Boletín de alerta

Boletín Nro.:
Fecha de publicación: 09/01/2025
Tema: Alert 2025-02-Explotacion activa de vulnerabilidades de Palo Alto PAN OS
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1 y PAN-OS 11.2 en los firewalls PA-Series, VM-Series y CN-Series y en Panorama (virtual y M-Series).

Descripción

En noviembre, desde BeaconLab, en nuestro boletín **Alerta 2024-65: Vulnerabilidades Críticas en Firewalls de Palo Alto Networks (PAN-OS),** habíamos advertido sobre algunas vulnerabilidades críticas de PanOS. Actualmente, estas vulnerabilidades están siendo explotadas activamente.

Específicamente se ha informado sobre la explotación activa de las vulnerabilidades CVE-2024-0012 y CVE-2024-9474, ambas afectando el software PAN-OS.

CVE-2024-0012:

Esta vulnerabilidad permite a un atacante no autenticado con acceso a la interfaz de administración de PAN-OS obtener privilegios de administrador. Con ello, un adversario podría realizar acciones administrativas, alterar configuraciones críticas o aprovechar otras vulnerabilidades de escalada de privilegios, como CVE-2024-9474.

CVE-2024-9474:

Esta vulnerabilidad, explotada como continuación de CVE-2024-0012, facilita la escalación de privilegios dentro del sistema PAN-OS, permitiendo la ejecución de acciones altamente privilegiadas, incluidas potencialmente la instalación de software malicioso.

Actividad Observada

Palo Alto Networks detectó actividad de amenazas asociada con estas vulnerabilidades en un número limitado de interfaces de administración web expuestas. La actividad posterior a la explotación incluye:

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 09/01/2025
Tema: Alert 2025-02-Explotacion activa de vulnerabilidades de Palo Alto PAN OS
Traffic Light Protocol (TLP): Amber

- Ejecución de comandos interactivos en los dispositivos comprometidos.
- Instalación de malware, como shells web ofuscados, para mantener persistencia en los sistemas afectados.

Unit 42 confirma, con alto grado de certeza, la existencia de un exploit público funcional que combina CVE-2024-0012 y CVE-2024-9474, lo que facilita una explotación más amplia de estos problemas.

Palo Alto Networks continuará investigando y publicará actualizaciones sobre la actividad relacionada con estas vulnerabilidades, si fuera necesario,

Solución

Actualice su firmware e instale las versiones más recientes del PAN-OS para mitigar las vulnerabilidades.

Información adicional:

- https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/#post-137539-_ydqdbjg0dngh
- https://security.paloaltonetworks.com/CVE-2024-0012
- https://security.paloaltonetworks.com/CVE-2024-9474