CERT-EU Security Advisory 2019-017

Vulnerabilities in Popular VPNs

August 26, 2019 — v1.0

History:

- *26/08/2019 — v1.0: Initial publication*

Summary

Several vulnerabilities impacting popular VPNs (by Palo Alto, Pulse Security, and Fortinet) have been recently seen being exploited in the wild. In most severe case, the vulnerabilities allow for remote code execution. Although the vulnerabilities have been reported to the vendors much earlier, and they have since been fixed, many services remain unpatched. Recently, significant amount of scanning and exploitation could be seen in the wild. Hence, it is imperative to patch as soon as possible.

Technical Details

Fortinet VPN

The following vulnerabilities were discovered:

- Pre-auth arbitrary file reading (CVE-2018-13379) [1],
- Pre-auth XSS (CVE-2018-13380) [2],
- Pre-auth heap overflow (CVE-2018-13381) [3].

By combining them, as explained in [4], it is possible to gain reverse shell.

Pulse VPN

The vulnerabilities were discovered and have been resolved in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS). This includes an authentication by-pass vulnerability that can allow an unauthenticated user to perform a remote arbitrary file access on the Pulse Connect Secure gateway, a remote code execution vulnerability that can allow an authenticated administrator to perform remote code execution on Pulse Connect Secure and Pulse Policy Secure gateways. Many of these vulnerabilities have a critical CVSS score and pose significant risk [5]. These vulnerabilities are now seen being exploited in the wild [6].

Palo Alto VPN

A remote code execution (RCE) vulnerability has been found in Palo Alto GlobalProtect portal and GlobalProtect Gateway interface products (CVE-2019-1579) [7]. Successful exploitation of this issue allows an unauthenticated attacker to execute arbitrary code.

Products Affected

Fortinet

- FortiOS 6.0.0 to 6.0.4
- FortiOS 5.6.0 to 5.6.7
- FortiOS 5.4 and below

Pulse Secure

Most versions are affected by at least some of these vulnerabilites. For details – please consult [5].

Palo Alto

PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier releases. PAN-OS 9.0 is not affected.

Recommendations

Fortinet

- Upgrade to FortiOS 5.6.8, 6.0.5, 6.2.0 or above
- If not possible to upgrade, a possible workaround is to disable the SSL-VPN web portal service [1, 2, 3]

Pulse Secure

- Upgrade to the following versions depending on the release used:
  - Pulse Connect Secure 9.0R3.4 and 9.0R4
  - Pulse Connect Secure 8.3R7.1
  - Pulse Connect Secure 8.2R12.1
  - Pulse Connect Secure 8.1R15.1
  - Pulse Policy Secure 9.0R3.2 and 9.0R4
  - Pulse Policy Secure 5.4R7.1

  - Pulse Policy Secure 5.3R12.1
  - Pulse Policy Secure 5.2R12.1
  - Pulse Policy Secure 5.1R15.1

Palo Alto

Upgrade to PAN-OS 7.1.19 and later, PAN-OS 8.0.12 and later, and PAN-OS 8.1.3 and later releases.

References

[1] https://fortiguard.com/psirt/FG-IR-18-384

[2] https://fortiguard.com/psirt/FG-IR-18-383

[3] https://fortiguard.com/psirt/FG-IR-18-387

[4] https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/

[5] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

[6] https://opensecurity.global/forums/topic/184-pulse-secure-ssl-vpn-vulnerability-being-exploited-in-wild/

[7] https://securityadvisories.paloaltonetworks.com/Home/Detail/158