America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Continued Threat Actor Exploitation Post Pulse Secure VPN Patching

Last Revised: October 24, 2020 **Alert Code:** AA20-107A

Summary

Note: *This Activity Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise <https://attack.mitre.org/versions/v7/matrices/enterprise/> framework for all referenced threat actor techniques and mitigations.*

This Alert provides an update to Cybersecurity and Infrastructure Security Agency (CISA) Alert AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-010a>, which advised organizations

to immediately patch CVE-2019-11510—an arbitrary file reading vulnerability affecting Pulse Secure virtual private network (VPN) appliances.[1] <https://kb.pulsesecure.net/articles/pulse_security_advisories/sa44101> CISA is providing this update to alert administrators that threat actors who successfully exploited CVE-2019-11510 and stole a victim organization's credentials will still be able to access—and move laterally through—that organization's network after the organization has patched this vulnerability if the organization did not change those stolen credentials.

This Alert provides new detection methods for this activity, including a CISA-developed tool <https://github.com/cisagov/check-your-pulse> that helps network administrators search for indicators of compromise (IOCs) associated with exploitation of CVE-2019-11510. This Alert also provides mitigations for victim organizations to recover from attacks resulting from CVE-2019-11510. CISA encourages network administrators to remain aware of the ramifications of exploitation of CVE-2019-11510 and to apply the detection measures and mitigations provided in this report to secure networks against these attacks.

For a downloadable copy of IOCs, see STIX file </sites/default/files/publications/aa20-107a_iocs(white).stix.xml>.

Background

CISA has conducted multiple incident response engagements at U.S. Government and commercial entities where malicious cyber threat actors have exploited CVE-2019-11510—an arbitrary file reading vulnerability affecting Pulse Secure VPN appliances—to gain access to victim networks. Although Pulse Secure released patches for CVE-2019-11510 in April 2019,[2] <https://kb.pulsesecure.net/articles/pulse_security_advisories/sa44101> CISA has observed incidents where compromised Active Directory credentials were used months after the victim organization patched their VPN appliance.

Technical Details

CISA determined that cyber threat actors have been able to obtain plaintext Active Directory credentials after gaining *Initial Access* [TA0001] <https://attack.mitre.org/versions/v7/tactics/ta0001/> to a victim organization's network via VPN appliances. Cyber threat actors used these *Valid Accounts* [T1078] <https://attack.mitre.org/versions/v7/techniques/t1078/> in conjunction with:

- *External Remote Services* [T1133] <https://attack.mitre.org/versions/v7/techniques/t1133> for access,
- *Remote Services* [T1021] <https://attack.mitre.org/versions/v7/techniques/t1021> for *Lateral Movement* [TA0008] <https://attack.mitre.org/versions/v7/tactics/ta0008/> to move quickly throughout victim network environments, and
- *Data Encrypted for Impact* [T1486] <https://attack.mitre.org/versions/v7/techniques/t1486> for impact, as well as
- *Exfiltration* [TA0010] <https://attack.mitre.org/versions/v7/tactics/ta0010/> and sale of the data.

Initial Access

CVE-2019-11510 is a pre-authentication arbitrary file read vulnerability affecting Pulse Secure VPN appliances. A remote attacker can exploit this vulnerability to request arbitrar files from a VPN server. The vulnerability occurs because directory traversal is hard coded be allowed if the path contains `dana/html5acc/`.[3] <https://twitter.com/xmppwocky/status/1164874297690611713/photo/1>,[4] For example, a malicious cyber actor can obtain the contents of `/etc/passwd` [5] <https://github.com/bishopfox/pwn-pulse/blob/master/pwn-pulse.sh> by requesting the following uniform resource identifier (URI):

`https://vulnvpn.example[.]com/dana-na/../dana/html5acc/guacamole/../../../../../../../etc/passwd?/dana/html5acc/guacamole/`

Obtaining the contents of `/etc/passwd` gives the attacker access to basic information about local system accounts. This request was seen in the proof of concept (POC) code for this exploit on Github <https://github.com/bishopfox/pwn-pulse/blob/master/pwn-pulse.sh>. An attacker can also leverage the vulnerability to access other files that are useful for remote exploitation. By requesting the data.mdb object, an attacker can leak plaintext credentials of enterprise users.[6] <https://www.exploit-db.com/exploits/47297>,[7],[8]

Open-source reporting indicates that cyber threat actors can exploit CVE-2019-11510 to retrieve encrypted passwords;[9] however, CISA has not observed this behavior. By reviewing victim VPN appliance logs, CISA has noted cyber threat actors crafting requests that request files that allow for *Credential Dumping* [T1003] <https://attack.mitre.org/versions/v7/techniques/t1003> plaintext passwords from the VPN appliance.

