Mitigating Recent VPN Vulnerabilities

Active Exploitation

Multiple Nation State Advanced Persistent Threat (APT) actors have weaponized CVE-2019-11510, CVE-2019-11539, and CVE-2018-13379 to gain access to vulnerable VPN devices.

In August, 2019, the Canadian Centre for Cyber Security released guidance for mitigating vulnerabilities in 3 major VPN products (Pulse Secure®, Palo Alto GlobalProtect™, and Fortinet Fortigate®). That guidance lists indicators of compromise for detecting malicious activity [1]. This Cybersecurity Advisory is intended to convey additional actions for compromise recovery and longer-term actions for hardening.

Mitigations for Pulse Secure® VPN Client

On April 24, 2019, security researchers released a series of vulnerabilities in the Pulse Secure® VPN from version 5.1RX to 9.0RX [2]. These vulnerabilities allow for remote arbitrary file downloads and remote code execution on Pulse Connect Secure and Pulse Policy Secure gateways. Other vulnerabilities in the series allow for interception or hijacking of encrypted traffic sessions. Exploit code is freely available online via the Metasploit® framework, as well as GitHub®. Malicious cyber actors are actively using this exploit code. System owners are strongly recommended to upgrade to the respective versions listed in the table below [3].

Affected Versions	Recommended Patch Version Deployment
Pulse Connect Secure 9.0RX	Pulse Connect Secure 9.0R3.4 & 9.0R4
Pulse Connect Secure 8.3RX	Pulse Connect Secure 8.3R7.1
Pulse Connect Secure 8.2RX	Pulse Connect Secure 8.2R12.1
Pulse Connect Secure 8.1RX	Pulse Connect Secure 8.1R15.1
Pulse Policy Secure 9.0RX	Pulse Policy Secure 9.0R3.2& 9.0R4
Pulse Policy Secure 5.4RX	Pulse Policy Secure 5.4R7.1
Pulse Policy Secure 5.3RX	Pulse Policy Secure 5.3R12.1
Pulse Policy Secure 5.2RX	Pulse Policy Secure 5.2R12.1
Pulse Policy Secure 5.1RX	Pulse Policy Secure 5.1R15.1

CVE-2019-11508 and CVE-2019-11538 can also be mitigated by disabling File Share features on the Pulse Connect Secure device if such file sharing is not needed [3].

It was previously reported that requiring certificate-based authentication would mitigate the CVE-2019-11510 vulnerability, but in fact the vulnerability is still exploitable due to traversals from unauthenticated directories [4].

Mitigations for Palo Alto VPN Client

Vulnerability CVE-2019-1579 against Palo Alto GlobalProtect VPN allows remote code execution and is being exploited in the wild, according to researchers [5] [6]. Upgrade devices to the latest version.

Mitigations for Fortinet Fortigate VPN Client

Vulnerabilities in Fortinet Fortigate VPN devices have also been disclosed recently, including CVE 2018-13379, and security researchers are reporting active exploitation [7]. Upgrading to the latest version will remove the vulnerabilities.

Resetting Credentials

If a malicious actor previously exploited the vulnerability to collect legitimate credentials, these credentials would still be valid after patching. NSA recommends resetting credentials after a vulnerable VPN device is upgraded and before it is reconnected to the external network:

- Immediately update VPN user, administrator, and service account credentials.
- Immediately revoke and generate new VPN server keys and certificates. This may require redistributing VPN connection information to users.
- If compromise is suspected, review accounts to ensure no new accounts were created by adversaries.

Public-facing VPN Deployment & Hardening Controls

Once credentials have been reset, the following actions will further harden the VPN:

