendo vulnerables, ya que FIRESTARTER no se elimina con actualizaciones de firmware."

Cisco, que rastrea esta actividad bajo el nombre UAT4356 (también conocido como Storm-1849), describe FIRESTARTER como una puerta trasera que permite ejecutar shellcode arbitrario recibido por el proceso LINA mediante el análisis de solicitudes de autenticación WebVPN especialmente diseñadas que contienen un "paquete mágico".

El origen exacto de esta actividad maliciosa sigue sin confirmarse, aunque un análisis de la plataforma Censys en mayo de 2024 sugirió posibles vínculos con China. UAT4356 se asoció inicialmente con una campaña llamada ArcaneDoor, que explotó dos vulnerabilidades de día cero en equipos de red Cisco para desplegar malware personalizado capaz de interceptar tráfico y realizar reconocimiento.

"Para eliminar completamente el mecanismo de persistencia, Cisco recomienda

encarecidamente reinstalar la imagen del sistema y actualizar el dispositivo", señaló la compañía. *"En casos confirmados de compromiso en plataformas Cisco Secure ASA o FTD, todos los elementos de configuración deben considerarse no confiables."*

Como medida temporal hasta realizar la reinstalación, la empresa aconseja efectuar un reinicio en frío para eliminar el implante FIRESTARTER. *"Los comandos CLI de apagado, reinicio o recarga no eliminarán el implante persistente; es necesario desconectar el cable de alimentación y volver a conectarlo"*, añadió.

Hackers chinos cambian de infraestructuras individuales a redes encubiertas

Esta revelación coincide con un aviso conjunto emitido por Estados Unidos, Reino Unido y otros socios internacionales sobre redes a gran escala formadas por routers SOHO y dispositivos IoT comprometidos, controlados por actores vinculados a China para ocultar sus actividades de espionaje y dificultar su atribución.

Grupos patrocinados por el Estado como Volt Typhoon y Flax Typhoon han utilizado estas botnets —compuestas por routers domésticos, cámaras de seguridad, grabadores de video y otros dispositivos IoT— para atacar infraestructuras críticas y realizar espionaje cibernético de forma *"económica, de bajo riesgo y difícil de atribuir"*, según la alerta.

La situación se complica porque estas redes se actualizan constantemente y, además, varios grupos vinculados a China pueden emplear la misma botnet simultáneamente, lo que dificulta su detección y bloqueo mediante listas estáticas de direcciones IP.

"Las redes encubiertas están formadas principalmente por routers SOHO comprometidos, pero también integran cualquier dispositivo vulnerable que pueda explotarse a gran escala", indicaron las agencias. *"El tráfico se redirige a través de múltiples dispositivos comprometidos que actúan como nodos intermedios antes de salir por un nodo final, generalmente ubicado en la misma región geográfica que el objetivo."*

Estos hallazgos reflejan un patrón habitual en ataques patrocinados por Estados: el enfoque en dispositivos perimetrales de redes residenciales, empresariales y gubernamentales, con el objetivo de convertirlos en nodos proxy o interceptar información y comunicaciones sensibles.