Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PALO ALTO NETWORKS ADVIERTE SOBRE EXPLOITS EN FIREWALLS: CVE-2025-0111 Y MÁS FALLOS

19/ 02 / 2025

CONTENIDO

INTRODUCCIÓN....3
RESUMEN....5
NOTICIA COMPLETA....7
CONTACTOS DE SOPORTE....8

INTRODUCCIÓN

Palo Alto Networks ha emitido una alerta sobre la explotación activa de la vulnerabilidad CVE-2025-0111 en sus firewalls que ejecutan PAN-OS. Este fallo crítico, junto con CVE-2025-0108 y CVE-2024-9474, representa un riesgo significativo para las organizaciones que dependen de estos dispositivos para su seguridad perimetral. La explotación de estas vulnerabilidades podría permitir a los atacantes evadir controles de seguridad, ejecutar código malicioso o incluso comprometer por completo la red protegida por estos firewalls.

PALO ALTO NETWORKS ADVIERTE SOBRE EXPLOITS EN FIREWALLS: CVE-2025-0111 Y MÁS FALLOS

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

ID de alerta:	DSOC-CERT_2025_02_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/02/2025
Es día cero (0 day):	No

RESUMEN

Palo Alto Networks ha emitido una alerta sobre la explotación activa de la vulnerabilidad CVE-2025-0111 en sus firewalls que ejecutan PAN-OS. Este fallo crítico, junto con CVE-2025-0108 y CVE-2024-9474, representa un riesgo significativo para las organizaciones que dependen de estos dispositivos para su seguridad perimetral. La explotación de estas vulnerabilidades podría permitir a los atacantes evadir controles de seguridad, ejecutar código malicioso o incluso comprometer por completo la red protegida por estos firewalls.

¿Qué pasó?

Investigadores en ciberseguridad han detectado que **CVE-2025-0111** está siendo utilizada en ataques dirigidos. Esta vulnerabilidad permite la **ejecución remota de código (RCE)** sin autenticación, lo que significa que un atacante podría tomar el control del firewall sin necesidad de credenciales válidas. Una vez comprometido, el atacante podría modificar configuraciones, crear puertas traseras o interrumpir servicios esenciales de la red.

Además, esta vulnerabilidad está vinculada a otras dos fallas en PAN-OS:

- **CVE-2025-0108:** Permite la evasión de autenticación, facilitando el acceso no autorizado a configuraciones críticas del firewall. Un atacante podría desactivar reglas de seguridad o modificar políticas para permitir tráfico malicioso dentro de la red.
- **CVE-2024-9474:** Este fallo puede ser aprovechado para ejecutar código de manera remota o escalar privilegios, otorgando al atacante control total sobre el firewall. Combinada con las vulnerabilidades anteriores, permite desde la manipulación de configuraciones hasta la instalación de malware persistente.

¿Cómo funcionan estas vulnerabilidades?

- **CVE-2025-0111:** Debido a una validación inadecuada de entradas en la interfaz de gestión web, un atacante puede enviar comandos maliciosos que el sistema ejecuta sin requerir autenticación.
- **CVE-2025-0108:** Esta vulnerabilidad permite a un atacante eludir el proceso de autenticación en la interfaz de gestión web, otorgando acceso no autorizado a configuraciones sensibles del firewall.
- **CVE-2024-9474:** Un fallo en la gestión de privilegios en la interfaz de gestión web permite a un atacante escalar sus privilegios, obteniendo control total sobre el sistema afectado.

La combinación de estas vulnerabilidades puede ser utilizada en ataques encadenados, donde un atacante primero elude la autenticación, luego ejecuta código malicioso y finalmente escala privilegios para obtener control completo del dispositivo. Palo Alto Networks ha observado intentos de explotación que combinan estas fallas en interfaces de gestión web no parcheadas y desprotegidas.

Parches y pruebas de concepto

Palo Alto Networks ha lanzado parches, donde se abordar esta vulnerabilidad e investigadores han publicado pruebas de concepto (PoC) para ayudar a las organizaciones a comprender la naturaleza de las fallas y cómo pueden ser explotadas. Se recomienda encarecidamente a las empresas aplicar estas actualizaciones de seguridad de inmediato y verificar que sus sistemas estén adecuadamente protegidos. A continuación, se presentan las versiones afectadas y las soluciones sugeridas para mitigar los riesgos asociados.

Version	Minor Version	Suggested Solution
PAN-OS 10.1	10.1.0 through 10.1.14	Upgrade to 10.1.14-h9 or later
PAN-OS 10.2	10.2.0 through 10.2.13	Upgrade to 10.2.13-h3 or later
	10.2.7	Upgrade to 10.2.7-h24 or 10.2.13-h3 or later
	10.2.8	Upgrade to 10.2.8-h21 or 10.2.13-h3 or later
	10.2.9	Upgrade to 10.2.9-h21 or 10.2.13-h3 or later
	10.2.12	Upgrade to 10.2.12-h6 or 10.2.13-h3 or later
PAN-OS 11.0 (EoL)		Upgrade to a supported fixed version
PAN-OS 11.1	11.1.0 through 11.1.6	Upgrade to 11.1.6-h1 or later
PAN-OS 11.2	11.2.0 through 11.2.4	Upgrade to 11.2.4-h4 or later

Conclusión

La explotación activa de las vulnerabilidades **CVE-2025-0111, CVE-2025-0108 y CVE-2024-9474** en los firewalls que ejecutan PAN-OS destaca la importancia de mantener una postura de seguridad proactiva. Estas fallas, especialmente cuando se combinan, pueden permitir a los atacantes eludir mecanismos de autenticación, ejecutar código malicioso y comprometer la integridad de la red protegida. La disponibilidad de parches oficiales y pruebas de concepto subraya la necesidad de que las organizaciones actúen con rapidez para proteger sus infraestructuras críticas.

Recomendaciones y Mitigación

Para proteger sus sistemas y minimizar el riesgo asociado con estas vulnerabilidades, se aconseja a las organizaciones:

- **Aplicar Actualizaciones de Seguridad:** Instale inmediatamente las versiones parcheadas de PAN-OS proporcionadas por Palo Alto Networks. Estas actualizaciones abordan las vulnerabilidades mencionadas y están disponibles en el sitio oficial de seguridad de Palo Alto Networks.

- **Restringir el Acceso a la Interfaz de Gestión:** Configure el firewall para que la interfaz de gestión web sea accesible únicamente desde direcciones IP internas y de confianza, reduciendo la superficie de ataque y limitando la posibilidad de explotación remota.
- **Monitorear Actividad Sospechosa:** Implemente sistemas de detección de intrusiones (IDS) y revise regularmente los registros de actividad en busca de comportamientos anómalos que puedan indicar intentos de explotación.
- **Educar al Personal de TI:** Asegure que su equipo de tecnología esté informado sobre estas vulnerabilidades y las mejores prácticas para mitigarlas, incluyendo la aplicación de parches y la configuración segura de los sistemas.
- **Evaluar la Exposición Externa:** Realice auditorías periódicas para identificar y minimizar los servicios expuestos a Internet que no sean estrictamente necesarios, reduciendo así las posibles vías de ataque.

NOTICIA COMPLETA

https://devel.group/blog/palo-alto-networks-advierte-sobre-exploits-en-firewalls-cve-2025-0111-y-mas-fallos/

CONTACTOS DE SOPORTE

Correo electrónico: info@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/