Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ELEVACIÓN DE PRIVILEGIOS EN EL CLIENTE DE WINDOWS DE NETSKOPE A TRAVÉS DE UN SERVIDOR MALICIOSO

01/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

Investigadores de seguridad han identificado una vulnerabilidad en el cliente de Windows de Netskope, asignada como CVE-2025-5942 . Esta falla afecta al controlador epdlpdrv.sys cuando el módulo Endpoint DLP (Data Loss Prevention) está habilitado.

ELEVACIÓN DE PRIVILEGIOS EN EL CLIENTE DE WINDOWS DE NETSKOPE A TRAVÉS DE UN SERVIDOR MALICIOSO

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_01_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	01/09/2025
Es día cero (0 day):	No

RESUMEN

Investigadores de seguridad han identificado una vulnerabilidad en el cliente de Windows de Netskope, asignada como CVE-2025-5942 . Esta falla afecta al controlador epdlpdrv.sys cuando el módulo Endpoint DLP (Data Loss Prevention) está habilitado.

La vulnerabilidad puede ser explotada por un usuario sin privilegios para provocar un desbordamiento de montón, lo que genera un bloqueo completo del sistema (BSOD) y deja la máquina fuera de servicio. Aunque Netskope clasificó la vulnerabilidad con una severidad media (CVSS 5.7), el riesgo aumenta en entornos corporativos donde la estabilidad del cliente es crítica.

¿Cómo funciona la vulnerabilidad?

El fallo se encuentra en el manejo inadecuado de la memoria dentro del controlador epdlpdrv.sys.

- Un usuario local sin privilegios puede enviar solicitudes manipuladas que generan un desbordamiento en el montón.
- Esto provoca una corrupción de memoria en el proceso del conductor, lo que finalmente causa una pantalla azul de la muerte (BSOD).
- El resultado es una denegación de servicio local con impacto directo en la disponibilidad del sistema.

Aunque no se ha demostrado que pueda usarse para ejecutar código arbitrario, la explotación podría servir como un vector inicial en ataques internos, interrumpiendo servicios críticos o facilitando movimientos posteriores.

Versiones afectadas

- Todas las versiones del cliente Netskope para Windows anteriores a R129.
- Netskope ya ha liberado la versión R129 y también la R126.0.9 (un hotfix retrocompatible) para entornos que no puedan migrar de inmediato.

Impacto real en las organizaciones

- Usuarios internos maliciosos: Empleados o contratistas con acceso físico podrían explotar la falla para sabotear sistemas.
- Riesgo de interrupción operativa: Un BSOD masivo en equipos con Netskope activo puede afectar la productividad, la disponibilidad de datos y las operaciones críticas.
- Afectación a la reputación: Las caídas de servicios de seguridad internos pueden generar dudas en clientes y auditores sobre la madurez de la empresa en la gestión de parches.

RECOMENDACIONES

- Actualiza inmediatamente a Netskope Client R129 o aplica la R126.0.9 si no es posible migrar.
- Monitorea los eventos del sistema: Revisa los logs de Windows y las alertas relacionadas con fallos del driver epdlpdrv.sys.
- Realiza pruebas controladas: Valida la actualización en un entorno de prueba (staging) antes de implementarla masivamente en toda la organización.

NOTICIA COMPLETA

https://devel.group/blog/elevacion-de-privilegios-en-el-cliente-de-windows-de-netskope-a-traves-de-un-servidor-malicioso/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group