BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-62
Fecha de publicación: 19/11/2024
Tema: Vulnerabilidades críticas en firewalls de Palo Alto Networks (PAN-OS)
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Firewalls de próxima generación (NGFW) de Palo Alto Networks con versiones de PAN-OS 10.2, 11.0, 11.1 y 11.2.

Descripción

Se han identificado dos vulnerabilidades críticas en los firewalls de **próxima generación de Palo Alto Networks (NGFW),** designadas como **CVE-2024-0012** y **CVE-2024-9474**. La primera, CVE-2024-0012, es una vulnerabilidad de omisión de autenticación en la interfaz web de gestión de PAN-OS, que permite a atacantes remotos obtener privilegios de administrador sin necesidad de autenticación ni interacción del usuario. La segunda, CVE-2024-9474, es una vulnerabilidad de escalada de privilegios que permite a administradores malintencionados de PAN-OS ejecutar acciones en el firewall con privilegios de root.

Palo Alto Networks ha observado actividad maliciosa que explota estas vulnerabilidades en un número limitado de interfaces web de gestión expuestas a tráfico de internet. La explotación exitosa de estas fallas podría comprometer gravemente la seguridad de la infraestructura de red de las organizaciones.

Según datos de **Shodan**, se han identificado más de 11,000 direcciones IP que ejecutan interfaces de administración PAN-OS de Palo Alto expuestas en línea. El siguiente mapa global proporcionado por Netlas.io, muestra que los dispositivos más vulnerables se encuentran en Estados Unidos, UK, Canada y **México**, encontrando en este último 519 dispositivos.

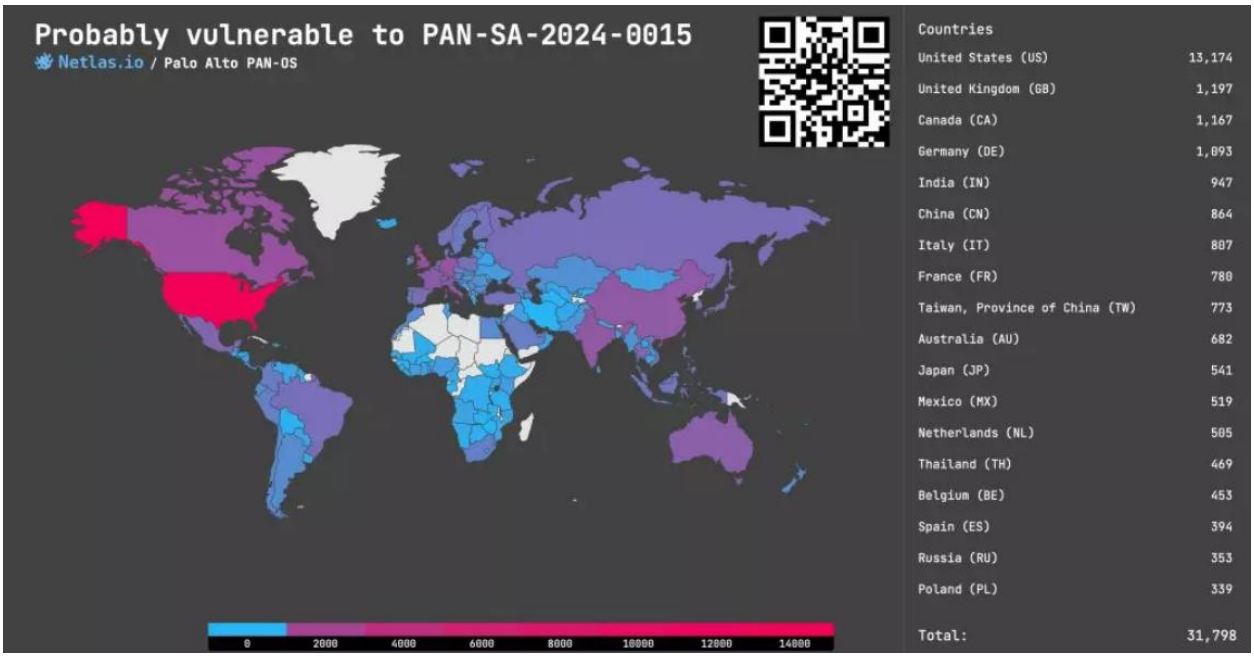

Figura 1. Captura de pantalla de Netlas.io

Es importante destacar que los servicios Cloud NGFW y Prisma Access no se ven afectados por la vulnerabilidad CVE-2024-9474.

Solución

Palo Alto Networks ha publicado actualizaciones de seguridad para abordar estas vulnerabilidades. Se recomienda a todos los usuarios actualizar sus dispositivos a las versiones corregidas de PAN-OS para mitigar estos riesgos y evitar compromisos en los sistemas.

Palo Alto Networks insta a los administradores a:

1. Revisar las configuraciones de la interfaz de gestión: Asegúrese de que el acceso esté limitado a redes internas confiables.
2. Verificar activos en el portal de soporte:
    - Acceda a la sección “Assets” en el portal de soporte.
    - Identifique dispositivos etiquetados con “PAN-SA-2024-0015” en la lista de remediación requerida.

Información adicional:

- Palo Alto Networks advierte sobre vulnerabilidad en la interfaz de gestión de PAN-OS - Devel Group
- Threat Brief: Operation Lunar Peek, Activity Related to CVE-2024-0012
- Palo Alto Networks parchea dos cortafuegos de día cero utilizados en los ataques

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com