National Cyber Security Centre
a part of GCHQ

Alert: APTs exploiting multiple vulnerabilities in several VPN products used worldwide

Version 2.0

8 October 2019

Introduction

The NCSC is investigating the exploitation, by APT actors, of known vulnerabilities affecting a number of VPN products from vendors Pulse Secure, Fortinet and Palo Alto.

This activity is ongoing, targeting both UK and international organisations. Affected sectors include government, military, academic, business and healthcare. These vulnerabilities are well documented in open source, and industry data indicates that hundreds of UK hosts may be vulnerable.[1]

Details

Vulnerabilities exist in several SSL VPN products which allow an attacker to retrieve arbitrary files, including those containing authentication credentials.

An attacker can use these stolen credentials to connect to the VPN and change configuration settings, or connect to further internal infrastructure.

Unauthorised connection to a VPN could also provide the attacker with the privileges needed to run secondary exploits aimed at accessing a root shell.

Top vulnerabilities

The highest-impact vulnerabilities known to be exploited by APTs are listed below, although this is not an exhaustive list of CVEs associated with these products.

Sample exploit code for these vulnerabilities is publicly available online. The NCSC cautions against testing infrastructure with untrusted third-party code.

Pulse Connect Secure:

- CVE-2019-11510: Pre-auth arbitrary file reading
- CVE-2019-11539: Post-auth command injection

Fortinet:

- CVE-2018-13379: Pre-auth arbitrary file reading
- CVE-2018-13382: Allows an unauthenticated attacker to change the password of an SSL VPN web portal user.
- CVE-2018-13383: Post-auth heap overflow. This allows an attacker to gain a shell running on the router.

[1] https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/

Palo Alto:

- CVE-2019-1579: Palo Alto Networks GlobalProtect Portal

Detecting exploitation

Users of these VPN products should investigate their logs for evidence of compromise, especially if it is possible that patches were not applied immediately after their release.

Apart from specific product advice below, administrators should also look for evidence of compromised accounts in active use, such as anomalous IP locations or times.

Snort rules are available in open source but may not pick up events for exploits over HTTPS.

Pulse Connect Secure

The best way to detect exploitation attempts is to search for evidence of connections to vulnerable URLs on the device.

Pulse Secure logging is highly configurable, so to test whether web requests are logged on a system, make an HTTPS request to the web interface directly, not via the VPN, and then check if it appears in the event logs.

Once you have established that logging is working, search for the URLs below. Hits before a patch was applied may indicate a compromise and should be investigated further.

Vulnerability	**Detection**
CVE-2019-11510	Search logs for URLs containing **?** and ending with **/dana/html5acc/guacamole/** (Regular Expression: **\?.*dana/html5acc/guacamole/**) If any are found dated before the patch was applied, it may indicate a compromise. The matching string will contain the name of the file the attacker attempted to read.
CVE-2019-11539	Search for requests to **/dana-admin/diag/diag.cgi** with an **options=** parameter in the URL. An exploit will almost certainly contain: -r, # or 2> [Data between -r and # is perl code that would be executed.]

Fortigate

Fortigate devices do not log web requests by default, but if a device is configured to write firewall logs for all connections, or if firewall or netflow logs are available from another device in front of it, it might be possible to detect exploitation.

When exploiting CVE-2018-13379, an attacker may download sslvpn_websession, which contains the usernames and passwords of active users. This file is typically at least 200 KB.

Searching firewall, or netflow logs, for TCP sessions with 200,000-250,000 bytes from the SSL VPN device's web interface port to the client, and a small number of bytes (less than 2,000) from the client, may return evidence of exploitation.

Palo Alto

In July 2019 Palo Alto released a security notification (CVE-2019-1579) for a vulnerability they previously patched in August 2018. The following versions may be vulnerable:

- Palo Alto GlobalProtect SSL VPN 7.1.x < 7.1.19
- Palo Alto GlobalProtect SSL VPN 8.0.x < 8.0.12
- Palo Alto GlobalProtect SSL VPN 8.1.x < 8.1.3

It may be difficult to detect past exploitation in logs. But failed exploit attempts may cause a crash, which could be visible in logs.

Essential mitigation

To mitigate these vulnerabilities, owners of vulnerable products should take two steps:

1. Apply the latest security patches released by vendors
2. Reset authentication credentials associated with affected VPNs and accounts connecting through them

The most effective way to mitigate the risk of actors exploiting these vulnerabilities is to ensure that the affected products are patched with the latest security updates.

Pulse secure, Fortinet and Palo Alto have all released patches for these vulnerabilities.

Security patches should always be applied promptly. More guidance is available on the NCSC website. The NCSC acknowledges that patching is not always straightforward and in some cases can cause business disruption, but it remains the single most important step an organisation or individual can take to protect itself.

If you suspect exploitation

System administrators who suspect that exploitation may have occurred or cannot rule out this possibility should revoke credentials that were at risk of theft. This may include both administrative and user credentials.

Resetting authentication credentials will defend against unauthorised access using credentials acquired prior to patching affected systems.

Additional mitigations

The NCSC strongly recommends that organisations previously targeted by APT actors, or which have detected successful exploitation of their VPNs, carry out the following additional mitigation steps:

- **VPN settings**: Check all configuration options for unauthorised changes. This includes the SSH authorized_keys file, new iptables rules and commands set to run on connecting clients. If you have known-good backups of the configuration you can restore then restoring these may be prudent. More information on potential post-exploitation actions is available online.

- **Log analysis and monitoring:** Review and continue to monitor logs for the VPN, network traffic and services users connect to through the VPN such as email. Check for connections from uncommon IP addresses, particularly those with successful logins or large data lengths returned. Identify replay attempts using old credentials that have been reset.

- **Wipe the device:** If you suspect exploitation has occurred but cannot find specific evidence of changes made, you may wish to factory reset (or wipe) your device. Follow the device manufacturer's guidance on how to do this.

- **Two-factor authentication:** Where possible, enable two-factor authentication for the VPN to defend against password replay attacks.

- **Reduce threat surface:** Disable any functionality and ports on the VPN which are not required, or used.

Reporting to the NCSC

Any current activity related to these threats should be reported via the NCSC website here where the NCSC can offer help and guidance.

The NCSC is also interested in receiving indicators of compromise and threat intelligence, even if the activity has already been remediated.