Security Advisory 2022-061

Reflected Amplification DoS Vulnerability in PAN-OS

August 11, 2022 — v1.0

TLP:WHITE

History:

- *11/08/2022 — v1.0 – Initial publication*

Summary

On August 10, 2022, PaloAlto released a security advisory regarding a Denial-of-Service (DoS) vulnerability affecting PAN-OS [1]. Exploiting this vulnerability, a network-based attacker would be able to obfuscate its identity and implicate the vulnerable firewall as the source of an attack.

While some software updates are not yet available, some mitigation and workarounds are available and should be applied as soon as possible.

Technical Details

The vulnerability is identified as `CVE-2022-0028` and has a severity score of 8.6 out of 10. It is due to an insufficient monitoring or control of transmitted network traffic volume, so that an actor can cause the software to transmit more traffic than should be allowed for that actor. Once exploited, an attacker might be able to conduct a reflected and amplified TCP denial-of-service (RDoS) attack against an attacker-specified target, obfuscating its identity and implicating the vulnerable firewall as the source of the attack.

Affected Products

The following product versions are affected:

- PAN-OS 8.1 with version < 8.1.23-h1 (Patch ETA: August 15, 2022)
- PAN-OS 9.0 with version < 9.0.16-h3 (Patch ETA: week of August 15, 2022)
- PAN-OS 9.1 with version < 9.1.14-h4 (Patch ETA: week of August 15, 2022)
- PAN-OS 10.0 with version < 10.0.11-h1 (Patch ETA: week of August 15, 2022)
- PAN-OS 10.1 with version < 10.1.6-h6 (Patch Available)
- PAN-OS 10.2 with version < 10.2.2-h2 (Patch ETA: week of August 15, 2022)

To be vulnerable, the firewall should be configured with a URL filtering profile with one or more blocked categories assigned to a security rule with a source zone that has an external

facing interface for this issue to be misused by an external attacker. This configuration is not typical for URL filtering and is likely unintended by the administrator.

This issue is applicable to PA-Series (hardware), VM-Series (virtual), and CN-Series (container) firewalls only when all three of the following conditions are true:

- The security policy on the firewall that allows traffic to pass from Zone A to Zone B includes a URL filtering profile with one or more blocked categories;
- Packet-based attack protection is not enabled in a Zone Protection profile for Zone A including both (Packet Based Attack Protection > TCP Drop > TCP Syn With Data) and (Packet Based Attack Protection > TCP Drop > Strip TCP Options > TCP Fast Open);
- Flood protection through SYN cookies is not enabled in a Zone Protection profile for Zone A (Flood Protection > SYN > Action > SYN Cookie) with an activation threshold of 0 connections.

Recommendations

CERT-EU strongly recommends applying the software updates as soon as they are available. While waiting for the software updates to be released, CERT-EU recommends applying the workarounds and mitigation listed below.

Workarounds and Mitigation

If a URL filtering policy with one or more blocked categories assigned to a security rule with a source zone that has an external facing interface is enabled, removing this configuration will prevent this issue from being exploited by remote attackers to conduct reflected DoS.

Also, enabling one of two following zone protection mitigation on all Security zones with an assigned Security policy that includes a URL filtering profile will prevent denial-of-service (DoS) attacks resulting from this issue from all sources (it is not necessary nor advantageous to apply both the attack and flood protections):

1. Packet-based attack protection including both (Packet Based Attack Protection > TCP Drop > TCP SYN with Data) and (Packet Based Attack Protection > TCP Drop > Strip TCP Options > TCP Fast Open) [2];
2. Flood protection (Flood Protection > SYN > Action > SYN Cookie) with an activation threshold of 0 connections [3].

Note: None of these protections should be enabled if using Aporeto software; instead, wait for and install a fixed version of PAN-OS software.

References

[1] https://security.paloaltonetworks.com/CVE-2022-0028

[2] https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-based-attack-protection

[3] https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection