Palo Alto Networks ha informado sobre una vulnerabilidad de alta gravedad que afecta al software PAN-OS, la cual podría ocasionar una condición de denegación de servicio (DoS) en dispositivos vulnerables.

El problema, identificado como CVE-2024-3393 (con una puntuación CVSS de 8.7), afecta a las versiones 10.X y 11.X de PAN-OS, así como a Prisma Access ejecutando versiones de PAN-OS desde la 10.2.8 en adelante y anteriores a la 11.2.3. La vulnerabilidad ha sido solucionada en las versiones PAN-OS 10.1.14-h8, PAN-OS 10.2.10-h12, PAN-OS 11.1.5, PAN-OS 11.2.3 y versiones posteriores.

> *«Una vulnerabilidad en la funcionalidad de seguridad DNS del software PAN-OS de Palo Alto Networks permite que un atacante no autenticado envíe un paquete malicioso a través del plano de datos del firewall, lo que provoca que este se reinicie»,* explicó la empresa en un comunicado emitido el viernes.
>
> *«Si este proceso se repite continuamente, el firewall entrará en modo de mantenimiento»,* añadió la compañía.

Palo Alto Networks indicó que esta falla fue descubierta en un entorno de producción y confirmó que algunos clientes ya han experimentado un estado de denegación de servicio (DoS) cuando el firewall bloquea paquetes DNS maliciosos que explotan esta vulnerabilidad.

Cabe destacar que esta vulnerabilidad, CVE-2024-3393, afecta a los firewalls que tienen habilitado el registro de seguridad DNS. Además, la gravedad de la vulnerabilidad se reduce a un puntaje CVSS de 7.1 cuando solo usuarios autenticados tienen acceso a través de Prisma Access.

Las correcciones también se han aplicado a varias versiones comunes de mantenimiento, como:

- PAN-OS 11.1 (11.1.2-h16, 11.1.3-h13, 11.1.4-h7 y 11.1.5)
- PAN-OS 10.2 (10.2.8-h19, 10.2.9-h19, 10.2.10-h12, 10.2.11-h10, 10.2.12-h4, 10.2.13-h2 y 10.2.14)
- PAN-OS 10.1 (10.1.14-h8 y 10.1.15)
- PAN-OS 10.2.9-h19 y 10.2.10-h12 (aplicable únicamente a Prisma Access)
- PAN-OS 11.0 (sin actualización debido a que llegó al fin de su ciclo de vida el 17 de noviembre de 2024)

Para mitigar el problema en firewalls no administrados o gestionados mediante Panorama, los usuarios pueden desactivar el registro de seguridad DNS estableciendo la severidad del registro en «ninguno» en todas las categorías configuradas de seguridad DNS dentro de cada perfil de antispyware. Esto se puede realizar navegando a Objects > Security Profiles > Anti-spyware > (seleccionar un perfil) > DNS Policies > DNS Security.

En el caso de los firewalls administrados a través de Strata Cloud Manager (SCM), los usuarios pueden aplicar esta configuración en cada dispositivo individualmente o de forma global abriendo un caso de soporte. Para los entornos de Prisma Access gestionados por SCM, se sugiere también abrir un caso de soporte para desactivar el registro hasta que se pueda realizar una actualización.