Palo Alto Networks ha publicado actualizaciones de seguridad para corregir cinco fallas en sus productos, incluyendo una vulnerabilidad crítica que podría permitir la omisión de autenticación.

Identificada como CVE-2024-5910 (puntuación CVSS: 9.3), esta vulnerabilidad se describe como una falta de autenticación en su herramienta de migración Expedition, lo que podría resultar en la toma de control de una cuenta de administrador.

> *«La ausencia de autenticación en una función crítica de Palo Alto Networks Expedition puede llevar a que atacantes con acceso a la red a Expedition tomen control de una cuenta de administrador de Expedition. Los secretos de configuración, credenciales y otros datos importados a Expedition están en riesgo debido a este problema»,* explicó la compañía en un comunicado.

La falla afecta a todas las versiones de Expedition anteriores a la versión 1.2.92, que soluciona el problema. Brian Hysell, del Centro de Investigación en Ciberseguridad de Synopsys (CyRC), ha sido reconocido por descubrir y reportar el problema.

Aunque no hay evidencia de que la vulnerabilidad haya sido explotada en la práctica, se recomienda a los usuarios actualizar a la versión más reciente para protegerse contra posibles amenazas.

Como medidas provisionales, Palo Alto Networks sugiere que el acceso a la red a Expedition se limite a usuarios, hosts o redes autorizados.

La firma de ciberseguridad estadounidense también ha corregido una nueva falla en el protocolo RADIUS, denominada BlastRADIUS (CVE-2024-3596), que podría permitir a un atacante con capacidades realizar un ataque de adversario-en-el-medio (AitM) entre el firewall PAN-OS de Palo Alto Networks y un servidor RADIUS, eludiendo así la autenticación.

La vulnerabilidad permite al atacante *«escalar privilegios a 'superusuario' cuando se utiliza la*

autenticación RADIUS y se selecciona CHAP o PAP en el perfil del servidor RADIUS», indicó la compañía.

Los siguientes productos se ven afectados por estas deficiencias:

- PAN-OS 11.1 (versiones < 11.1.3, corregido en >= 11.1.3)
- PAN-OS 11.0 (versiones < 11.0.4-h4, corregido en >= 11.0.4-h4)
- PAN-OS 10.2 (versiones < 10.2.10, corregido en >= 10.2.10)
- PAN-OS 10.1 (versiones < 10.1.14, corregido en >= 10.1.14)
- PAN-OS 9.1 (versiones < 9.1.19, corregido en >= 9.1.19)
- Prisma Access (todas las versiones, corrección prevista para el 30 de julio)

También se destacó que ni CHAP ni PAP deben usarse a menos que estén encapsulados en un túnel cifrado, ya que estos protocolos de autenticación no ofrecen Seguridad de la Capa de Transporte (TLS). No son vulnerables en los casos donde se usan junto con un túnel TLS.

Sin embargo, es importante señalar que los firewalls PAN-OS configurados para usar EAP-TTLS con PAP como protocolo de autenticación para un servidor RADIUS tampoco son susceptibles a este ataque.