HC3: Sector Alert

August 27, 2021 TLP: White Report: 202108271200

Pulse Secure Vulnerabilities Keep on Going

Executive Summary:

Since April 2021 there have been several vulnerabilities in Pulse Secure VPN technology which are being actively compromised. These allow for a variety of malicious activity, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching, all of which can facilitate further attacks on an information infrastructure. The Department of Homeland Security has observed threat actors creating scheduled tasks and remote access trojans to establish persistence, exfiltrate files, and execute ransomware on the victim's network environment including healthcare organizations. It is imperative that the corresponding patches are tested and implemented to prevent healthcare organizations from being compromised.

Impact to HPH Sector:

These vulnerabilities pose a serious threat to HPH as they allow the attacker or threat actor to maintain remote command and control of the target system. In addition to this, the attacker could gain lateral access to a network allowing the harvesting of administrative credentials which would allow the threat actor to have access to all sensitive data. They have been leveraged by threat actors to target the healthcare sector and public health organizations. As indicated in HC3's July alert, this vulnerability continues to impact organizations through the Ivanti Pulse Connect Secure products.

Report /Analysis:

Pulse Secure revealed prior vulnerabilities along with previously unknown CVE-2021-22893, also discovered in April 2021, which were the cause of the initial infection vector. Ivanti, Pulse Secure's parent company released mitigations for a vulnerability exploited in relation to 12 malware families associated with the exploitation of Pulse Secure VPN devices and the Pulse Connect Secure Integrity Tool for customers to determine if their systems were compromised.

In May 2021, the company released a final patch to address the vulnerability. Pulse Secure worked with Mandiant, forensic experts, affected customers, and government partners to address these issues. It is worth noting, during this investigation, there was no indication that backdoors were introduced through a supply chain compromise of the company's network or software.

The Department of Homeland Security has observed threat actors successfully installing ransomware at hospitals, creating scheduled tasks and remote access trojans to establish persistence, amassing files for exfiltration, and executing ransomware on the victim's network environment. To reduce the possibility of detection, threat actors used the Tor infrastructure and virtual private servers. As stated previously, we do not know the threat actors are targeting critical infrastructure, which leaves the HPH as a potential target; therefore, we recommend you remain informed as new information on these vulnerabilities are reported.

On August 24, 2021, the Cybersecurity & Infrastructure Security Agency (CISA) released their analysis of five malware samples that are connected to exploited Pulse Secure devices. CISA encourages both users and administrators to review the following five malware analysis reports (MARs) for threat actor tactics, techniques, and procedures (TTPs) along with indicators of compromise (IOCs). For additional information, review CISA's updated Alert (AA21-110A): Exploitation of Pulse Connect Secure Vulnerabilities .

According to CISA, to gain initial access, the threat actor is leveraging multiple vulnerabilities, including CVE-2019-11510, CVE-2020-8260, CVE-2020-8243, and the newly disclosed CVE-2021-22893. The threat actor is using this access to place webshells on the Pulse Connect Secure appliance for further access and persistence. The known

webshells allow for a variety of functions, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching.

1) MAR-10336935-2.v1: Pulse Connect Secure Malware Analysis Report (AR21-236A)

CISA received two Common Gateway Interface (CGI) scripts for analysis. The two CGI scripts are Pulse Secure system files that were modified by a malicious actor. The files contain a malicious modification which allows the attacker to maintain remote command and control (C2) access to the target's system. This analysis is derived from malicious files found on Pulse Connect Secure devices. For a downloadable copy of indicators of compromise, see: MAR-10336935-2.v1.stix.

2) MAR-10333243-3.v1: Pulse Connect Secure Malware Analysis Report (AR21-236B)

CISA received one unique file for analysis. This file contains a malicious shell script recovered from a compromised Pulse Secure device. This malicious script is designed to modify the Pulse Secure login.cgi script effectively causing it to log a valid user's username and password credentials into a file stored on a disk. This analysis is derived from malicious files found on Pulse Connect Secure devices. See: MAR-10333243-3.v1.stix for downloadable IOCs.

This shell script was used by the attacker to change the Pulse Secure system script named login.cgi. Linux sed command was used to make the modifications the application login.cgi. The attacker implements these changes to cause the system application to log a user's password and username credentials to a file when the user logs into a compromised Pulse Secure device. After this, the credentials can then be retrieved by the attacker or threat actor and used to access the compromised Pulse Secure device remotely, or to pivot to other systems and networks.

Modifications are made to the Pulse Secure login.cgi application by sed commands and effectively result in the user's username and passwords being logged to a file named "/tmp/dswebserver.statementcounters" when the user logs into a compromised Pulse Secure device.

3) MAR-10338401-2.v1: Pulse Connect Secure Malware Analysis Report (AR21-236C)

Of the four files CISA received for analysis, some consist of shell scripts designed to modify a Pulse Secure Perl Common Gateway Interface (CGI) script file in place to become a webshell. One file is designed to intercept certificate-based multi-factor authentication while the other files were created to check, parse and decrypt incoming web request data. This analysis is derived from malicious files found on Pulse Connect Secure devices. For a downloadable copy of indicators of compromise, see: MAR-10338401-r2.v1.stix.

