Un equipo de investigadores de seguridad cibernética reveló una nueva vulnerabilidad grave que afecta a la mayoría de los sistemas operativos similares a Linux y Unix, incluyendo FreeBSD, OpenBSD, MacOS, iOS y Android, que podría permitir que los *«atacantes adyacentes de red»* remotos espíen y manipulen la VPN encriptada.

La vulnerabilidad, rastreada como CVE-2019-14899, reside en la pila de redes de varios sistemas operativos y puede explotarse tanto en flujos TCP IPv4 como IPv6.

Debido a que la vulnerabilidad no depende de la tecnología VPN utilizada, el ataque funciona contra protocolos de red privada virtual ampliamente implementados como OpenVPN, WireGuard, IKEv2/IPSec y más, según confirmaron los investigadores.

Esta vulnerabilidad puede ser explotada por un atacante de la red, controlando un punto de acceso o conectado a la red de la víctima, simplemente al enviar paquetes de red no solicitados a un dispositivo objetivo y observando respuestas, incluso si están encriptados.

Según los investigadores, aunque existen variaciones para cada uno de los sistemas operativos afectados, la vulnerabilidad permite a los atacantes:

- Determinar la dirección IP virtual de una víctima asignada por el servidor VPN
- Determinar si existe una conexión activa en un sitio web determinado
- Determinar los números exactos de seq y ack contando los paquetes cifrados y/o examinando su tamaño
- Inyectar datos en el flujo TCP y secuestrar conexiones

> *«El punto de acceso puede determinar la IP virtual de la víctima enviando paquetes SYN-ACK al dispositivo de la víctima por medio del espacio de IP virtual»,* dijo el equipo en un aviso.
>
> *«Cuando envías un SYN-ACK a la IP virtual en el dispositivo de la víctima, el dispositivo responde con un RST, cuando el SYN-ACK se envía a la IP virtual*

> *incorrecta, el atacante no recibe nada».*

Al explicar las variaciones en el comportamiento de los diferentes sistemas operativos, como ejemplo, los investigadores dijeron que el ataque no funciona contra dispositivos macOS/iOS como se describe.

A diferencia de esto, un atacante necesita *«usar un puerto abierto en la máquina Apple para determinar la dirección IP virtual»*. En sus pruebas, los investigadores usan el *«puerto 5223, que se usa para iCloud, iMessage, FaceTime, Game Center, Photo Stream, notificaciones push, etc».*

Los investigadores probaron y explotaron con éxito la vulnerabilidad contra los siguientes sistemas operativos y sistemas init, pero creen que esta lista podría durar mucho tiempo, ya que los investigadores prueban la falla en más sistemas.

- Ubuntu 19.10
- Fedora
- Debian 10.2 (systemd)
- Arco 2019.06 (systemd)
- Manjaro 18.1.1 (systemd)
- Devuan (sysV init)
- MX Linux 19 (Mepis + antiX)
- Linux vacío (runit)
- Slackware 14.2 (rc.d)
- Deepin (rc.d)
- FreeBSD (rc.d)
- OpenBSD (rc.d)

> *«La mayoría de las distribuciones de Linux que probamos eran vulnerables, especialmente las distribuciones de Linux que usan una versión de systemd extraída después del 28 de noviembre de 2018, que desactivó el filtrado de ruta*

> *inversa»*, dijeron los investigadores.
>
> *«Sin embargo, recientemente descubrimos que el ataque también funciona contra IPv6, por lo que activar el cifrado de ruta inversa no es una solución razonable».*

Como una posible mitigación, los investigadores sugirieron activar el filtrado de ruta inversa, implementar el filtrado de bogones y cifrar el tamaño y el tiempo del paquete para evitar que los atacantes hagan alguna inferencia.

Aunque los investigadores no han revelado detalles técnicos de la vulnerabilidad, planean publicar un análisis profundo de la falla y sus implicaciones relacionadas, luego de que los proveedores afectados, incluyendo Systemd, Google, Apple, OpenVPN, WireGuard, y diferentes distribuciones de Linux puedan emitir soluciones y parches satisfactorios.