Palo Alto Networks emitió un aviso el viernes, instando a sus clientes a reforzar la seguridad de acceso a la interfaz de administración de PAN-OS debido a una posible vulnerabilidad de ejecución remota de código.

> *«La empresa tiene conocimiento de una posible vulnerabilidad de ejecución remota de código en la interfaz de administración de PAN-OS. Actualmente, desconocemos los detalles exactos de la vulnerabilidad alegada. Estamos monitoreando de cerca cualquier señal de explotación»,* señaló Palo Alto Networks.

Mientras tanto, el proveedor de seguridad de redes ha recomendado que los usuarios configuren correctamente la interfaz de administración conforme a las mejores prácticas y se aseguren de que el acceso solo sea posible desde IPs internas confiables para reducir la exposición a posibles ataques.

Es importante recordar que la interfaz de administración no debe estar disponible en Internet. Algunas otras pautas recomendadas para minimizar el riesgo incluyen:

- Aislar la interfaz de administración en una VLAN dedicada exclusivamente a la administración.
- Utilizar servidores de salto para acceder a la IP de administración.
- Restringir las direcciones IP de acceso a la interfaz de administración a dispositivos de administración aprobados.
- Permitir únicamente comunicaciones seguras, como SSH y HTTPS.
- Habilitar PING solo para verificar la conectividad con la interfaz.

Este aviso sigue la inclusión, un día antes, de una vulnerabilidad crítica de seguridad en la herramienta Palo Alto Networks Expedition en el catálogo de Vulnerabilidades Conocidas Explotadas (KEV) de la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA), debido a pruebas de explotación activa.

La vulnerabilidad, designada como CVE-2024-5910 (con una puntuación CVSS de 9.3), se

debe a una falta de autenticación en la herramienta de migración Expedition, lo cual podría permitir el control de una cuenta de administrador y, potencialmente, el acceso a datos sensibles.

Aunque por el momento no se sabe exactamente cómo se está explotando en la práctica, se ha recomendado a las agencias federales que apliquen las actualizaciones necesarias antes del 28 de noviembre de 2024 para proteger sus redes contra esta amenaza.