A Chinese APT is now going after Pulse Secure and Fortinet VPN servers

By Written by Catalin Cimpanu, ContributorContributor Sept. 5, 2019 at 7:11 a.m. PT

Archived: 2026-04-05 15:04:08 UTC

See als

-

A group of Chinese state-sponsored hackers is targeting enterprise VPN servers from Fortinet and Pulse Secure after details about security flaws in both products became public knowledge last month.

The attacks are being carried out by a group known as APT5 (also known as Manganese), ZDNET has learned from sources familiar with the attacks.

According to a FireEye report, APT5 has been active since 2007, and "appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure."

FireEye says the group has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies primarily, and taking a special interest in satellite communications firms.

APT5 attacks began last month

Starting in late August, a subgroup of the larger APT5 umbrella group appears to have set up infrastructure through which they started conducting internet scans to search for Fortinet and Pulse Secure VPN servers.

APT5 was among the first to start scanning the internet and then later attempt to exploit two vulnerabilities in the two VPN server products.

Details about these two vulnerabilities were presented two weeks before, at the Black Hat USA security conference, in Las Vegas.

Both vulnerabilities (CVE-2018-13379 for Fortinet and CVE-2019-11510 for Pulse Secure) are so-called "pre-auth file reads," which allow an attacker to retrieve files from the VPN server without needing to authenticate.

APT5 -- and other threat groups -- were using these two vulnerabilities to steal files storing password information or VPN session data from the affected products. These files would have allowed attackers to take over vulnerable devices.

Sources who observed the APT5 attacks said they weren't in a position to determine if the group was successful in breaching the devices.

Targeted VPN servers are high-end products

Both Fortinet's Fortigate SSL VPN and Pulse Secure's SSL VPN products are extremely popular. For example, Fortinet's Fortigate VPN is the absolute market leader, with over 480,000 Fortigate SSL VPN servers operating across the world.

On the other side, Pulse Secure's SSL VPN is considered the SSL VPN market's most high-end product, being installed to protect access to internal networks at many Fortune 500 companies, the internet's biggest tech firms, and government agencies.

According to threat intelligence firm Bad Packets LLC, there are around 42,000 Pulse Secure VPN servers available online.

Many companies failed to patch

Both the Fortinet and Pulse Secure vulnerabilities were discovered earlier this year by security researchers from a company named Devcore.

The issues were reported to both vendors in March, and patched by both vendors with the utmost urgency, Devcore said in two blog posts describing both issues [1, 2]. Pulse Secure released a patch in April, and Fortinet followed with their own in May.

However, owners of these two SSL VPN servers appear to have failed to install these patches. The reasons for not doing so vary.

On one hand, there have been many Fortinet customers who reported on social media that they didn't even know that there was a security fix available for the Fortigate VPN, let alone that they had to patch.

The company did not return a request for comment sent earlier this week, seeking more information. However, Fortinet published a blog post days before, on August 28, bring the issue of its May patch into the attention of its site readers once more.

Pulse Secure warned and contacted customers

On the other hand, Pulse Secure was a lot more active in notifying customers, but that didn't mean clients heeded the company's advice.

A scan in mid-August found that almost 14,500 of the 42,000 Pulse Secure SSL VPN servers were still running a vulnerable version. A second scan performed last week found that the number barely went down, reaching 10,500.

But the blame here doesn't seem to be on Pulse Secure.

"We not only issued a public Security Advisory - SA44101, but commencing that day in April, we actively informed our customers, partners and service providers of the availability and need for the patch via email, in-product alerts, on our community site, within our partner portal, and our customer support web site," Scott Gordon, Chief Marketing Officer at Pulse Secure, told ZDNet in an email, describing the company's efforts to notify customers.

"Our customer success managers have also been directly contacting and working with customers," he added. "In addition, Pulse Secure support engineers have been available 24x7, including weekends and holidays, to help customers who need assistance to apply the patch fix.

"We also offered assistance to customers to apply the patch fix for these vulnerabilities even if they were not under an active maintenance contract," Gordon said.

"Customers that still need assistance should contact Pulse Secure support using the contact information on the following URL: https://support.pulsesecure.net/support/support-contacts/"

Gordon said that these efforts have been fruitful, as the majority of the company's customers had successfully applied the patch by late August.

Nonetheless, not all customers have heeded the company's advice, and these organizations might end up paying a steeper price later down the road.

Chinese APTs (advanced threat groups) don't just breach into foreign targets (companies, government organizations, universities) for the purpose of intelligence gathering or political cyber-espionage. They also steal intellectual property, which many times makes its way into the hands of Chinese competitors, hurting the hacked companies for years to come in ways many didn't expect.

The world's most famous and dangerous APT (state-developed) malware

Security
