Boletín de alerta

Boletín Nro.:
Fecha de publicación: 20/01/2025
Tema: Alerta 2025-06 Múltiples Vulnerabilidades Críticas en Palo Alto Networks Expedition
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Expedition 1 < 1.2.101.

Descripción

Palo Alto Networks ha identificado múltiples vulnerabilidades críticas en su herramienta. Estas fallas de seguridad podrían permitir a un atacantes acceder y manipular información sensible, como credenciales de acceso, configuraciones de dispositivos y claves API. Es crucial que los usuarios de Expedition tomen medidas inmediatas para mitigar estos riesgos

Expedition es una herramienta temporal y gratuita que ayuda a los usuarios a migrar a la plataforma NGFW de Palo Alto Networks. Sin embargo, esta herramienta ha llegado al final de su ciclo de vida y ya no cuenta con soporte técnico.

Inyección SQL (CVE-2025-0103): Un atacante podría explotar esta vulnerabilidad para acceder a la base de datos de Expedition y robar información confidencial, incluyendo contraseñas en texto plano y claves API.

XSS Reflejada (CVE-2025-0104): Al hacer clic en un enlace malicioso, un usuario podría ser víctima de un ataque de phishing que comprometa su sesión y permita al atacante realizar acciones en su nombre.

Eliminación Arbitraria de Archivos (CVE-2025-0105): Atacadores no autenticados podrían eliminar archivos del sistema Expedition, potencialmente causando daños irreparables.

Expansión de Comodines (CVE-2025-0106): Esta vulnerabilidad permite a atacantes enumerar los archivos del sistema, lo que podría servir como punto de partida para otros ataques.

Inyección de Comandos (CVE-2025-0107): Un atacante podría ejecutar comandos arbitrarios en el sistema Expedition, lo que podría resultar en la ejecución de código malicioso o la exfiltración de datos.

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 20/01/2025
Tema: Alerta 2025-06 Múltiples Vulnerabilidades Críticas en Palo Alto Networks Expedition
Traffic Light Protocol (TLP): Amber

A través de una prueba de concepto, los investigadores de seguridad han demostrado la viabilidad de explotar esta vulnerabilidad

Solución

- Actualice a la versión 1.2.101 de Expedition o posterior.
- Asegúrese de que todo el acceso a la red de Expedition esté restringido únicamente a los usuarios, hosts y redes autorizados.
- Si no está utilizando Expedition de forma activa, asegúrese de que el software de Expedition esté apagado.

Información adicional:

- https://security.paloaltonetworks.com/PAN-SA-2025-0001
- https://live.paloaltonetworks.com/t5/expedition-articles/important-update-end-of-life-announcement-for-palo-alto-networks/ta-p/589642
- https://cybersecuritynews.com/poc-exploit-palo-alto-command-injection/