Boletín de alerta

Boletín Nro.: 93
Fecha de publicación: 29/10/2025
Tema: Alerta 2025-93: Vulnerabilidad crítica en OpenVPN
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **OpenVPN**, versión de 2.7_alpha1 a 2.7_beta1.

Descripción

Se ha reportado una vulnerabilidad de alta gravedad, identificada como CVE-2025-10680 con un CVSS 8.8 (alta), que afecta a las versiones de OpenVPN. Esta falla expone los sistemas tipo Unix a ataques de inyección de scripts al conectarse a servidores VPN no confiables, lo que podría permitir la ejecución remota de código en el lado del cliente.

Según el anuncio de la comunidad de OpenVPN, los argumentos **–dns** y **–dhcp-option** introducidos no se sanean correctamente cuando se pasan al hook del script **–dns-updown**, lo que les permite inyectar comandos adicionales que se ejecutan en el cliente.

El problema surge cuando un cliente OpenVPN se conecta a un servidor VPN comprometido o malicioso capaz de enviar opciones de configuración de DNS o DHCP durante el inicio de sesión. El manejo incorrecto de estas opciones permite al atacante crear argumentos con un formato especial que inyectan comandos de shell adicionales en el sistema que ejecuta el gancho de actualización de DNS.

Solución:

El equipo de OpenVPN actuó rápidamente para resolver el problema en OpenVPN 2.7_beta2, lanzado con un parche que introduce una limpieza de entrada adecuada para las cadenas DNS.

https://www.mail-archive.com/openvpn-announce@lists.sourceforge.net/msg00149.html

Información adicional:

- https://community.openvpn.net/Security%20Announcements/CVE-2025-10680
- https://www.mail-archive.com/openvpn-announce@lists.sourceforge.net/msg00149.html

- https://securityonline.info/high-severity-openvpn-flaw-cve-2025-10680-allows-script-injection-on-linux-macos-via-malicious-dns-server/