



BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-73

Fecha de publicación: 27/12/2024

Tema: Vulnerabilidad crítica en PAN-OS de Palo Alto

Traffic Light Protocol (TLP): White



Boletín de Alerta



Producto(s) afectado(s):

- PAN-OS 11.1 (11.1.2-h16, 11.1.3-h13, 11.1.4-h7 y 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 y 10.2.14)
- PAN-OS 10.1 (10.1.14-h8 y 10.1.15)
- PAN-OS 10.2.9-h19 y 10.2.10-h12 (solo aplicable a Prisma Access)
- PAN-OS 11.0 (no se ha corregido debido a que alcanzó el estado de fin de vida útil el 17 de noviembre de 2024)

Descripción

Se ha publicado una vulnerabilidad de criticidad alta que afecta al software PAN-OS de Palo Alto y que podría provocar una condición de denegación de servicio (DoS) en dispositivos afectados, la falla, fue identificada como CVE-2024-3393 con puntuación CVSS 8.7.

De acuerdo a comentarios hechos por técnicos de Palo Alto, la vulnerabilidad de DoS afecta a la función de seguridad DNS del software PAN-OS permitiendo a un atacante no autenticado enviar un paquete malicioso a través del plano de datos del firewall haciendo que este se reinicie. Para que la vulnerabilidad afecta al firewall es necesario tener habilitado el registro de seguridad DNS.

Mitigación

NGFW no administrados, NGFW administrados por Panorama o Prisma Access administrado por Panorama:

Como solución alternativa y mitigaciones para firewalls no administrados o aquellos administrados por Panorama de Palo Alto, los clientes tienen la opción de configurar la

Gravedad del registro en "ninguna" para todas las categorías de Seguridad DNS configuradas para cada [perfil Anti-Spyware](#) navegando a Objetos > Perfiles de seguridad > Anti-spyware > (seleccione un perfil) > Políticas DNS > Seguridad DNS.

(En inglés sería: Objects → Security Profiles → Anti-spyware → (select a profile) → DNS Policies → DNS Security.)

Anti-Spyware Profile ? ☰

Name:

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

DNS Policies

10 items → X

<input type="checkbox"/>	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
- Palo Alto Networks Content				
<input type="checkbox"/>	default-paloalto-dns		sinkhole	disable
- DNS Security				
<input checked="" type="checkbox"/>	Ad Tracking Domains	none	default (allow)	disable
<input type="checkbox"/>	Command and Control Domains	default	default (block)	disable
<input type="checkbox"/>	Dynamic DNS Hosted Domains	none	default (allow)	disable
<input type="checkbox"/>	Grayware Domains	low	default (block)	disable
<input type="checkbox"/>	Malware Domains	informational	default (block)	disable
<input type="checkbox"/>	Parked Domains	medium	default (allow)	disable
<input type="checkbox"/>	Phishing Domains	high	default (block)	disable
<input type="checkbox"/>	Proxy Avoidance and Anonymizers	critical	default (block)	disable

DNS Sinkhole Settings

Sinkhole IPv4:

Sinkhole IPv6:

Block DNS Record Types

SVCB HTTPS ANY

Anti-Spyware Profile

Name:

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions

DNS Policies

<input type="checkbox"/>	SIGNATURE SOURCE	LOG SEVERITY
- External Dynamic Lists		
<input type="checkbox"/>	Domain-EDL	medium
- Palo Alto Networks Content		
<input type="checkbox"/>	default-paloalto-dns	
- DNS Security		
<input type="checkbox"/>	Ad Tracking Domains	none
<input type="checkbox"/>	Command and Control Domains	none
<input type="checkbox"/>	Dynamic DNS Hosted Domains	none
<input type="checkbox"/>	Grayware Domains	none
<input type="checkbox"/>	Malware Domains	none
<input type="checkbox"/>	Parked Domains	none
<input type="checkbox"/>	Phishing Domains	none
<input type="checkbox"/>	Proxy Avoidance and Anonymizers	none
<input type="checkbox"/>	Newly Registered Domains	none

Recuerde revertir la configuración de gravedad del registro una vez que se apliquen las correcciones.

NGFW administrado por Strata Cloud Manager (SCM):

En el caso de los firewalls administrados por Strata Cloud Manager (SCM), los usuarios pueden seguir los pasos anteriores para desactivar el registro de seguridad de DNS directamente en cada dispositivo o en todos ellos abriendo un caso de soporte.

Prisma Access administrado por Strata Cloud Manager (SCM):

En el caso de los inquilinos de Prisma Access administrados por SCM, se recomienda abrir un caso de soporte para desactivar el registro hasta que se realice una actualización.

Solución

Según el equipo de Palo Alto, este problema se solucionó en PAN-OS 10.1.14-h8, PAN-OS 10.2.10-h12, PAN-OS 11.1.5, PAN-OS 11.2.3 y todas las versiones posteriores de PAN-OS. Para PAN-OS 11.0 la cual llegó al final de su vida útil (EOL) el 17 de noviembre de 2024, no habrá actualización que solucione dicha vulnerabilidad.

Puede encontrar un guía para actualización en el siguiente enlace:

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

Los clientes de Prisma Access que utilicen DNS Security con versiones de PAN-OS afectadas deben aplicar una de las soluciones alternativas que se ofrecen a continuación:

Las actualizaciones se realizarán en dos fases para los clientes afectados, durante los fines de semana del 3 y el 10 de enero. Puede solicitar una actualización acelerada de Prisma Access a la última versión de PAN-OS abriendo un [caso de soporte](#).

Además, para brindar la ruta de actualización más fluida, pusieron a disposición correcciones para otras versiones de mantenimiento preferidas de TAC e implementadas comúnmente.

Versiónes adicionales de PAN-OS 11.1 con la corrección :

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

Versiónes adicionales de PAN-OS 10.2 con la corrección :

- 10.2.8-h19 (hora estimada de llegada: 31 de diciembre)
- 10.2.9-h19 (disponible)
- 10.2.10-h12 (disponible)
- 10.2.11-h10 (hora estimada de salida: 31 de diciembre)
- 10.2.12-h4 (fecha estimada de llegada: 31 de diciembre)
- 10.2.13-h2 (fecha estimada de llegada: 31 de diciembre)
- 10.2.14 (ETA: finales de enero)

Versiones adicionales de PAN-OS 10.1 con la corrección :

- 10.1.14-h8 (disponible)
- 10.1.15 (ETA: finales de enero)

Versiones adicionales de PAN-OS con correcciones aplicables únicamente a Prisma Access:

- 10.2.9-h19 (disponible)
- 10.2.10-h12 (disponible)

Información adicional:

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



BEACON LAB

C S I R T

CYBOLT 
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com

