Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MÁS DE 2,000 FIREWALLS DE PALO ALTO NETWORKS COMPROMETIDOS MEDIANTE VULNERABILIDADES CRÍTICAS

21 / 11 / 2024

CONTENIDO

INTRODUCCIÓN

En las últimas semanas, una campaña de ciberataques ha comprometido más de 2,000 firewalls de Palo Alto Networks, explotando dos vulnerabilidades críticas recientemente parcheadas. Estas fallas, que permiten a los atacantes tomar control total de los dispositivos mediante omisión de autenticación y escalada de privilegios, destacan la urgencia de aplicar medidas de seguridad proactivas. A pesar de los esfuerzos de Palo Alto Networks por mitigar el impacto, la rápida explotación de estas vulnerabilidades evidencia el sofisticado nivel de las amenazas actuales y la necesidad de reforzar la protección en infraestructuras críticas.

MÁS DE 2,000 FIREWALLS DE PALO ALTO NETWORKS COMPROMETIDOS MEDIANTE VULNERABILIDADES CRÍTICAS

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

ID de alerta:	DSOC-CERT_2024_11_21_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	21/11/2024
Es día cero (0 day):	No

RESUMEN

En una reciente campaña de ciberataques, más de 2,000 firewalls de Palo Alto Networks han sido comprometidos, aprovechando dos vulnerabilidades críticas recientemente parcheadas. Estas fallas afectan la interfaz de gestión web de PAN-OS, el sistema operativo que potencia los dispositivos de seguridad de la empresa.

Detalles Técnicos de las Vulnerabilidades

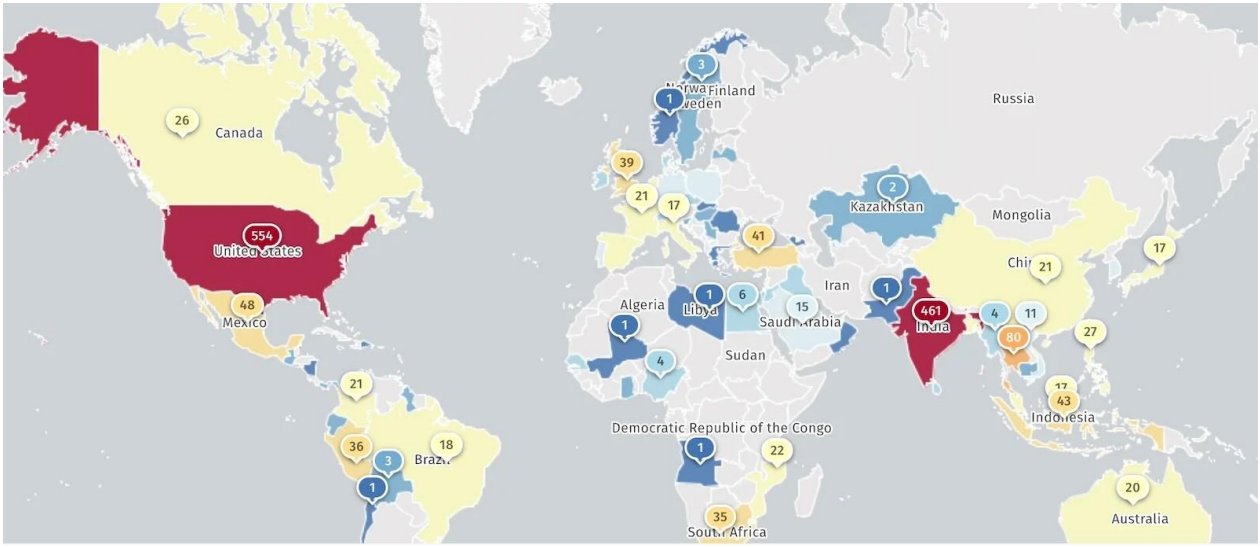
1. **CVE-2024-0012:** Esta vulnerabilidad fue alertada por primera vez el 8 de noviembre, clasificada como una falla crítica que podría permitir la ejecución remota de código (RCE).
2. **CVE-2024-9474:** Divulgada el lunes 18 de noviembre, facilita a los atacantes tomar control total del sistema al ejecutar comandos privilegiados.

Ambas vulnerabilidades están siendo utilizadas de manera conjunta, lo que aumenta el impacto de los ataques. Según Unit 42 de Palo Alto Networks, se sospecha con confianza moderada a alta que ya existe un exploit funcional público que permite encadenar estas dos fallas.

Impacto Global

Aunque Palo Alto Networks asegura que solo un "número muy limitado" de dispositivos están afectados, el monitoreo independiente realizado por Shadowserver señala que existen 2,700 dispositivos PAN-OS vulnerables a nivel global, y de ellos, aproximadamente 2,000 ya han sido hackeados.

La mayoría de los ataques detectados se originan desde direcciones IP asociadas con servicios de VPN anónimos, lo que dificulta rastrear a los atacantes.



Recomendaciones Críticas

Palo Alto Networks ha emitido directrices claras para mitigar los riesgos asociados con estas vulnerabilidades:

1. **Restringir Acceso:** Configurar las interfaces de gestión web de PAN-OS para que solo sean accesibles desde direcciones IP internas de confianza.
2. **Actualizar Inmediatamente:** Aplicar los parches de seguridad lanzados para CVE-2024-0012 y CVE-2024-9474.
3. **Seguir Buenas Prácticas:** Revisar las guías de despliegue seguro proporcionadas por la empresa.

Implicaciones para la Seguridad Empresarial

Estos incidentes subrayan la importancia de la gestión proactiva de vulnerabilidades en dispositivos críticos de seguridad. Los firewalls son el primer nivel de defensa para muchas organizaciones, y cualquier brecha en su seguridad puede tener consecuencias devastadoras, como robo de datos, interrupciones operativas o acceso no autorizado a redes corporativas.

¿Qué Hacer si Tu Firewall ha Sido Comprometido?

En caso de sospechar una intrusión, las empresas deben:

- **Realizar un análisis forense:** Revisar registros de actividad para identificar accesos no autorizados.
- **Aislar el dispositivo afectado:** Desconectarlo de la red hasta que se complete la evaluación.
- **Actualizar las contraseñas:** Cambiar las credenciales de todos los administradores del sistema.
- **Contactar a expertos:** Considerar recurrir a profesionales de respuesta a incidentes para gestionar el impacto.

Conclusión

Este incidente es un recordatorio contundente de que los ciberatacantes están en constante búsqueda de oportunidades para explotar vulnerabilidades. Las organizaciones deben priorizar la ciberseguridad adoptando un enfoque preventivo y manteniendo una postura de defensa activa. Aplicar parches de seguridad de manera oportuna y restringir el acceso a interfaces críticas son pasos esenciales para mitigar riesgos futuros.

NOTICIA COMPLETA

https://devel.group/blog/mas-de-2000-firewalls-de-palo-alto-networks-comprometidos-mediante-vulnerabilidades-criticas/

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://devel.group/