e-dea NETWORKS | CYBER SECURITY

BOLETÍN INFORMATIVO

20 – Enero - 2025

Vulnerabilidades en Palo Alto

Detalles:

El fabricante Palo Alto emite comunicado sobre varias vulnerabilidades en la herramienta de migración Expedition de Palo Alto Networks que permiten a un atacante leer el contenido de la base de datos permitiendo crear y eliminar archivos que contienen información como nombres de usuario, contraseñas, configuraciones de dispositivos y claves API de dispositivos para firewalls que ejecutan software PAN-OS.

CVE Relacionada:

CVE	Tipo de vulnerabilidad
CVE-2025-0103	SQL injection
CVE-2025-0104	A reflected cross-site scripting (XSS)
CVE-2025-0105	An arbitrary file deletion vulnerability
CVE-2025-0106	A wildcard expansion
CVE-2025-0107	OS command injection vulnerability

Versiones afectadas:

Producto	Versión
Palo Alto Networks Expedition migration tool	< 1.2.101

Severidad: ALTA

Recomendaciones:

- Los siguientes CVE están corregidos en la versión especificada y en todas las versiones posteriores.
- Asegurarse de que todo el acceso a la red esté restringido únicamente a los usuarios, hosts y redes autorizados.
- Si no está utilizando Expedition de forma activa, asegurarse de que el software de Expedition esté apagado.

Fuentes: Palo Alto; Update Paloalto