Boletín de alerta

Boletín Nro.: 05
Fecha de publicación: 15/01/2026
Tema: Alerta 2026-05 Vulnerabilidad de Denegación de Servicio (DoS) en PAN-OS GlobalProtectTraffic
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **PAN-OS (next-generation firewalls)**
  - 12.1 anteriores a 12.1.3-h3 / 12.1.4
  - 11.2 anteriores a 11.2.4-h15, 11.2.7-h8, 11.2.10-h2
  - 11.1 anteriores a 11.1.4-h27, 11.1.6-h23, 11.1.10-h9, 11.1.13
  - 10.2 anteriores a 10.2.7-h32, 10.2.10-h30, 10.2.13-h18, 10.2.16-h6, 10.2.18-h1
  - 10.1 anteriores a 10.1.14-h20
- **Prisma Access**
  - Versiones 11.2 anteriores a 11.2.7-h8
  - Versiones 10.2 anteriores a 10.2.10-h29

Descripción

Recientemente, Palo Alto Networks identificó y publicó una vulnerabilidad en su software PAN-OS, identificada como CVE-2026-0227 con un CVSS Base Score de 7.7, que impulsa sus firewalls de próxima generación y servicios de acceso seguro (GlobalProtect). Afecta específicamente al **GlobalProtect Gateway y Portal**, utilizados para acceso remoto seguro de clientes VPN y conexión de usuarios a redes corporativas protegidas.

Esta CVE es un **bug de lógica que provoca un estado de Denegación de Servicio (DoS)**. Debido a un **manejo incorrecto de condiciones excepcionales o inusuales** en la implementación de GlobalProtect dentro de PAN-OS, un atacante **no autenticado y sin privilegios puede enviar tráfico especialmente diseñado** a los servicios impactados. Repetidos intentos **rompen el procesamiento normal de tráfico del firewall**, provocando que el dispositivo:

- se *bloquee de manera parcial o total*,
- entre en **modo mantenimiento**,
- requiera **intervención manual de un administrador** para restaurar operaciones normales.

Se ha publicado un **proof-of-concept (PoC)** funcional, lo que significa que la vulnerabilidad puede ser replicada y automatizada con relativa facilidad. Hasta ahora **no se han reportado evidencias de explotación activa en ataques reales**, pero el riesgo de abuso es tangible debido a la naturaleza remota y sin autenticación de la falla.

Solución y mitigación:

La única mitigación efectiva es aplicar los parches y actualizaciones publicados por Palo Alto Networks para PAN-OS y Prisma Access en todas las versiones afectadas.

Algunas versiones parcheadas son:

- PAN-OS 12.1.4 o superior
- PAN-OS 11.2.10-h2 o superior
- PAN-OS 11.1.13 o superior
- PAN-OS 10.2.18-h1 o superior
- PAN-OS 10.1.14-h20 o superior

Estas y otras actualizaciones específicas están listadas por versión en el portal de soporte de Palo Alto Networks en el siguiente enlace:

Palo Alto Networks Security Advisories

Recomendaciones adicionales:

- Priorizar la actualización de **firewalls expuestos a Internet** y **Prisma Access** en producción.
- **Revisar logs de eventos y monitoreo de disponibilidad** para detectar patrones de interrupciones o intentos repetidos de conexión que coincidan con el vector de DoS.
- Asegurar que los equipos de operaciones de red puedan realizar **recuperación manual rápida** si un dispositivo entra en modo mantenimiento.

Información adicional:

- https://security.paloaltonetworks.com/CVE-2026-0227
- Palo Alto Networks Firewall Vulnerability Allows Unauthenticated Attackers to Trigger Denial of Service
- https://secalerts.co/vulnerability/CVE-2026-0227