Detecting a new Linux vulnerability allows hackers to gain control of the VPN connection

International security researchers have found an entirely new Linux vulnerability that allows potential attackers to hijack VPN connections on the device * NIX and 'inject' the arbitrary data payload into it. TCP4 and IPv6 streams.

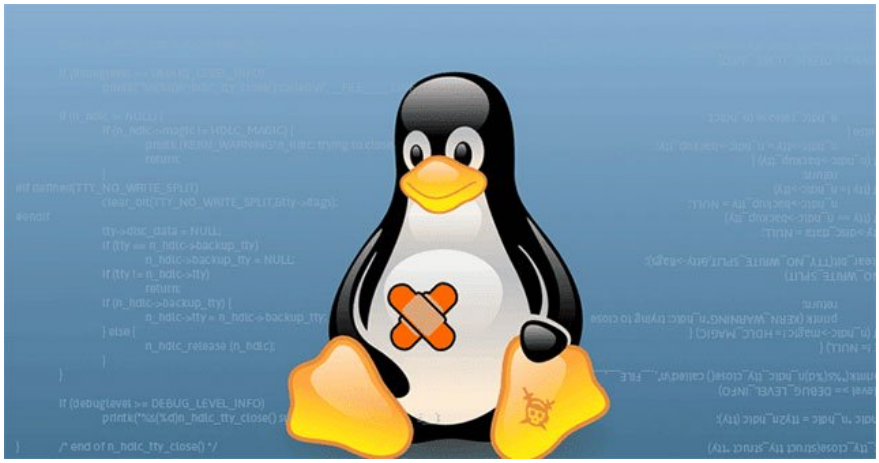
International security researchers have found an entirely new Linux vulnerability that allows potential attackers to hijack VPN connections on the device * NIX and 'inject' the arbitrary data payload into it. TCP4 and IPv6 streams.

This security flaw is currently being tracked with the identifier CVE-2019-14899, which is directly related to Linux distributions and kernel security groups, as well as a number of other affected groups such as Systemd, Google, Apple, OpenVPN and WireGuard. More specifically, the flaw affects most Linux distributions as well as Unix-like operating systems including FreeBSD, OpenBSD, macOS, iOS and Android. Below is a list (incomplete) of the operating systems vulnerable to the vulnerabilities as well as the init systems they come with:

1. Ubuntu 19.10 (systemd)
2. Fedora (systemd)
3. Debian 10.2 (systemd)
4. Arch 2019.05 (systemd)
5. Manjaro 18.1.1 (systemd)
6. Devuan (sysV init)
7. MX Linux 19 (Mepis + antiX)
8. Void Linux (runit)
9. Slackware 14.2 (rc.d)
10. Deepin (rc.d)
11. FreeBSD (rc.d)
12. OpenBSD (rc.d)

All VPN deployment models are affected

According to the findings of experts from the University of New Mexico, this security flaw "allows an attacker to determine which objects are connecting to the VPN, the virtual IP address assigned by the VPN server, and whether or not the connection is compatible with a particular website, and the vulnerability also allows hackers to determine the exact number of seq and ack by counting encrypted packets, or checking their size. This allows them to push data into the TCP stream and gain control.



These CVE-2019-14899 exploits are primarily against OpenVPN, WireGuard and IKEv2 / IPSec, and most likely with Tor. In addition, nearly all Linux distributions using the systemd version with the default configuration are vulnerable.

Below are the necessary steps that a hacker uses to launch an attack to exploit the CVE-2019-14899 vulnerability and hijack the target VPN connection:

1. Determine the virtual IP address of the VPN client.
2. Use virtual IP addresses to infer information about active connections.
3. Use encrypted replies for unsolicited packets to identify the sequence and confirmation number of an active connection in order to hijack a TCP session.

The team is planning to publish an in-depth analysis of this vulnerability as well as its implications after finding the most optimal response.