Los investigadores en ciberseguridad han revelado un conjunto de fallos que afectan a los clientes de redes privadas virtuales (VPN) de Palo Alto Networks y SonicWall. Estas vulnerabilidades podrían ser explotadas para ejecutar código de manera remota en sistemas Windows y macOS.

> *«Al aprovechar la confianza implícita que los clientes VPN depositan en los servidores, los atacantes pueden manipular el comportamiento del cliente, ejecutar comandos arbitrarios y obtener altos niveles de acceso con un esfuerzo mínimo»*, explicó AmberWolf en un análisis.

En un escenario de ataque hipotético, esto podría materializarse mediante un servidor VPN malicioso que engañe a los clientes para descargar actualizaciones maliciosas con consecuencias no deseadas.

El resultado de la investigación es una herramienta de prueba de concepto (PoC) llamada NachoVPN, que puede simular tales servidores VPN y explotar las vulnerabilidades para ejecutar código con privilegios elevados.

Las vulnerabilidades identificadas son las siguientes:

- CVE-2024-5921 (puntuación CVSS: 5.6): Una vulnerabilidad de validación insuficiente de certificados que afecta a Palo Alto Networks GlobalProtect en Windows, macOS y Linux, permitiendo que la aplicación se conecte a servidores arbitrarios y facilite la instalación de software malicioso. (Corregido en la versión 6.2.6 para Windows).
- CVE-2024-29014 (puntuación CVSS: 7.1): Una vulnerabilidad que afecta al cliente SonicWall SMA100 NetExtender para Windows, permitiendo a un atacante ejecutar código arbitrario al procesar una actualización del cliente End Point Control (EPC). (Afecta a versiones 10.2.339 y anteriores, corregido en la versión 10.2.341).

Palo Alto Networks subraya que el atacante necesitaría acceso como usuario local no administrativo en el sistema operativo o estar en la misma subred para instalar certificados

raíz maliciosos en el endpoint y software firmado con esos certificados.

Plugin	Product	CVE	Windows RCE	macOS RCE	Privileged	URI Handler	Packet Capture
Cisco	Cisco AnyConnect	N/A	✅	✅	❌	❌	✅
SonicWall	SonicWall NetExtender	CVE-2024-29014	✅	❌	✅	✅	❌
PaloAlto	Palo Alto GlobalProtect	CVE-2024-5921 (partial fix)	✅	✅	✅	❌	✅
PulseSecure	Ivanti Connect Secure	N/A	✅	✅	❌	✅ (Windows only)	✅

Con esto, la aplicación GlobalProtect podría ser utilizada para robar credenciales VPN de la víctima, ejecutar código arbitrario con privilegios elevados e instalar certificados raíz maliciosos que faciliten otros ataques.

De manera similar, un atacante podría engañar a un usuario para conectar su cliente NetExtender a un servidor VPN malicioso y entregar una actualización falsa del cliente EPC, firmada con un certificado válido pero robado, logrando finalmente ejecutar código con privilegios de SYSTEM.

> *«Los atacantes pueden explotar un manejador URI personalizado para forzar que el cliente NetExtender se conecte a su servidor. Los usuarios solo necesitan visitar un*

> *sitio web malicioso y aceptar un aviso del navegador, o abrir un documento malicioso para que el ataque tenga éxito»,* mencionó AmberWolf.

Aunque no hay evidencia de que estas vulnerabilidades hayan sido explotadas en ataques reales, se recomienda a los usuarios de Palo Alto Networks GlobalProtect y SonicWall NetExtender que apliquen los parches más recientes para protegerse contra posibles amenazas.

Este desarrollo ocurre mientras los investigadores de Bishop Fox detallaron su enfoque para descifrar y analizar el firmware integrado en los cortafuegos SonicWall. Esto tiene como objetivo mejorar la investigación de vulnerabilidades y desarrollar capacidades de identificación para evaluar el estado actual de seguridad de los cortafuegos SonicWall expuestos a internet.