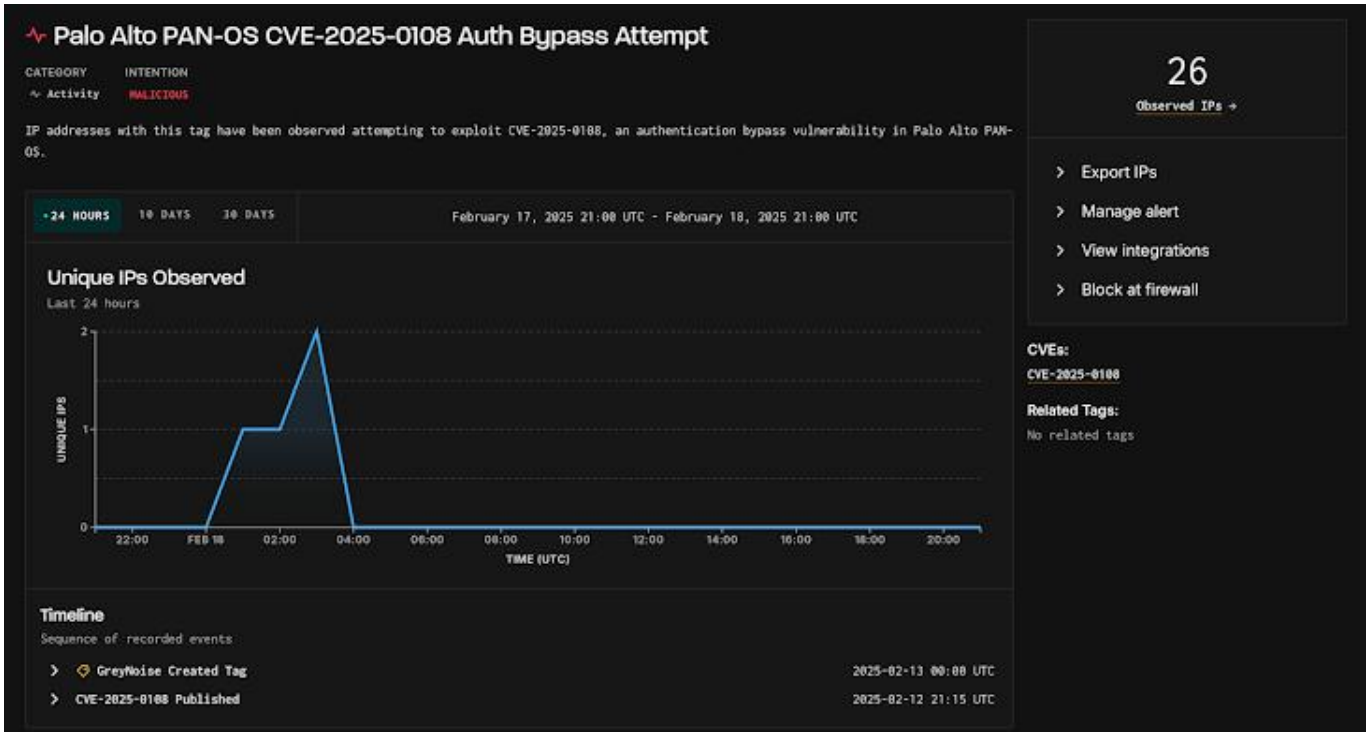
La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incorporado dos fallos de seguridad, que afectan a Palo Alto Networks PAN-OS y SonicWall SonicOS SSLVPN, a su lista de Vulnerabilidades Explotadas Conocidas (KEV), debido a evidencia de explotación activa.

Las vulnerabilidades identificadas son las siguientes:

- CVE-2025-0108 (calificación CVSS: 7.8): un fallo de omisión de autenticación en la interfaz web de administración de PAN-OS de Palo Alto Networks, que permite a un atacante sin credenciales, pero con acceso a la red, evitar la autenticación requerida e invocar ciertos scripts PHP.
- CVE-2024-53704 (calificación CVSS: 8.2): un problema de autenticación inadecuada en el mecanismo SSLVPN, que posibilita que un atacante remoto evite el proceso de autenticación.

Palo Alto Networks confirmó que ha detectado intentos de explotación activa de la vulnerabilidad CVE-2025-0108, indicando que esta podría combinarse con otros fallos, como CVE-2024-9474, para facilitar accesos no autorizados a firewalls desprotegidos y sin actualizaciones.

> *«Hemos observado intentos de explotación que combinan la CVE-2025-0108 con la CVE-2024-9474 y la CVE-2025-0111 en interfaces de administración web de PAN-OS que no han sido parcheadas ni aseguradas»*, señaló la empresa en un aviso actualizado.



La compañía de inteligencia de amenazas GreyNoise ha detectado que 25 direcciones IP maliciosas están aprovechando la vulnerabilidad CVE-2025-0108, con un incremento de la actividad de los atacantes de diez veces desde su detección inicial hace aproximadamente una semana. Los principales orígenes del tráfico de ataques son Estados Unidos, Alemania y los Países Bajos.

Respecto a CVE-2024-53704, la empresa de ciberseguridad Arctic Wolf informó que actores maliciosos están explotando esta vulnerabilidad poco después de que *Bishop Fox* publicara un código de prueba de concepto (PoC).

Dado el uso activo de estas vulnerabilidades por parte de ciberdelincuentes, las agencias pertenecientes a la Rama Ejecutiva Federal Civil (FCEB) deberán aplicar las correcciones necesarias antes del 11 de marzo de 2025 para fortalecer la seguridad de sus redes.