Test Environment

To confirm the open-source reporting and validate what the cyber threat actors had access to, CISA used a test environment to send crafted requests. CISA used requests found both in proof-of-concept, open-source code and in requests from the logs of compromised victims. By doing so, CISA confirmed that plaintext Active Directory credentials were leaked and th it was possible to leak the local admin password to the VPN appliance. (See figure 1.)

Give Feedback

Figure 1: Exploitation of the VPN appliance leading to plaintext local admin credentials

CISA's test environment consisted of a domain controller (DC) running Windows Server 2016, an attacker machine, and a Pulse Secure VPN appliance version 9.0R3 (build 64003). CISA connected the attacker machine to the external interface of the Pulse Secure VPN appliance and the DC to the internal interface.

CISA created three accounts for the purpose of validating the ability to compromise them by exploiting CVE-2019-11510.

- Local Pulse Secure Admin account
  - Username: `admin`; Password: `pulse-local-password`
- Domain Administrator Account
  - Username: `Administrator`; Password: `domain-admin-password1`
- CISA-test-user Account
  - Username: `cisa-test-user`; Password: `Use_s3cure_passwords`

After creating the accounts, CISA joined the VPN appliance to the test environment domain, making a point not to cache the domain administrator password. (See figure 2.)

Figure 2: VPN appliance joined to the domain without caching the domain administrator password

CISA used a similar file inclusion to test the ability to *Credential Dump* [T1003] <https://attack.mitre.org/versions/v7/techniques/t1003> the domain administrator password. CISA determined it was possible to leak the domain administrator password that was used to join the device to the domain without saving the credentials. Refer to figure 3 for the URI string tested by CISA.

Figure 3: Exploitation of the VPN appliance leading to cleartext domain admin credentials

Next, CISA validated the ability to *Credential Dump* [T1003] <https://attack.mitre.org/versions/v7/techniques/t1003> a user password from the VPN appliance. To do this, CISA created a *user realm* (Pulse Secure configuration terminology) and configured its roles/resource groups to allow for Remote Desktop Protocol (RDP) over HTML5 (Apache

Guacamole). After using the new user to remotely access an internal workstation over RDP, CISA used a crafted request (see figure 4) to leak the credentials from the device. (**Note:** the path to stored credentials is publicly available.)[10]

Figure 4: Exploitation of the VPN appliance leading to plaintext user credentials

This test confirmed CISA's suspicion that threat actors had access to each of the various compromised environments.

Cyber Threat Actor Behavior in Victim Network Environments

CISA observed—once credentials were compromised—cyber threat actors accessing victim network environments via the Pulse Secure VPN appliances. Cyber threat actors used *Connection Proxies* [T1090] <https://attack.mitre.org/versions/v7/techniques/t1090>—such as Tor infrastructure and virtual private servers (VPSs)—to minimize the chance of detection when they connected to victim VPN appliances.

Using traditional host-based analysis, CISA identified the following malicious cyber actor actions occurring in a victim's environment:

- Creating persistence via scheduled tasks/remote access trojans
- Amassing files for exfiltration
- Executing ransomware on the victim's network environment

By correlating these actions with the connection times and user accounts recorded in the victim's Pulse Secure `.access` logs, CISA was able to identify unauthorized threat actor connections to the victim's network environment. CISA was then able to use these Internet Protocol (IP) addresses and user-agents to identify unauthorized connections to the network environments of other victims. Refer to the Indicators of Compromise section for the IP addresses CISA observed making these unauthorized connections.

In one case, CISA observed a cyber threat actor attempting to sell the stolen credentials after 30 unsuccessful attempts to connect to the customer environment to escalate privileges and drop ransomware. CISA has also observed this threat actor successfully dropping ransomware at hospitals and U.S. Government entities.

In other cases, CISA observed threat actors leveraging tools, such as LogMeIn and TeamViewer, for persistence. These tools would enable threat actors to maintain access to the victim's network environment if they lost their primary connection.

Initial Detection

Conventional antivirus and endpoint detection and response solutions did not detect this type of activity because the threat actors used legitimate credentials and remote services.

An intrusion detection system may have noticed the exploitation of CVE-2019-11510 if the sensor had visibility to the external interface of the VPN appliance (possible in a customer's demilitarized zone) and if appropriate rules were in place. Heuristics in centralized logging may have been able to detect logins from suspicious or foreign IPs, if configured.

Post-Compromise Detection and IOC Detection Tool

Given that organizations that have applied patches for CVE-2019-11510 may still be at risk for exploitation from compromises that occurred pre-patch, CISA developed detection methods for organizations to determine if their patched VPN appliances have been targeted by the activity revealed in this report.

To detect past exploitation of CVE-2019-11510, network administrators should:

1. Turn on unauthenticated log requests (see figure 5). (**Note:** there is a risk of overwriting logs with unauthenticated requests so, if enabling this feature, be sure to frequently back up logs; if possible, use a remote syslog server.)

Figure 5: Checkbox that enables logging exploit attacks

2. Check logs for exploit attempts. To detect lateral movement, system administrators should look in the logs for strings such as `../../../data` (see figure 6).

Figure 6: Strings for detection of lateral movement

3. Manually review logs for unauthorized sessions and exploit attempts, especially sessions originating from unexpected geo-locations.
4. Run CISA's IOC detection tool. CISA developed a tool that enables administrators to triage logs (if authenticated request logging is turned on) and automatically search for IOCs associated with exploitation of CVE-2019-11510. CISA encourages administrators visit CISA's GitHub page <https://github.com/cisagov/check-your-pulse> to download and run the tool. While not exhaustive, this tool may find evidence of attempted compromise.

Indicators of Compromise

CISA observed IP addresses making unauthorized connections to customer infrastructure. (**Note:** these IPs were observed as recently as February 15, 2020.) The IP addresses seen making unauthorized connections to customer infrastructure were different than IP addresses observed during initial exploitation. Please see the STIX file below for IPs.

CISA observed the following user agents with this activity:

- Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
- Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55[.]0.2883.87 Safari/537.36

CISA also observed:

- A cyber threat actor renaming portable executable (PE) files in an attempt to subvert application allow listing or antivirus (AV) protections. See table 1 for hashes of files used.
- A threat actor "living off the land" and utilizing C:\Python\ArcGIS to house malicious PE files, as well as using natively installed Python.
- A threat actor attack infrastructure: 38.68.36(dot)112 port 9090 and 8088

Table 1: Filenames and hashes of files used by a threat actor

Filename	MD5
t.py (tied to scheduled task, python meterpreter reverse shell port 9090)	5669b1fa6bd8082ffe306aa6e597d7f5
g.py (tied to scheduled task, python meterpreter reverse shell port 8088)	61eebf58e892038db22a4d7c2ee65579

For a downloadable copy of IOCs, see STIX file </sites/default/files/publications/aa20-107a_iocs(white).stix.xml>.

Mitigations

CISA strongly urges organizations that have not yet done so to upgrade their Pulse Secure VPN to the corresponding patches for CVE-2019-11510. If—after applying the detection measures in this alert—organizations detect evidence of CVE-2019-11510 exploitation, CISA recommends changing passwords for all Active Directory accounts, including administrators and services accounts.

CISA also recommends organizations to:

- Look for unauthorized applications and scheduled tasks in their environment.
- Remove any remote access programs not approved by the organization.
- Remove any remote access trojans.
- Carefully inspect scheduled tasks for scripts or executables that may allow an attacker to connect to an environment.

If organizations find evidence of malicious, suspicious, or anomalous activity or files, they should consider reimaging the workstation or server and redeploying back into the environment. CISA recommends performing checks to ensure the infection is gone even if the workstation or host has been reimaged.

Contact Information

To report suspicious activity related to information found in this joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at contact@mail.cisa.dhs.gov or by calling 1-844-Say-CISA (1-844-729-2472). When available, please include the information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

References

[1] Pulse Secure Advisory SA44101
<https://kb.pulsesecure.net/articles/pulse_security_advisories/sa44101>

[2] Pulse Secure Advisory SA44101
<https://kb.pulsesecure.net/articles/pulse_security_advisories/sa44101>
[3] Twitter. @XMPPwocky. (2019, August 23). Your least favorite construct
<https://twitter.com/xmppwocky/status/1164874297690611713/photo/1>
[4] OpenSecurity Forums. Public vulnerability discussion. (2019, August 23).
[5] GitHub. BishopFox / pwn-pulse. <https://github.com/bishopfox/pwn-pulse/blob/master/pwn-pulse.sh>
[6] File disclosure in Pulse Secure SSL VPN (Metasploit) <https://www.exploit-db.com/exploits/47297>
[7] Twitter. @alyssa_herra
[8] OpenSecurity Forums. Public vulnerability discussion. (2019, August 23).
[9] OpenSecurity Forums. Public vulnerability discussion. (2019, August 31).
[10] Twitter. @alyssa_herra

Revisions

April 16, 2020: Initial Version

October 23, 2020: Revision

September 05, 2023: Revision

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Give Feedback