Vulnerable Private Networks: Corporate VPNs Exploited in the Wild

volexity.com/blog/2019/09/11/vulnerable-private-networks-corporate-vpns-exploited-in-the-wild/

September 11, 2019

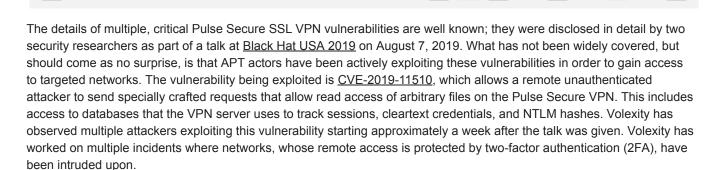
by Sean Koessel, Steven Adair



INTELLIGENCE

Active Exploitation of Pulse Secure VPN

- Mass Scanning & Targeted Exploitation
- Database Theft Containing Session IDs & Credentials
- VPN Session Take Over, Bypassing 2FA
- Stolen Credentials Leveraged in Attacks Against Other Resources



The arbitrary file read vulnerability, along with a handful of other security issues, was initially described and patched on April 25, 2019, by Pulse Secure as detailed in a security advisory from the company, tracked as <u>SA44101</u>. Volexity believes that as of mid-August, a significant number of organizations had not actually applied updates that would have fixed this issue. This means that numerous organizations were—and still are—at risk and are potentially allowing unauthorized access to their networks and systems.

Active Exploitation

Volexity has observed attackers actively exploiting CVE-2019-11510 against vulnerable Pulse Secure VPN servers. Decrypted TLS sessions and logs confirm that attackers have been accessing various files to assist in compromising target networks.

The following files have been observed as part of testing/vulnerability confirmation:

/etc/passwd (testing/confirmation of vulnerability)

/etc/hosts (testing/confirmation of vulnerability)



The following files have been observed being accessed to obtain session IDs, cleartext credentials, and other stored or cached system and user data:

/data/runtime/mtmp/Imdb/randomVal/data.mdb

/data/runtime/mtmp/lmdb/dataa/data.mdb

/data/runtime/mtmp/system

Once the attackers obtained the database files, Volexity observed the following behavior:

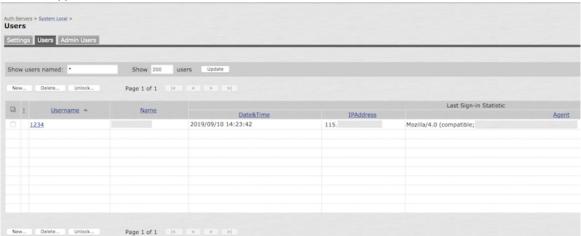
- · Connections to the VPN using obtained session IDs in order to resume or takeover an existing valid session
- · Locally stored accounts cracked and leveraged to connect to VPN services
- Connections to the VPN's administrative interface using obtained sessions IDs, possibly in an attempt to conduct remote code execution against newly connecting VPN clients
- Login attempts against other corporate resources, such as e-mail, using credentials that were stored by the Pulse Secure VPN server database in the clear

While it should not be a surprise, it should be noted that 2FA **will not** prevent an attacker from hijacking a valid authenticated session. Once the initial login occurs from the valid user that supplied credentials and a valid second authentication factor, that session can now be hijacked by an attacker who will ride in on the session without further impediment (more on this below).

Local Accounts

It is common for an organization to use a separate directory for its users, such as an LDAP server, for authentication. However, Pulse Secure devices will have one or more local administrator accounts. Any of the administrator accounts on the system, such as the default "admin" account, should have their password changed. It should be considered compromised and potentially cracked by a remote attacker. Furthermore, organizations should also check to see if they have any active or valid local accounts that are not administrative users and may potentially have VPN access. These accounts could potentially be set up in a manner that also circumvents 2FA.

The account settings can be found under Authentication -> Auth. Servers. The typical next step is to look at the users under "Administrators" and "System Local." Below is an example of how a locally enabled user account under System Local will appear.



Detection

If you are running a vulnerable version of the Pulse Secure SSL VPN, it would be safe to assume that credentials used on the device since early August 2019 may be compromised. It is possible that the database containing cleartext credentials could have been stolen and leveraged without leaving any indicators in the logs on your Pulse Secure VPN server. Special concern should be given to VPNs that are not protected by 2FA or other resources not protected by 2FA that leverage the

same credentials as the Pulse Secure VPN (e.g., Active Directory). Look for authentications from unknown sources or from IP addresses listed in the Network Indicators section below. Pay close attention to multi-factor authentication failures that were invalid or were otherwise incomplete/abandoned.

