VPN providers address vulnerability findings by researchers

25 July 2019, by Nancy Cohen

Credit: CC0 Public Domain

Virtual private networks (VPNs) are engineered to encrypt traffic between points on the internet. As *Computing* put it, they extend a private network across a public network, "often used to enable staff working remotely to access resources on their organisation's corporate network."

Well, VPNs are in the news this week but on a security note that researchers discovered that VPN security flaws could open a network to attacks.

Pentesting, security consulting company Devcore made the discovery which promoted them to open their blog report with ".SSL VPNs protect corporate assets from Internet exposure, but what if SSL VPNs themselves are vulnerable?"

The Devcore researchers claimed security flaws in three VPNs that could enable attackers to steal confidential information from a company's network. They wrote about three providers, namely, Palo Alto Networks, Fortinet and Pulse Secure.

They said that "we disclose practical attacks capable of compromising millions of targets, including tech giants and many industry leaders. These techniques and methodologies are published in the hope that it can inspire more security researchers to think out-of-the-box."

Their recent post is titled "Attacking SSL VPN—Part 1: PreAuth RCE on Palo Alto GlobalProtect, with Uber as Case Study!" discussing findings from Orange Tsai and Meh Chang, the two security researchers.

They are on a mission: "In the past several months, we started a new research on the security of leading SSL VPN products. We plan to publish our results on 3 articles."

As of July 17, they posted their first article. According to the team's survey, Palo Alto GlobalProtect before July of last year were vulnerable. The bug was said to be very straightforward, a simple format string vulnerability with no authentication required.

(That is interesting because, as Dev Kundaliya in *Computing* said, "Usually, companies provide their staff with a corporate username and password that need to be entered, along with a two-factor authentication code, before access to the company's network can be granted for the VPN." Yet the flaw could enable a person to break into a network without username/password.)

But why did they mention Uber in their title? That is because they set out to see if any large corporations were using the vulnerable GlobalProtect, and they said they found Uber as one of them. Uber, according to their finding, owned about 22 servers running the GlobalProtect around the world.

Result? No napping at Uber. They sped a response and fixed the vulnerability but also commented on their own investigation. "During our internal investigation, we found that the Palo Alto SSL VPN is not the same as the primary VPN which is used by the majority of our employees."

Did you think a discovery of VPN flaws are special to these three? No, not at all. As pointed out in *Computing*, "It is not the first time that security flaws have been highlighted in VPN software..."

An article back in 2015 in *Computing* said the majority of VPN services suffered from IPv6 traffic leakage.

In May of this year, *Computing*'s Graeme Burton reported on warnings about VPN services used to eavesdrop on users.

The remote code execution flaw, indexed as CVE-2019-1579 carried this description:

"Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code."

The vulnerability affects only older versions of the software.

Palo Alto Networks, meanwhile, acted in response to the report. "Palo Alto Networks is aware of the reported remote code execution (RCE) vulnerability in its GlobalProtect portal and GlobalProtect Gateway interface products. The issue is already addressed in prior maintenance releases. (Ref: CVE-2019-1579)."

Pulse Secure said they released a patch in April, according to *Computing*. *TechRadar* said that Fortinet updated its firmware to address the vulnerability.

You can expect to hear more from them on August 7, where their work is scheduled as a briefing at Black Hat.

APA citation: VPN providers address vulnerability findings by researchers (2019, July 25) retrieved 23 January 2022 from https://techxplore.com/news/2019-07-vpn-vulnerability.html