Alerta de seguridad cibernética	9VSA20-00210-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2020
Última revisión	11 de mayo de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de múltiples fuentes referente a vulnerabilidad que afecta a OpenVPN. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-11810

CVE-2020-11810

Es posible detener el tráfico de una conexión VPN mediante un ataque DoS en OpenVPN.
Un atacante podría inyectar un paquete "P_DATA_V2" utilizando la ID de par de una víctima. Normalmente estos paquetes se descartan, pero si este paquete llega antes que los parámetros criptográficos del canal de datos, causará una denegación de servicio en la conexión de la víctima.
Para una explotación exitosa de esta vulnerabilidad, se requiere enviar este paquete justo después de que la víctima comience la conexión, y el servidor envíe la respuesta "PUSH_REPLY", teniendo tan solo unos segundos para realizar el ataque. Este ataque solo es efectivo si se utiliza NCP (Negotiable Cipher Parameters).

Mitigación

Producto Afectado
OpenVPN versión 2.4.x.

Mitigación
Actualizar a la versión 2.4.9 de OpenVPN.

Enlaces
https://security-tracker.debian.org/tracker/CVE-2020-11810
https://github.com/OpenVPN/openvpn/commit/37bc691e7d26ea4eb61a8a434ebd7a9ae76225ab
https://community.openvpn.net/openvpn/ticket/1272
https://bugzilla.suse.com/show_bug.cgi?id=1169925
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11810