e-dea NETWORKS | CYBER SECURITY

BOLETÍN INFORMATIVO

11 - Octubre - 2024

Múltiples vulnerabilidades en Palo Alto

Detalles: +

El fabricante PaloAlto emite comunicado sobre múltiples vulnerabilidades descubiertas, de las cuales permiten ejecución de código que podría ocasionar la divulgación de nombres de usuario, contraseñas en texto claro, configuraciones de dispositivos y claves API de dispositivos firewall PAN-OS.

Versiones afectadas:

Producto	Versión
Palo Alto Networks Expedition	< 1.2.96

CVE Relacionadas:

CVE	CVSS	Tipo de vulnerabilidad
CVE-2024-9463	9.9	Vulnerabilidad de Inyección de comandos
CVE-2024-9464	9.3	Vulnerabilidad de Inyección de comandos
CVE-2024-9465	9.2	Vulnerabilidad de Inyección SQL
CVE-2024-9466	8.2	Almacenamiento de texto plano
CVE-2024-9467	7.0	Vulnerabilidad de XSS reflejado

Severidad: Crítica

Recomendaciones:

- Aplicar las actualizaciones de seguridad.
- Priorizar la implementación de parches de seguridad, comenzando por las vulnerabilidades críticas y luego las calificadas como importantes.
- Aplicar cambios en usuarios, contraseñas y claves API después de actualizar a la versión fija de Expedition.

Fuentes: Palo Alto; INCIBE