BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-50
Fecha de publicación: 10/10/2024
Tema: Vulnerabilidades Críticas en Firewalls PAN-OS
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Palo Alto Expedition (herramienta de migración de configuraciones para firewalls de Palo Alto Networks). versiones anteriores a la 1.2.96

Descripción

Palo Alto Networks ha emitido una advertencia sobre varias vulnerabilidades críticas en su herramienta Expedition, utilizada para migrar configuraciones de firewalls. Estas vulnerabilidades permiten a los atacantes tomar control de cuentas administrativas de los firewalls PAN-OS, accediendo a información sensible como nombres de usuario, contraseñas en texto claro, configuraciones de dispositivos y claves API.

Las fallas incluyen inyecciones de comandos no autenticadas, vulnerabilidades de inyección SQL, y almacenamiento en texto claro de información confidencial. Entre las vulnerabilidades destacadas están:

- CVE-2024-9463: Permite a un atacante no autenticado ejecutar comandos del sistema operativo como root, exponiendo datos sensibles (CVSS 9.9).
- CVE-2024-9464: Un atacante autenticado puede ejecutar comandos de forma remota como root (CVSS 9.3).
- CVE-2024-9465: Vulnerabilidad de inyección SQL que permite acceso no autenticado a la base de datos de *Expedition*, exponiendo credenciales y permitiendo la creación y lectura de archivos arbitrarios (CVSS 9.2).

Solución

Para mitigar estos riesgos, Palo Alto recomienda actualizar *Expedition* a la versión 1.2.96 o superior y rotar todas las credenciales afectadas, incluyendo nombres de usuario,

contraseñas y claves API. Asimismo, se recomienda restringir el acceso a la red solo a usuarios y hosts autorizados.

Es crucial aplicar estas actualizaciones para proteger los sistemas de posibles ataques.

Para más información y parches, puedes acceder al sitio oficial de Palo Alto Networks.

Información adicional:

- https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-firewall-hijack-bugs-with-public-exploit
- https://www.techmonitor.ai/technology/cybersecurity/palo-alto-networks-urges-urgent-patch-for-firewall-hijack-vulnerabilities
- https://informationsecuritybuzz.com/palo-alto-exploitable-firewall-hijack/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com