Palo Alto Networks ha lanzado actualizaciones para corregir varias vulnerabilidades en su herramienta de migración Expedition, incluyendo una falla de alta severidad que podría ser aprovechada por un atacante autenticado para acceder a información sensible.

> *«Las vulnerabilidades en la herramienta de migración Expedition permiten a un atacante acceder al contenido de la base de datos de Expedition y a archivos arbitrarios, además de crear y eliminar archivos en el sistema Expedition»*, informó la compañía en su comunicado.
>
> *«Entre estos archivos se encuentran datos como nombres de usuario, contraseñas en texto plano, configuraciones de dispositivos y claves API de dispositivos para firewalls que ejecutan el software PAN-OS.»*

Expedition, una herramienta gratuita diseñada para facilitar la migración desde otros proveedores de firewalls hacia la plataforma de Palo Alto Networks, alcanzó su fin de vida útil (EoL) el 31 de diciembre de 2024. Las vulnerabilidades identificadas son las siguientes:

- CVE-2025-0103 (Puntuación CVSS: 7.8): Una falla de inyección SQL que permite a un atacante autenticado acceder a la base de datos de Expedition, exponiendo hashes de contraseñas, nombres de usuario, configuraciones de dispositivos y claves API. También permite crear y leer archivos arbitrarios.
- CVE-2025-0104 (Puntuación CVSS: 4.7): Una vulnerabilidad de cross-site scripting (XSS) reflejado que posibilita la ejecución de código JavaScript malicioso en el navegador de un usuario autenticado si este interactúa con un enlace malicioso. Esto podría facilitar ataques de phishing o el robo de sesiones.
- CVE-2025-0105 (Puntuación CVSS: 2.7): Un fallo que permite la eliminación de archivos arbitrarios en el sistema por parte de un atacante no autenticado, siempre que los archivos sean accesibles para el usuario «www-data».
- CVE-2025-0106 (Puntuación CVSS: 2.7): Una vulnerabilidad que permite a un atacante no autenticado enumerar archivos en el sistema mediante la expansión de comodines.

- CVE-2025-0107 (Puntuación CVSS: 2.3): Un fallo de inyección de comandos en el sistema operativo que permite a un atacante autenticado ejecutar comandos arbitrarios como el usuario «www-data». Esto puede resultar en la exposición de nombres de usuario, contraseñas en texto claro, configuraciones de dispositivos y claves API para firewalls que usen PAN-OS.

Palo Alto Networks solucionó estas vulnerabilidades en las versiones 1.2.100 (CVE-2025-0103, CVE-2025-0104 y CVE-2025-0107) y 1.2.101 (CVE-2025-0105 y CVE-2025-0106). Sin embargo, la compañía no planea lanzar más actualizaciones o parches de seguridad para Expedition.

Como medidas de mitigación, se recomienda limitar el acceso a Expedition únicamente a usuarios, hosts y redes autorizados o desactivar el servicio si ya no es necesario.

Actualizaciones de seguridad para SonicOS de SonicWall

Por otro lado, SonicWall ha lanzado correcciones para varias vulnerabilidades en SonicOS. Dos de ellas son especialmente graves, ya que podrían ser usadas para evitar autenticación y escalar privilegios:

- CVE-2024-53704 (Puntuación CVSS: 8.2): Una falla en el mecanismo de autenticación SSLVPN que permite a un atacante remoto eludir la autenticación.
- CVE-2024-53706 (Puntuación CVSS: 7.8): Una vulnerabilidad en la plataforma en la nube Gen7 SonicOS NSv (aplicable solo a las ediciones de AWS y Azure) que permite a un atacante autenticado y con privilegios limitados elevarlos a nivel root, lo que podría derivar en la ejecución de código.

Aunque no hay indicios de que estas fallas hayan sido explotadas activamente, es fundamental que los usuarios instalen las actualizaciones correspondientes lo antes posible.

Falla crítica descubierta en Aviatrix Controller

Finalmente, la empresa de ciberseguridad polaca Securing ha identificado una vulnerabilidad crítica en Aviatrix Controller (CVE-2024-50603, puntuación CVSS: 10.0) que podría ser utilizada para ejecutar código de manera remota. Este problema afecta a las versiones 7.x hasta 7.2.4820.

El fallo está relacionado con la falta de sanitización de ciertos parámetros proporcionados por los usuarios en un endpoint de la API («list_flightpath_destination_instances» y «flightpath_connection_test»). Este problema fue corregido en las versiones 7.1.4191 y 7.2.4996.

> *«Debido a la neutralización insuficiente de ciertos elementos especiales en un comando del sistema operativo, un atacante no autenticado podría ejecutar comandos de forma remota»*, explicó Jakub Korepta, investigador de seguridad.