APT groups are exploiting vulnerabilities in various VPN products

Reference: Memo [191010-1] – Version: 1.0
Keywords: China, APT5, Manganese, VPN, government
Sources: Publicly available information

Key Points

- APT groups are reportedly exploiting vulnerabilities in several unpatched VPN products used worldwide.
- US and UK agencies advise consumers to update VPN products from certain producers.
- Affected VPN products were from Fortinet, Palo Alto Networks and Pulse Secure.
- Certain bugs were detailed at Black Hat USA in August, before detecting attacks on Fortinet and Pulse Secure.

Summary

US and UK agencies advise consumers to update VPN products from Fortinet, Pulse Secure and Palo Alto Networks, stating that state-sponsored advanced persistent threat (APT) groups are using flaws in outdated VPN products to carry out cyberattacks.

The National Security Agency (NSA) issued a Cybersecurity Advisory[1] about the threats and offered mitigation suggestions, warning that multiple APT actors have weaponised three critical vulnerabilities first published in August - CVE-2019-11539, CVE-2019-11510 and CVE-2018-13379 - to gain access to vulnerable VPN devices. The first two affect Pulse Secure VPNs while the third affects Fortinet technology.

The National Cyber Security Centre (NCSC) in the UK posted a separate warning[2] about the threats, which stem from vulnerabilities that allow "an attacker to retrieve arbitrary files, including those containing authentication credentials," according to the post[3]. According to the NCSC UK, sectors affected by these APT attacks against such vulnerable VPNs include government, military, academia, business and healthcare.

Some of the vulnerabilities were detailed at Black Hat USA in August, shortly before attacks on Fortinet and Pulse Secure were first detected. For each of the affected products, Pulse Secure, Palo Alto and Fortinet have all released security updates.

Early September, analysts from the Threat Intelligence Center of Microsoft discovered that a threat actor tracked as Manganese (also known as APT5) had been exploiting the above mentioned vulnerabilities since July/August.

Comments

Security flaws affecting VPN are not uncommon. For example, a few days ago a security researcher discovered a privilege escalation flaw (CVE-2019-6145) that impacts all versions of Forcepoint VPN Client for Windows except the latest release.

It is however less usual to obtain evidence of quick exploitation of VPN vulnerabilities by APT groups.

By exploiting the vulnerabilities attackers could connect to a VPN then change the configuration settings, collect usernames and passwords and obtain the access necessary to introduce secondary exploits, which then could provide attackers with more valuable privileges. This means that these vulnerabilities would enable stealing files that store password information or VPN session data from the affected products. These files would allow attackers to take over the vulnerable devices.

According to FireEye[4], APT5 has been active since at least 2007. APT5 has targeted or breached organisations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications. It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. The group uses malware with keylogging capabilities to specifically target telecommunication companies' corporate networks, employees and executives.

It is not currently known which are the possible other APT groups involved in attacks against the mentioned VPN.

1 https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF
2 https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities
3 https://threatpost.com/apt-groups-exploiting-flaws-in-unpatched-vpns-officials-warn/148956/
4 https://www.fireeye.com/current-threats/apt-groups.html