VULNERABILITY BULLETINS

Actors Create New Tools to Exploit Pulse Secure VPN Appliances

TLP:WHITE

May 28, 2021

Security researchers have uncovered four new malware families designed to target Pulse Secure VPN appliances. FireEye's Mandiant cyber forensics team disclosed attacks against defense, government, and financial organizations utilizing vulnerabilities in the software.

The major vulnerability, CVE-2021-22893, issued a CVSS severity score of 10, is as an authentication bypass opening impacting Pulse Connect Secure permitting unauthenticated attackers to perform remote arbitrary code execution (RCE). Other security flaws connected to attacks are CVE-2019-11510, CVE-2020-8260, and CVE-2020-8243, which can be used to establish persistence on a vulnerable appliance and further compromise devices.

Mandiant suspects that Chinese threat actors are exploiting the vulnerabilities, and now, intrusions have been detected at defense, government, technology, transport, and financial entities in the United States and Europe.

Additionally, the United States Cybersecurity and Infrastructure Security Agency (CISA) has updated Alert AA21-110A: Exploitation of Pulse Connect Secure Vulnerabilities to include new threat actor techniques, tactics, and procedures (TTPs), indicators of compromise (IOCs), and updated mitigations related to the newly published alert from Mandiant.

According to the Mandiant researchers, UNC2630 and UNC2717 are the main advanced persistent threat (APT) groups involved in these attacks, and both of which support key Chinese government priorities.

Mandiant notes that in some cases of intrusion, the Chinese threat actors removed a number of backdoors but left persistence patchers potentially as a means to regain access in the future demonstrating an unusual concern for operational security and a sensitivity to publicity.

Reference(s)	Mitre, FireEye, amazonaws, PulseTechnical_BulletinTSB44767, cisa, DHS, Mitre, FireEye, PulseTechnical_BulletinTSB44767, PulseTechnical_BulletinTSB44767, Mitre, Mitre

Recommendations

Pulse Secure parent company Ivanti has released patches and an integrity tool for users to check their builds for risk. It is recommended that the fixes are applied as soon as possible.

CISA encourages users and administrators to review AA21-110A and the following resources for more information:

Re-Checking Your Pulse

Ivanti KB44755 - Pulse Connect Secure (PCS) Integrity Assurance

Ivanti Security Advisory SA44784

Emergency Directive 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities

Sources
ZDNet: Researchers Find Four New Malware Tools Created to Exploit Pulse Secure VPN Appliances

FireEye: Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day

CISA: Exploitation of Pulse Connect Secure Vulnerabilities

Pulse Secure: KB44755 - Pulse Connect Secure (PCS) Integrity Assurance

Pulse Secure: SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4

Emergency Directive 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities

Alert ID 02539e25

View Alert

Tags Pulse Secure, CISA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more update and alerts, visit: **https://health-isac.cyware.com**