


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



VOLEXITY

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 details of multiple, critical Pulse Secure SSL VPN vulnerabilities are well known; they were disclosed in detail by two security researchers as part of a talk at [Black Hat USA 2019](#) on August 7, 2019. What has not been widely covered, but should come as no surprise, is that APT actors have been actively exploiting these vulnerabilities in order to gain access to targeted networks. The vulnerability being exploited is [CVE-2019-11510](#), which allows a remote unauthenticated attacker to send specially crafted requests that allow read access of arbitrary files on the Pulse Secure VPN. This includes access to databases that the VPN server uses to track sessions, cleartext credentials, and NTLM hashes. Volexity has observed multiple attackers exploiting this vulnerability starting approximately a week after the talk was given. Volexity has worked on multiple incidents where networks, whose remote access is protected by two-factor authentication (2FA), have been intruded upon.

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 [SA44101](#). 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/lmdb/randomVal/data.mdb  
/data/runtime/mtmp/lmdb/dataaa/data.mdb  
/data/runtime/mtmp/system
```

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

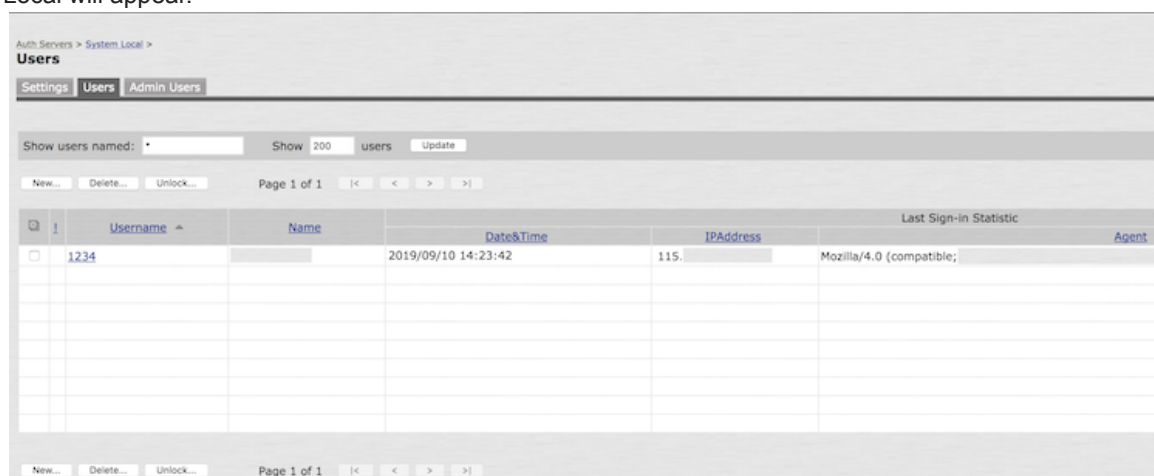
- Connections to the VPN using obtained session IDs in order to resume or takeover an existing valid session
- Locally stored accounts cracked and leveraged to connect to VPN services
- Connections to the VPN's administrative interface using obtained sessions IDs, possibly in an attempt to conduct remote 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.



The screenshot shows the Pulse Secure web interface for managing users. The breadcrumb trail is 'Auth Servers > System Local > Users'. The page title is 'Users'. There are tabs for 'Settings', 'Users', and 'Admin Users'. Below the tabs, there are controls for 'Show users named:' (a dropdown menu), 'Show 200 users', and an 'Update' button. There are also buttons for 'New...', 'Delete...', and 'Unlock...'. The main content is a table with the following columns: 'Username', 'Name', 'Date&Time', 'IPAddress', 'Last Sign-in Statistic', and 'Agent'. The table contains one row with the following data: Username: 1234, Name: (redacted), Date&Time: 2019/09/10 14:23:42, IPAddress: 115., Last Sign-in Statistic: Mozilla/4.0 (compatible;), Agent: (redacted). The table is on 'Page 1 of 1'.

	Username	Name	Date&Time	IPAddress	Last Sign-in Statistic	Agent
<input type="checkbox"/>	1234		2019/09/10 14:23:42	115.	Mozilla/4.0 (compatible;)	

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

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](#).