REN-ISAC

August 28, 2019

REN-ISAC Security Advisory

Subject: Important Vulnerabilities in Multiple SSL VPN Products
Sharing Guideline: PUBLIC (TLP:WHITE)

Executive Summary

Multiple vendors have announced high-severity vulnerabilities in SSL VPN products that can result in information disclosure and remote code injection or execution. In some cases, public exploit code for these vulnerabilities has been released, and recent scanning activity has been observed [1, 2].

Given the security functions these products serve and their typical exposure on the network, REN-ISAC encourages operators to evaluate the status of their appliances and apply vendor updates as soon as possible.

Vulnerability Impact

Vulnerability impact differs by product and product version; however, in many cases, these vulnerabilities may be leveraged individually or in combination to

- Disclose sensitive session details, such as plaintext usernames and passwords stored on the appliance (pre-authentication)
- Result in remote code execution on the VPN appliance
- Result in remote command injection on the connected VPN client endpoints

Recommended Remediation

Fortinet FortiGuard

- Apply vendor updates
- Change passwords for any end user, administrator, or service accounts local to the appliance

Palo Alto Networks

- Apply vendor updates

Pulse Secure

- Apply vendor updates
- Change passwords for any end user, administrator, or service accounts local to the appliance (*Note: third-party reports indicate that credentials for Active Directory users could also be exposed; although, this has not been confirmed. [6])*

REN-ISAC

August 28, 2019

Vulnerability Details

Fortinet FortiGuard

CVE	Description	Vendor Advisory	Affected Versions
CVE-2018-13379	FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests	https://fortiguard.com/psirt/FG-IR-18-384	FortiOS 5.6.3 - 5.6.7, 6.0.0 - 6.0.4
CVE-2018-13382	Unauthenticated SSL VPN user's password modification	https://fortiguard.com/psirt/FG-IR-18-389	FortiOS 5.4.1- 5.4.10, 5.6.0 to 5.6.8, 6.0.0 - 6.0.4
CVE-2018-13383	SSL VPN buffer overrun when parsing javascript href content	https://fortiguard.com/psirt/FG-IR-18-388	FortiOS 5.6.10 and below, 6.0.0 - 6.0.4

Palo Alto Networks

CVE	Description	Vendor Advisory	Affected Versions
CVE-2019-1579	Remote Code Execution in GlobalProtect Portal/Gateway Interface	https://securityadvisories.paloaltonetworks.com/Home/Detail/158	PAN-OS 7.1.18 and earlier, 8.0.11-h1 and earlier, 8.1.2 and earlier releases

Pulse Secure

Vendor Advisory:	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/	
CVE	**Description**	**Affected Versions**
CVE-2019-11510	Unauthenticated arbitrary file reading vulnerability	Pulse Connect Secure 8.2RX, 8.3RX, 9.0RX
CVE-2019-11539	Admin web interface allows an authenticated attacker to inject and execute commands	Pulse Connect Secure 8.1RX, 8.2RX, 8.3RX, 9.0RX
CVE-2019-11509	Authenticated attacker via the admin web interface can exploit this issue to execute arbitrary code on the Pulse Secure appliance	Pulse Connect Secure 8.1RX, 8.2RX, 8.3RX, 9.0RX

Additional Resources

1. https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/
2. https://opensecurity.global/forums/topic/181-fortinet-ssl-vpn-vulnerability-from-may-2019-being-exploited-in-wild/
3. https://www.us-cert.gov/ncas/current-activity/2019/07/26/vulnerabilities-multiple-vpn-applications
4. https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf
5. https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/
6. https://opensecurity.global/forums/topic/184-pulse-secure-ssl-vpn-vulnerability-being-exploited-in-wild/?do=findComment&comment=887