Unauthenticated Web Requests

If a Pulse Secure VPN is set up to log unauthenticated web requests, logs can be examined for entries similar to the following:

info - [x.x.x.x] - System()[][] - 2019/08/14 09:15:26 - VPN-Remote - Connection from IP x.x.x.x not authenticated yet (URL=/dana-

na/../dana/html5acc/guacamole/../../../../data/runtime/mtmp/lmdb/randomVal/data.mdb?/dana/html5acc/guacamole/)

Entries like the above indicate exploit attempts against the SSL VPN. These logs can be studied further to look for access to other files and to identify IP addresses responsible for probing and attacking an organization's VPN server. Attempted access to the /admin URL may also be of particular interest when reviewing these logs.

Note: Unauthenticated web request logging may not be enabled by default. In order to enable this logging, an administrator must go to System -> Log/Monitoring -> User Access -> Settings and check [x] Unauthenticated Requests.

Session Hijacking

One of the major risks this vulnerability poses it that it can allow a remote attacker to bypass all forms of authentication typically required by an organization's VPN server, especially one that otherwise requires 2FA to access. Volexity has observed multiple attackers leveraging data taken from the session databases to then directly access a target's VPN server. This is done simply by providing an active session ID in a cookie called **DSID**. Setting the DSID cookie to a valid active session will allow an attacker to drop right into the authenticated user's VPN session on a Pulse Secure VPN and begin accessing whatever resources are available to that user. The Pulse Secure VPN will also allow multiple simultaneous users with the same session ID. The valid authenticated user will not receive any indication that their session is in use on another device nor will it impact their session.

Pulse Secure VPN logs do give an indication that this activity has occurred. Log lines such as the following should appear:

2019-08-14 09:35:32 - PulseSecure - [1.2.3.4] DOMAIN\username - Remote address for user DOMAIN\username changed from 1.2.3.4 to 5.6.7.8.

Additionally, the logs may also appear similar to the following:

 $2019-08-14\ 09:38:56$ - PulseSecure - [1.2.3.4] DOMAIN\username - Remote address for user DOMAIN\username changed from 5.6.7.8 to .

If you see several lines like this with the IP addresses changing back and forth, this may be a good indication of multiple active users on a single session. It should be noted that logs entries like this will happen legitimately as users change IP addresses. Seeing lines like this should be expected. Look for frequent occurrences, suspect IPs, or one IP address showing up on several occasions for multiple different users.

Mitigation

To mitigate this vulnerability, upgrade to a non-vulnerable version of the Pulse Secure VPN software. Volexity would strongly recommend cutting off all access to any Pulse Secure VPN servers until they are patched. All credentials used on the system, both locally stored and from remote authentication sources, should be reset/changed immediately. This also includes any multi-factor authentication API keys that may have been stored on the device. Furthermore, it is critical that any credential or secret that is stored or used on the Pulse Secure VPN be changed immediately. Attackers are actively leveraging credentials to attempt to connect to other resources that may not required 2FA.

Network Indicators

Volexity has observed the following IP addresses exploiting this vulnerability or taking advantage of data likely obtained from exploitation between August 14, 2019 - August 28, 2019:

IPv4 Address	Notes
104.217.128.133	IP address observed actively scanning and exploiting CVE-2019-11510.
185.163.46.141	IP address observed actively scanning and exploiting CVE-2019-11510.
185.200.116.203	IP address observed actively scanning and exploiting CVE-2019-11510.
192.126.124.26	IP address observed actively scanning and exploiting CVE-2019-11510.
23.152.0.247	IP address observed actively scanning and exploiting CVE-2019-11510.
27.102.70.150	IP address observed actively scanning and exploiting CVE-2019-11510.
37.120.150.98	IP address observed actively scanning and exploiting CVE-2019-11510.
5.157.10.2	IP address observed actively scanning and exploiting CVE-2019-11510.
5.197.149.19	IP address observed actively scanning and exploiting CVE-2019-11510.
5.254.81.170	IP address observed actively scanning and exploiting CVE-2019-11510.
5.254.81.178	IP address observed actively scanning and exploiting CVE-2019-11510.
94.242.246.46	IP address observed actively scanning and exploiting CVE-2019-11510.

Conclusion

Several organizations recently experienced, or are currently experiencing, breaches due to data accessed or compromised from VPN instances that were not updated prior to early-to-mid August. Volexity observed widespread exploitation of this vulnerability on August 14, 2019. The actual details of the exploit were widely released to the public on August 7, 2019. Organizations that patched vulnerable instances of their Pulse Secure VPN on August 14 or later should consider any credentials used or stored on their Pulse Secure to be compromised. It is also reasonable to expect that exploitation was widely known from August 7, 2019, and onward as well. Volexity strongly recommends organizations take a close look at their logs and determine if they may have been breached. Any organization with questions about how best to analyze their logs or that need assistance determining if they have experienced a breach are welcome to reach out to Volexity via our website contact form.