Boletín de alerta

Boletín Nro.:

Fecha de publicación: 21/07/2026

Tema: Alerta 2026-75 Explotación Activa de Vulnerabilidad en Palo Alto GlobalProtect Utilizada por el Ransomware Qilin

Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **PAN-OS 12.1**: versiones anteriores a 12.1.4-h6 y 12.1.7.
- **PAN-OS 11.2**: versiones anteriores a 11.2.4-h17, 11.2.7-h14, 11.2.10-h7 y 11.2.12.
- **PAN-OS 11.1:** versiones anteriores a 11.1.4-h33, 11.1.6-h32, 11.1.7-h6, 11.1.10-h25, 11.1.13-h5 y 11.1.15.
- **PAN-OS 10.2**: versiones anteriores a 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7 y 10.2.18-h6.
- **Prisma Access** 11.2.0: versiones anteriores a 11.2.7-h13.
- **Prisma Access** 10.2.0: versiones anteriores a 10.2.10-h36.

Descripción

Investigadores confirmaron que el grupo de ransomware **Qilin** está explotando activamente la vulnerabilidad **CVE-2026-0257** en **Palo Alto Networks GlobalProtect**, la cual permite a un atacante eludir los controles de autenticación y establecer conexiones VPN no autorizadas.

Una vez obtenido el acceso inicial, los atacantes realizan reconocimiento de la red, extraen credenciales, ejecutan movimientos laterales mediante **PsExec**, despliegan herramientas de acceso remoto y, finalmente, cifran los sistemas comprometidos o realizan ataques de doble extorsión mediante el robo de información. Debido a la amplia adopción de GlobalProtect en entornos empresariales, esta vulnerabilidad representa un alto riesgo para organizaciones que aún no han aplicado las actualizaciones de seguridad.

Indicadores de Compromiso (IOC)

Rutas utilizadas por el ransomware

C:\PerfLogs\

Herramientas observadas durante la post-explotación

- PsExec
- AnyDesk
- Ngrok

- LogMeIn

Técnicas identificadas

- Extracción de credenciales desde **LSASS**
- Robo de la base de datos **NTDS.dit**
- Movimiento lateral mediante recursos administrativos (ADMIN$, C$)
- Borrado de registros (Windows Event Logs)
- Despliegue de cargas útiles protegidas con contraseña
- Cifrado masivo de sistemas
- Exfiltración de información hacia servicios de almacenamiento en la nube

Repositorio oficial de IOC

- **https://github.com/rtkwlf/wolf-tools/tree/main/threat-intelligence/cookie-crumbles-qilin**

Solución:

Se recomienda realizar las siguientes acciones de forma inmediata:

- Actualizar **PAN-OS** a una versión que incluya la corrección para **CVE-2026-0257**.

Producto	Versiones afectadas	Versiones corregidas
Cloud NGFW	No afectado	Todas las versiones
PAN-OS 12.1	Versiones anteriores a **12.1.4-h6** y **12.1.7**	**12.1.4-h6**, **12.1.7** o superiores
PAN-OS 11.2	Versiones anteriores a **11.2.4-h17**, **11.2.7-h14**, **11.2.10-h7** y **11.2.12**	**11.2.4-h17**, **11.2.7-h14**, **11.2.10-h7**, **11.2.12** o superiores
PAN-OS 11.1	Versiones anteriores a **11.1.4-h33**, **11.1.6-h32**, **11.1.7-h6**, **11.1.10-h25**, **11.1.13-h5** y **11.1.15**	**11.1.4-h33**, **11.1.6-h32**, **11.1.7-h6**, **11.1.10-h25**, **11.1.13-h5**, **11.1.15** o superiores
PAN-OS 10.2	Versiones anteriores a **10.2.7-h34**, **10.2.10-h36**, **10.2.13-h21**, **10.2.16-h7** y **10.2.18-h6**	**10.2.7-h34**, **10.2.10-h36**, **10.2.13-h21**, **10.2.16-h7**, **10.2.18-h6** o superiores
Prisma Access 11.2.0	Versiones anteriores a **11.2.7-h13**	**11.2.7-h13** o superior
Prisma Access 10.2.0	Versiones anteriores a **10.2.10-h36**	**10.2.10-h36** o superior

Información adicional:

- Cookie Crumbles: How Exploitation of CVE-2026-0257 Leads to Qilin Ransomware – Arctic Wolf
- Critical Palo Alto VPN bug now exploited by Qilin ransomware gang
- https://security.paloaltonetworks.com/CVE-2026-0257
- https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/pan-os-software-updates