4) MAR-10334057-3.v1: Pulse Connect Secure Malware Analysis Report (AR21-236D)

One CGI script was submitted to CISA for analysis. It was determined the Pulse Secure file had been maliciously modified to siphon login credentials to a file stored in the /tmp directory on the compromised Pulse Secure device. The analysis is derived from malicious files found on Pulse Connect Secure devices. Please see: MAR-10334057-3.v1.stix for a downloadable copy of indicators of compromise.

5) MAR-10339606-1.v1: Pulse Connect Secure Malware Analysis Report (AR21-236E)

Of the five files CISA received for analysis, two files are Perl scripts that execute the attacker's commands stored in the environment variable; one file is a Perl library that provides functions to an installer; one file is a Perl script that

creates a table and that table's first record; and one file is a shell script that manipulates the '/bin/umount' file and executes it. This analysis is derived from malicious files found on Pulse Connect Secure devices. Please see: MAR-10339606-1.v1.stix for a downloadable copy of indicators of compromise.

Recommendations:

HC3 recommends that users and administrators strengthen the security posture of their organization's systems, by following the bulleted items below. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up to date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrator's group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

(*Recommendation Source: CISA)*

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, "Guide to Malware Incident Prevention & Handling for Desktops and Laptops".

HC3: Sector Alert

August 27, 2021 TLP: White Report: 202108271200

Vulnerabilities:

Date:	Vulnerabilities / Data:
(Updated August 24, 2021)	• MAR-10336935-2.v1: Pulse Connect Secure • MAR-10333243-3.v1: Pulse Connect Secure • MAR-10338401-2.v1: Pulse Connect Secure • MAR-10334057-3.v1: Pulse Connect Secure • MAR-10339606-1.v1: Pulse Connect Secure
(Updated August 11, 2021)	Please see CISA's new Malware Analysis Reports for analysis of malicious activity discovered on Pulse Secure Connect devices
(Updated July 21, 2021)	• MAR-10333209-1.v1: Pulse Connect Secure • MAR-10333243-1.v1: Pulse Connect Secure • MAR-10334057-1.v1: Pulse Connect Secure • MAR-10334057-2.v1: Pulse Connect Secure • MAR-10334587-1.v1: Pulse Connect Secure • MAR-10334587-2.v1: Pulse Connect Secure • MAR-10335467-1.v1: Pulse Connect Secure • MAR-10336161-1.v1: Pulse Connect Secure • MAR-10336935-1.v1: Pulse Connect Secure • MAR-10337580-1.v1: Pulse Connect Secure • MAR-10337580-2.v1: Pulse Connect Secure • MAR-10338401-1.v1: Pulse Connect Secure
(Updated May 27, 2021)	CISA has updated this alert to include new threat actor techniques, tactics, and procedures (TTPs), indicators of compromise (IOCs), and updated mitigations. See Ivanti KB44755 - Pulse Connect Secure (PCS) Integrity Assurance for updated guidance to ensure the full integrity of your Pulse Connect Secure software.
(Updated May 3, 2021)	Ivanti has released Security Advisory SA44784 addressing CVE-2021-22893 and three additional newly disclosed CVEs—CVE-2021-22894, CVE-2021-22899, and CVE-2021-22900. CISA strongly encourages organizations using Ivanti Pulse Connect Secure appliances to immediately run the Pulse Secure Connect Integrity Tool, update to the latest software version, and investigate for malicious activity.

References:

Alert (AA21-110A)
Exploitation of Pulse Connect Secure Vulnerabilities
https://us-cert.cisa.gov/ncas/alerts/aa21-110a

Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day
https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

CISA Releases Five Pulse Secure-Related MARs
https://us-cert.cisa.gov/ncas/current-activity/2021/08/24/cisa-releases-five-pulse-secure-related-mars

DHS Warns Hackers Compromising Patched VPNs with Stolen Credentials
https://healthitsecurity.com/news/dhs-warns-hackers-compromising-patched-vpns-with-stolen-credentials

Downloadable lists of IOCs
https://us-cert.cisa.gov/sites/default/files/publications/AA21-110A.xml

Malware Analysis Report (AR21-236A)
MAR-10336935-2.v1: Pulse Secure Connect
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236a

Malware Analysis Report (AR21-236B)
MAR-10333243-3.v1: Pulse Secure Connect
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236b

Malware Analysis Report (AR21-236C)
MAR-10338401-2.v1: Pulse Secure Connect
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236c

Malware Analysis Report (AR21-236D)
MAR-10334057-3.v1: Pulse Secure Connect
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236d

Malware Analysis Report (AR21-236E)
MAR-10339606-1.v1: Pulse Secure Connect
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-236e

NIST Special Publication 800-83 Revision 1
Guide to Malware Incident Prevention and Handling for Desktops and Laptops
http://dx.doi.org/10.6028/NIST.SP.800-83r1

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback