Alert Bulletin

Bulletin N.:
Publication Date: 28/12/2024
Subject: Alert 2024-73 DoS vulnerability in Palo Alto PAN-OS
Traffic Light Protocol (TLP): White

Affected product(s):

- PAN-OS 11.1 (11.1.2-h16, 11.1.3-h13, 11.1.4-h7, and 11.1.5)
- PAN-OS 10.2 (10.2.8-h19, 10.2.9-h19, 10.2.10-h12, 10.2.11-h10, 10.2.12-h4, 10.2.13-h2, and 10.2.14)
- PAN-OS 10.1 (10.1.14-h8 and 10.1.15)
- PAN-OS 10.2.9-h19 and 10.2.10-h12 (only applicable to Prisma Access)
- PAN-OS 11.0 (not patched due to reaching End of Life status on November 17, 2024)

Description

A high-severity vulnerability affecting Palo Alto's PAN-OS software has been disclosed that could cause a denial of service (DoS) condition on affected devices. The flaw was identified as CVE-2024-3393 with a CVSS score of 8.7.

According to comments made by Palo Alto technicians, the DoS vulnerability affects the DNS security feature of the PAN-OS software, allowing an unauthenticated attacker to send a malicious packet through the firewall's data plane, causing it to restart. For the vulnerability to affect the firewall, DNS security logging must be enabled.

Mitigation

For unmanaged NGFWs, Panorama-managed NGFWs, or Panorama-managed Prisma Access:

As a workaround and mitigations for unmanaged firewalls or those managed by Palo Alto Panorama, customers have the option to set Log Severity to "none" for all DNS Security categories configured for each Anti-Spyware profile by navigating to

Objects > Security Profiles > Anti-spyware > (select a profile) > DNS Policies > DNS Security.

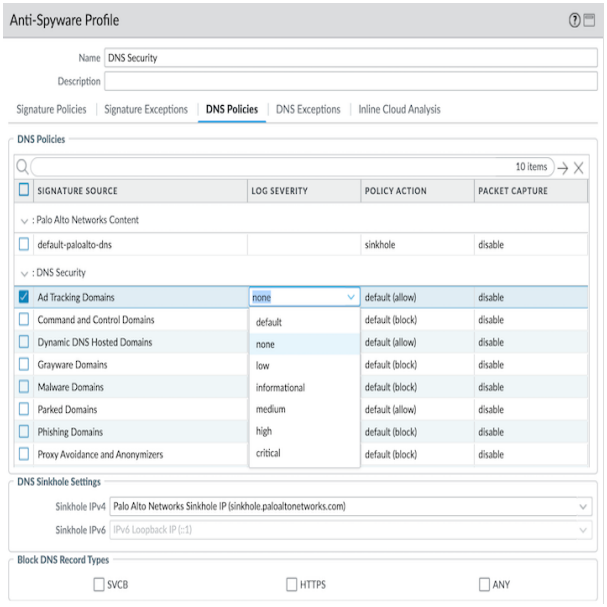
Alert Bulletin

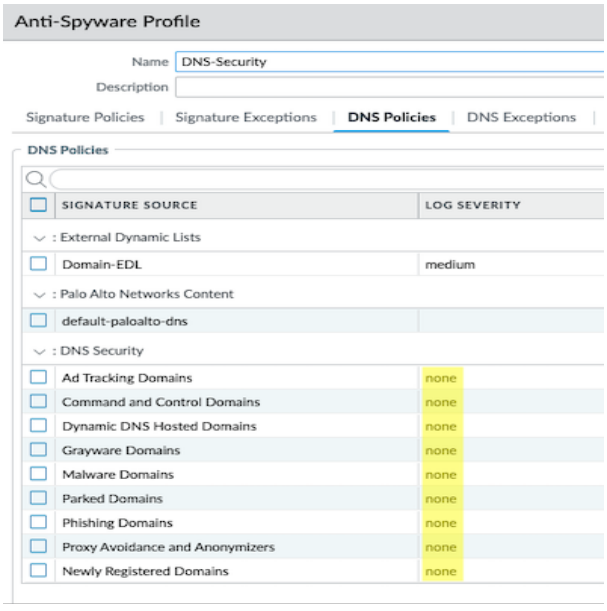
Bulletin N.:

Publication Date: 28/12/2024

Subject: Alert 2024-73 DoS vulnerability in Palo Alto PAN-OS

Traffic Light Protocol (TLP): White





Remember to revert the Log Severity settings once the fixes are applied.

Alert Bulletin

Bulletin N.:
Publication Date: 28/12/2024
Subject: Alert 2024-73 DoS vulnerability in Palo Alto PAN-OS
Traffic Light Protocol (TLP): White

For NGFW managed by Strata Cloud Manager (SCM):

For firewalls managed by Strata Cloud Manager (SCM), users can follow the steps above to disable DNS security logging directly on each device or on all devices by opening a support case.

For Prisma Access managed by Strata Cloud Manager (SCM):

For Prisma Access tenants managed by SCM, it is recommended to open a support case to disable logging until an upgrade is performed.

Solution

According to the Palo Alto team, this issue has been fixed in PAN-OS 10.1.14-h8, PAN-OS 10.2.10-h12, PAN-OS 11.1.5, PAN-OS 11.2.3, and all later PAN-OS versions.

For PAN-OS 11.0 which reached End of Life (EOL) on November 17, 2024, there will be no update that addresses this vulnerability.

An update guide can be found at the following link:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/pan-os-software-updates

Prisma Access customers using DNS Security with affected PAN-OS versions should apply one of the workarounds provided below:

For affected customers, upgrades will occur in two phases over the weekends of January 3 and January 10. By opening a support case, you can request an expedited upgrade of Prisma Access to the latest version of PAN-OS.

Additionally, to provide the smoothest upgrade path, fixes have been made available for other commonly deployed and preferred TAC maintenance releases.

Additional PAN-OS 11.1 releases with the fix:

Alert Bulletin

Bulletin N.:
Publication Date: 28/12/2024
Subject: Alert 2024-73 DoS vulnerability in Palo Alto PAN-OS
Traffic Light Protocol (TLP): White

- 11.1.2-h16 (available)
- 11.1.3-h13 (available)
- 11.1.4-h7 (available)
- 11.1.5 (available)

Additional PAN-OS 10.2 releases with fix:

- 10.2.8-h19 (estimated arrival time: 31 December)
- 10.2.9-h19 (available)
- 10.2.10-h12 (available)
- 10.2.11-h10 (estimated departure time: 31 December)
- 10.2.12-h4 (estimated arrival date: 31 December)
- 10.2.13-h2 (estimated arrival date: 31 December)
- 10.2.14 (ETA: end of January)

Additional PAN-OS 10.1 releases with fix:

- 10.1.14-h8 (available)
- 10.1.15 (ETA: end of January)

Additional PAN-OS releases with fixes applicable only to Prisma Access:

- 10.2.9-h19 (available)
- 10.2.10-h12 (available)

Additional information:

- https://security.paloaltonetworks.com/CVE-2024-3393
- https://thehackernews.com/2024/12/palo-alto-releases-patch-for-pan-os-dos.html