Boletín de alerta

Boletín Nro.:
Fecha de publicación: 08/12/2025
Tema: Alerta 2025-100 Ataques Masivos contra Portales VPN GlobalProtect
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- GlobalProtect VPN, componentes Portales VPN / PAN-OS

Descripción

Desde el 14 de noviembre de 2025 se ha identificado una campaña global de ataques dirigida a los portales VPN GlobalProtect de Palo Alto Networks. Firmas de inteligencia como GreyNoise han registrado más de **2.3 millones de sesiones maliciosas**, un incremento de **hasta 40 veces en 24 horas**, lo que representa el nivel de actividad más alto en meses. Los atacantes provienen de más de **7,000 direcciones IP únicas** distribuidas entre infraestructura comprometida, proxies residenciales y proveedores de alojamiento a prueba de balas.

Los ataques se enfocan en la ruta **/global-protect/login.esp**, donde intentan **fuerza bruta y explotación de configuraciones débiles** en portales expuestos a Internet, especialmente aquellos que permiten acceso previo a la autenticación o mantienen configuraciones por defecto. Se han observado patrones consistentes como huellas JA4t y tráfico anómalo hacia el puerto UDP 4501, junto con intentos de exfiltración de tokens de sesión que permitirían movimiento lateral dentro de las redes internas.

La infraestructura ofensiva está altamente concentrada, con el **62% del tráfico proveniente del ASN AS200373 (3xK Tech GmbH)**, complementada por otros ASN vinculados a campañas previas. Este comportamiento refleja operaciones coordinadas, posiblemente vinculadas a actores avanzados con capacidad de automatización y evasión.

Palo Alto Networks emitió un aviso urgente el 5 de diciembre instando a las organizaciones a aplicar **autenticación multifactor (MFA)**, restringir la exposición pública de portales y aplicar las últimas actualizaciones de PAN-OS. La CISA ha incluido los indicadores en su catálogo de vulnerabilidades activamente explotadas, exigiendo correcciones aceleradas

URI objetivo atacada

- /global-protect/login.esp

Solución:

Para reducir el riesgo de explotación, se recomienda habilitar

- La autenticación multifactor (MFA) en todos los portales GlobalProtect
- Restringir su acceso únicamente a redes o direcciones IP autorizadas mediante firewalls, listas blancas o conexiones VPN internas
- Aplicar de forma prioritaria los parches y actualizaciones más recientes de PAN-OS conforme a las directrices oficiales de Palo Alto Networks.

Información adicional:

- https://cybersecuritynews.com/palo-alto-globalprotect-attacks/
- https://blog.elhacker.net/2025/12/ataque-masivo-portales-vpn-palo-alto.html
- https://www.greynoise.io/blog/palo-alto-scanning-surges-90-day-high