- Discourage use of proprietary SSLVPN/TLSVPN protocols. Transition SSLVPN/TLSVPN deployments to either IETF standard-conformant TLS - for single application use cases, or to IKE/IPsec VPNs, preferring the evaluated TLS software applications and IPSec VPN gateways/clients listed on the National Information Assurance Partnership (NIAP) Product Compliant List (PCL).
- If continuing to use SSLVPNs, require public-facing VPN web applications to only use strong TLS (i.e. TLS 1.2 or later) for network traffic encryption, certificate-based authentication, and integrity.
- Discourage the use of self-signed and wild card certificates for public-facing VPN web applications, and periodically rotate and update legitimate certificates.
- Attackers that manage to compromise administrator credentials could try to authenticate into web management interfaces and maliciously perform privileged operations. Do not allow VPN administrators to login to the management interface via the public-facing VPN web application; instead, restrict administrative access to dedicated internal management networks. If an attacker tries to use administrator credentials to access the public-facing VPN web application, the access attempt should be denied, even if the credentials were correct.
- Require mutual TLS authentication for remote TLS clients attempting to access the VPN. Solutions should be set to drop connections with clients that do not present valid, trusted TLS certificates.
- Use multi-factor authentication to prevent attackers from authenticating with compromised passwords by requiring a second authentication factor [8].
- Enable logging to record and track VPN user activity, including authentication and access attempts, configuration changes, and network traffic metadata (e.g. IP addresses, ports, protocols, and sessions).
- Some VPN vendors may provide features that help enhance web application security to prevent attacks against public-facing VPN web applications, such as malicious re-use of users' previous, outdated sessions to bypass authentication. Enable these features when possible. Pulse Secure provides session security guidance in their security configuration best practices document [9]. Palo Alto provides authentication session timeout settings in their documentation [10]. Review Fortinet documentation on authentication timeout settings to prevent session spoofing [11].
- Deploy a web application firewall that can detect and block web application attacks, like specially-crafted HTTP requests containing malformed strings that exploit VPN vulnerabilities, in front of the VPN web application.
- In cases where web traffic is encrypted, monitoring and detecting web application attacks may require tools that can inspect the encrypted traffic to see the underlying web plaintext.
- Constantly follow VPN vendors to look for the latest updates, and apply the updates immediately to patch vulnerabilities and fix bugs.
- Disable services (e.g. file share services) that could be leveraged for post-compromise activities like lateral movement, data exfiltration, and command and control.

- Continuously monitor and conduct analytics on all logs to look for unauthorized access, malicious configuration changes, anomalous network traffic, and other indicators of compromise [12].

Works Cited

[1] "Active exploitation of VPN vulnerabilities." Canadian Centre for Cyber Security, 28 August 2019. [Online] Available: https://cyber.gc.ca/en/alerts/active-exploitation-vpn-vulnerabilities

[2] O. Tsai and M. Chang, "Attacking SSL VPN – Part 3: The Golden Pulse Secure SSL VPN RCE Chain, with Twitter as Case Study!" DEVCORE Security Consulting, 02 September 2019. [Online] Available: https://devco.re/blog/2019/09/02/attacking-ssl-vpn-part-3-the golden-Pulse-Secure-ssl-vpn-rce-chain-with-Twitter-as-case-study/

[3] "SA44101 – 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX." Pulse Secure, 20 August 2019. [Online] Available: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

[4] "Multiple Vulnerabilities in Pulse Secure VPN." Carnegie Mellon University Software Engineering Institute, CERT Coordination Center, 16 October 2019. [Online] Available: https://www.kb.cert.org/vuls/id/927237

[5] "CVE-2019-1579." Common Vulnerabilities and Exposures. [Online database entry] Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1579

[6] O. Tsai and M. Chang. "Attacking SSL VPN – Part 1: PreAuth on Palo Alto GlobalProtect, with Uber as Case Study!" DEVCORE Security Consulting, 17 July 2019. [Online] Available: https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study/

[7] Z. Zorz. "Attackers are targeting vulnerable Fortigate and Pulse Secure SSL VPNs." Help Net Security, 26 August 2019. [Online] Available: https://www.helpnetsecurity.com/2019/08/26/vulnerable-fortigate-pulse-secure-ssl-vpn/

[8] "Transition to Multi-factor Authentication." National Security Agency, August 2019. [Online] Available: https://media.defense.gov/2019/Sep/09/2002180346/-1/-1/0/TRANSITION TO MULTI-FACTOR AUTHENTICATION.PDF

[9] "KB29805 – Pulse Connect Secure: Security configuration best practices." Pulse Secure, 02 July 2019. [Online] Available: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB29805

[10] "HOW TO CONFIGURE AUTHENTICATION IDLE TIMEOUT." Palo Alto Networks, 05 August 2019. [Online] Available: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm29CAC

[11] "Configuring authenticated access." Fortinet. [Online] Available: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Auth_Access.htm

[12] "Continuously Hunt for Network Intrusions." National Security Agency, August 2019. [Online] Available: https://media.defense.gov/2019/Sep/09/2002180360/-1/-1/0/CONTINOUSLY HUNT FOR NETWORK INTRUSIONS.PDF

Disclaimer of Endorsement

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov