Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PALO ALTO NETWORKS ADVIERTE SOBRE VULNERABILIDAD EN LA INTERFAZ DE GESTIÓN DE PAN-OS

13 / 11 / 2024

CONTENIDO

INTRODUCCIÓN

Palo Alto Networks emitió una alerta sobre una posible vulnerabilidad de ejecución remota de código (RCE) en la interfaz de gestión de PAN-OS, que podría afectar dispositivos accesibles desde Internet. Aunque no hay evidencia de explotación activa, se identificaron 31,798 dispositivos potencialmente vulnerables a nivel global, siendo Estados Unidos, Reino Unido y Canadá los más afectados. La empresa recomienda limitar el acceso a la interfaz de gestión solo a IPs internas confiables, verificar configuraciones a través del portal de soporte y seguir las mejores prácticas para proteger estos dispositivos. Palo Alto Networks continúa monitoreando la situación y actualizando la información para mitigar riesgos.

PALO ALTO NETWORKS ADVIERTE SOBRE VULNERABILIDAD EN LA INTERFAZ DE GESTIÓN DE PAN-OS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_11_13_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/11/2024
Es día cero (0 day):	No

RESUMEN

Palo Alto Networks emitió recientemente el boletín informativo PAN-SA-2024-0015, alertando a los usuarios sobre una posible vulnerabilidad de ejecución remota de código (RCE) en la interfaz de gestión de PAN-OS. Aunque no se conocen los detalles específicos de la vulnerabilidad, la empresa recomienda medidas inmediatas para mitigar riesgos potenciales, especialmente en dispositivos con interfaces de gestión accesibles desde Internet.

Descripción del problema

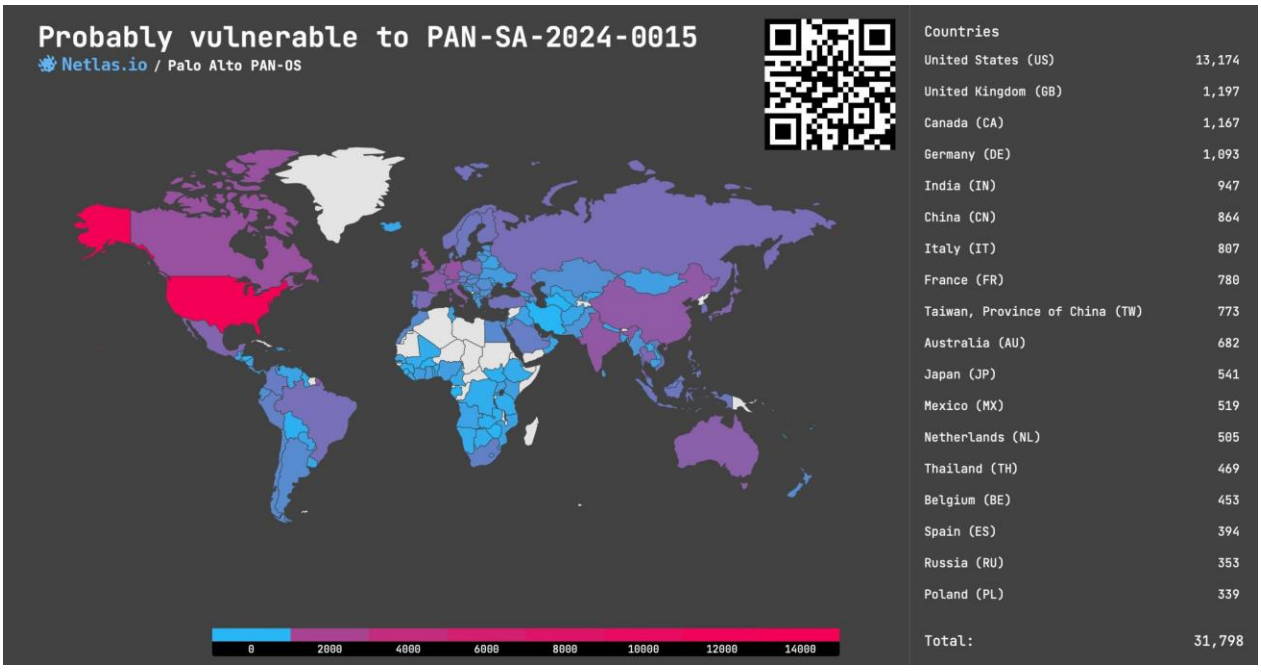
La alerta surge tras una reclamación externa sobre una posible vulnerabilidad en la interfaz de gestión de PAN-OS. A la fecha, no hay evidencia concreta de explotación activa ni indicadores de compromiso relacionados con esta vulnerabilidad.

Palo Alto Networks subraya la importancia de seguir las prácticas recomendadas para proteger el acceso a la interfaz de gestión, limitando su disponibilidad únicamente a IPs internas confiables y restringiendo su acceso desde Internet.

Impacto global

Un mapa global proporcionado por Netlas.io muestra la distribución de los dispositivos vulnerables por país. Algunos de los países más afectados son:

- Estados Unidos: 13,174 dispositivos.
- Reino Unido: 1,197 dispositivos.
- Canadá: 1,167 dispositivos.
- México: 519 dispositivos.
- España: 394 dispositivos.



Este panorama subraya la importancia de que las organizaciones en todas las regiones evalúen sus configuraciones actuales y apliquen las recomendaciones necesarias.

Medidas recomendadas

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.**
3. **Consultar guías de mejores prácticas:** Acceda a la página oficial de Palo Alto Networks para obtener detalles adicionales sobre cómo proteger la interfaz de gestión: Cómo asegurar el acceso de gestión de sus dispositivos.

¿Qué esperar?

Aunque no se han observado señales de explotación activa, Palo Alto Networks continúa monitoreando la situación y promete actualizaciones oportunas en caso de cualquier cambio.

NOTICIA COMPLETA

https://devel.group/blog/palo-alto-networks-advierte-sobre-vulnerabilidad-en-la-interfaz-de-gestion-de-pan-os/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente