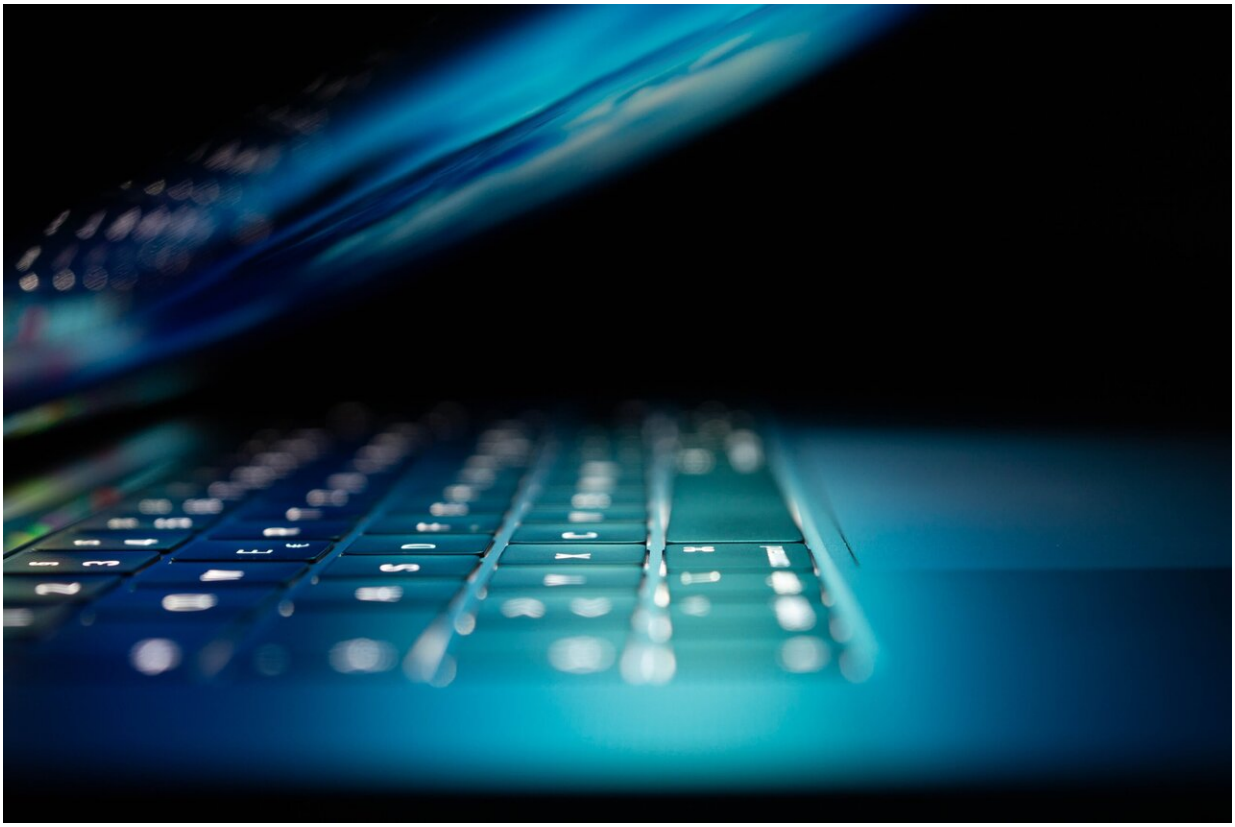
APT actors exploit authentication bypass techniques and Pulse Secure Zero-Day

May 3 2021, by Sarah Katz



Credit: Unsplash/CC0 Public Domain

American cybersecurity firm Mandiant has recently faced a number of security incidents surrounding compromises of Pulse Secure VPN appliances. The attackers involved have used authentication bypass

techniques to circumvent VPN security parameters. The threat groups appear to have installed APT via web shells to monitor systems despite VPN functionality.

These web shells have withstood multiple upgrades. So far, Pulse Secure has ascertained that this attack has built upon a series of prior vulnerabilities and one vulnerability just discovered in April 2021 (CVE-2021-22893) to carry out the initial infection. Since these attacks began, Pulse Secure's parent company Ivanti has provided fixes for a vulnerability exploited using this malware. In addition, the company will release the Pulse Connect Secure Integrity Tool in order for customers to assess whether their systems have been affected.

For now, Pulse Secure and Mandiant have been diligently collaborating to address this issue for customers, government partners and other forensics experts. Thus far, the investigation shows no evidence to suggest that any kind of compromise in the software deployment or supply chain processes introduced these detected backdoors.

Currently, ongoing code analysis initiatives are assessing the 12 seemingly unique malware families associated with these attacks. On the government side, Mandiant has joined forces with Ivanti and Pulse Secure to monitor agency networks for backdoor activity.

Across the board, research teams have labeled the relevant malicious Trojan code that bypasses multifactor authentication as SLOWPULSE. In terms of the web shells, the teams have coined the code names RADIALPULSE and PULSECHECK.

Evidently, threat groups have been using modified, but legitimate, Pulse Secure binaries and scripts to tamper with the VPN appliance. Indeed, attacks related to this vulnerability were uncovered going back to 2019 and 2020.

Researchers have identified the following steps in the attacker process: SLOWPULSE uses Trojanized shared objects with malicious code to log credentials and bypass authentication checks, insert malicious web shells into legitimate, Internet-accessible Pulse Secure VPN appliance administrative web pages for the target devices, toggle the filesystem between Read-Only and Read-Write modes in order to enable file modification, maintain persistence despite administrator upgrades to VPN appliance upgrades, unpatch modified files and remove scripts and utilities after use in order to avoid detection, and use a tool known as THINBLOOD to delete all relevant log files based on a regular expression set by the threat actor.

The final patch for this vulnerability will go into effect starting early this month, May 2021.

More information: Perez, D., et al. "Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day." FireEye, FireEye, Inc., 20 Apr. 2021, www.fireeye.com/blog/threat-re … secure-zero-day.html.