Investigadores en ciberseguridad han revelado detalles sobre una grave vulnerabilidad recientemente corregida en WatchGuard Fireware, la cual podría permitir a atacantes no autenticados ejecutar código arbitrario.

La falla, identificada como *CVE-2025-9242* (con una puntuación CVSS de 9.3), ha sido clasificada como una vulnerabilidad de escritura fuera de límites que afecta al sistema operativo Fireware OS desde la versión 11.10.2 hasta la 11.12.4_Update1, y desde la 12.0 hasta la 12.11.3, incluyendo la versión 2025.1.

"Una vulnerabilidad de escritura fuera de límites en el proceso iked del sistema WatchGuard Fireware OS puede permitir que un atacante remoto no autenticado ejecute código arbitrario," señaló WatchGuard en una advertencia publicada el mes pasado. *"Esta falla afecta tanto a usuarios de VPN móvil con IKEv2 como a las VPN de sucursal que usan IKEv2 cuando se configuran con un par de puerta de enlace dinámica."*

La vulnerabilidad ha sido corregida en las siguientes versiones:

- 2025.1 → *Corregida en 2025.1.1*
- 12.x → *Corregida en 12.11.4*
- 12.3.1 (versión con certificación FIPS) → *Corregida en 12.3.1_Update3 (B722811)*
- 12.5.x (modelos T15 y T35) → *Corregida en 12.5.13*
- 11.x → *Fin de vida útil (no recibirá correcciones)*

Un nuevo análisis del equipo de *watchTowr Labs* describió a *CVE-2025-9242* como una vulnerabilidad que *"tiene todas las características que encantan a los grupos de ransomware de tu vecindario,"* destacando que afecta un servicio expuesto a Internet, es explotable sin autenticación y permite la ejecución de código en dispositivos perimetrales.

De acuerdo con el investigador en seguridad *McCaulay Hudson*, el origen de la vulnerabilidad se encuentra en la función *«ike2_ProcessPayload_CERT»*, ubicada en el archivo *«src/ike/iked/v2/ike2_payload_cert.c»*. Esta función está diseñada para copiar una "identificación" del cliente en un búfer local de 520 bytes en la pila, y luego validar el

certificado SSL proporcionado por el cliente.

El problema surge debido a la ausencia de una verificación del tamaño del búfer de identificación, lo que permite a un atacante provocar un desbordamiento y ejecutar código de forma remota durante la fase *IKE_SA_AUTH* del proceso de autenticación utilizado para establecer un túnel VPN entre el cliente y el servicio VPN de WatchGuard a través del protocolo de gestión de claves IKE.

"El servidor sí realiza la validación del certificado, pero esta ocurre después de que se ejecuta el código vulnerable, permitiendo que dicho código sea alcanzado antes de la autenticación," explicó Hudson.

El equipo de *watchTowr* también señaló que, aunque Fireware OS no dispone de un shell interactivo como */bin/bash*, un atacante puede explotar esta falla para tomar control del registro de instrucciones (RIP o program counter) y lanzar un shell interactivo en Python a través de TCP. Esto se logra mediante el uso de una llamada al sistema *mprotect()*, lo cual permite eludir las protecciones del bit NX (*no-ejecutar*).

Una vez obtenido el shell remoto en Python, es posible escalar el acceso hasta obtener un shell completo de Linux mediante los siguientes pasos:

- Ejecutar directamente *execve* dentro de Python para volver a montar el sistema de archivos como lectura/escritura
- Descargar un binario de *BusyBox* en el dispositivo comprometido
- Crear un enlace simbólico de */bin/sh* apuntando al binario de *BusyBox*

Este desarrollo se produce al mismo tiempo que *watchTowr* demostró que una vulnerabilidad previamente solucionada de denegación de servicio (DoS) en *Progress Telerik UI for AJAX* (identificada como *CVE-2025-3600*, con puntuación CVSS de 7.5) también puede permitir ejecución remota de código, dependiendo del entorno afectado. Dicha vulnerabilidad fue corregida por *Progress Software* el 30 de abril de 2025.

"Dependiendo de la base de código objetivo —por ejemplo, la presencia de constructores sin argumentos, finalizadores o resolutores de ensamblados inseguros— el impacto puede escalar a una ejecución remota de código," indicó el investigador *Piotr Bazydlo*.

A inicios de este mes, *Sina Kheirkhah* de *watchTowr* también dio a conocer una grave vulnerabilidad de inyección de comandos, sin necesidad de autenticación previa, en *Dell UnityVSA* (*CVE-2025-36604*, CVSS 9.8/7.3), que podría resultar en ejecución remota de comandos. Dell resolvió la vulnerabilidad en julio de 2025 tras su divulgación responsable el 28 de marzo.