Nro. Alerta:	AL-2026-054	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	15-oct-2026	Explotación activa de la vulnerabilidad CVE-2026-0257 en GlobalProtect de Palo Alto Networks para el acceso inicial en operaciones de ransomware Qilin y Settra	Pág.: **1** of **7**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Elusión de autenticación (Authentication Bypass) y acceso no autorizado mediante VPN GlobalProtect.
Nivel de riesgo: Alta

II. ALERTA



Figura 1.- Explotación activa de la vulnerabilidad CVE-2026-0257 en GlobalProtect de Palo Alto Networks para el acceso inicial en operaciones de ransomware Qilin y Settra - figura referencial

La vulnerabilidad CVE-2026-0257, correspondiente a la falla de elusion de autenticación (authentication bypass) en los componentes de portal y gateway de GlobalProtect de las versiones vulnerables de PAN-OS y Prisma Access, de Palo Alto Networks, continúa siendo objeto de explotación por parte de las operaciones de ransomware Qilin y Settra. Esta vulnerabilidad permite a un atacante remoto no autenticado eludir los mecanismos de autenticación, establecer sesiones VPN no autorizadas a través del gateway GlobalProtect de un dispositivo afectado.

III. INTRODUCCIÓN

Unit 42 de Palo Alto Networks observó la explotación activa de la vulnerabilidad CVE-2026-0257 por parte de un atacante no identificado, quien intentó acceder a GlobalProtect.

GlobalProtect es una solución de acceso remoto seguro y conectividad VPN de Palo Alto Networks que permite a los usuarios conectarse de forma segura a los recursos de la red corporativa desde una ubicación externa. Se integra con los firewalls que ejecutan PAN-OS, el sistema operativo de los firewalls de nueva generación (Next-Generation Firewalls, NGFW) de Palo Alto Networks. GlobalProtect cuenta con dos componentes:

GlobalProtect Portal: es el componente encargado de proporcionar al cliente GlobalProtect (usuario final o endpoints) la configuración y los parámetros necesarios para establecer la conexión VPN.

GlobalProtect Gateway: gestiona las conexiones VPN de los usuarios remotos y aplica las políticas de seguridad al tráfico que accede a la red corporativa.

La explotación de la vulnerabilidad CVE-2026-0257 permite a un atacante remoto no autenticado eludir los mecanismos de autenticación de GlobalProtect, bajo determinadas condiciones de configuración y establecer sesiones VPN no autorizadas para obtener acceso inicial a redes internas. Esto la convierte en un vector de acceso relevante para las operaciones de ransomware. Según informes de empresas de ciberseguridad como ReliaQuest y Arctic Wolf, se han identificado campañas activas atribuidas a los grupos de ransomware Qilin y Settra que aprovechan esta falla para acceder a redes corporativas mediante la infraestructura de acceso remoto de GlobalProtect y desplegar malware.

IV. VECTOR DE ATAQUE

Palo Alto asigna a esta vulnerabilidad una puntuación de 4.7 severidad MEDIA de tipo RED, CVSS:3.1/AV: N/AC: L/PR: N/UI: N/S: U/C:H/I:H/A: N

Rapid7 es una empresa global de ciberseguridad que ayuda a las organizaciones a gestionar el riesgo digital, reducir su superficie de ataque y detectar y responder a amenazas. En este contexto, su equipo de MDR (Managed Detection and Response) documentó la actividad relacionada con la explotación de la vulnerabilidad CVE-2026-0257 tras recibir una alerta denominada «Autenticación VPN sospechosa: inicio de sesión en una cuenta local mediante una identidad genérica no humana» (Suspicious VPN Authentication – Local Account Logon via Generic Non-Human Identity).

Durante la primera oleada de actividad, Rapid7 MDR detectó autenticaciones sospechosas mediante cookies en cuentas de administrador local de varios entornos de clientes. Las conexiones se originaron desde la dirección IP 104.207.144[.]154, asociada al proveedor de alojamiento Vultr. Asimismo, se identificó la dirección MAC aa:bb:cc:dd:ee:ff.

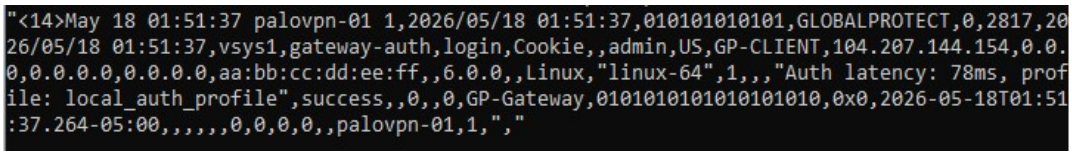

Figura 2.- GlobalProtect Authentication Log, alerta de autenticación VPN sospechosa detectada.

Rapid7 MDR también analizó los archivos de soporte técnico de Palo Alto Networks correspondientes a los clientes afectados y observó que el servicio de autenticación en la nube (Cloud Authentication Service, CAS) estaba deshabilitado y que las cookies de anulación de autenticación (authentication override cookies) estaban habilitadas en el portal o gateway de GlobalProtect. A partir de estos hallazgos, los analistas concluyeron que probablemente se trataba de una explotación de vulnerabilidad (CVE-2026-0257), lo cual fue confirmado posteriormente por Rapid7 Labs al validarlo mediante una prueba de concepto (PoC) exitosa.

Durante una segunda oleada de explotación, Rapid7 MDR identificó una dirección MAC que coincidía con la observada durante la primera oleada, Esta coincidencia llevó a los investigadores a considerar que ambas oleadas fueran llevadas a cabo por el mismo atacante. Sin embargo, la segunda oleada se originó desde una dirección IP diferente, 146.19.216[.]125, asociada al proveedor de alojamiento Dromatics Systems.

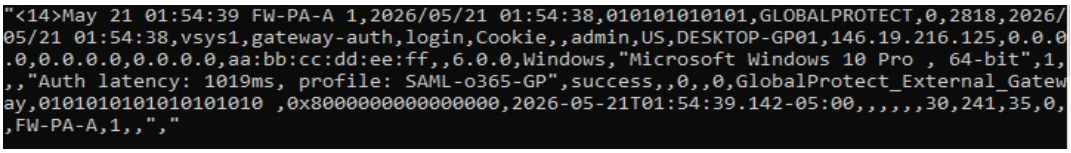

Figura 3.- GlobalProtect Authentication Log, alerta de autenticación VPN sospechosa detectada.

Como parte de la actividad de explotación investigada, Rapid7 observó la asignación de una dirección IP VPN después de la autenticación mediante cookies, lo que permitió a los atacantes acceder a la red interna. En los casos en los que se estableció correctamente un túnel VPN, se detectó solicitudes HTTP POST a los endpoints /ssl-vpn/hipreport.esp, que envía información del perfil de seguridad del dispositivo y /ssl-vpn/getconfig.esp, utilizado para establecer un túnel seguro.

Según el aviso de seguridad de Palo Alto Networks, la vulnerabilidad de omisión de autenticación está relacionada con la funcionalidad anulación de autenticación que permite al portal o al gateway de GlobalProtect emitir/generar cookies a usuarios autenticados, para posteriormente, estas cookies puedan utilizarse en comunicaciones futuras para evitar que el usuario tenga que volver a autenticarse mediante sus credenciales, de forma similar a un

bearer token (token portador). Aunque esta funcionalidad no está habilitada de forma predeterminada.

Además, el aviso señala que la explotación de esta vulnerabilidad es posible cuando se utiliza el mismo certificado para cifrar y descifrar las cookies de anulación de autenticación y para el servicio HTTPS del portal o gateway de GlobalProtect. Esta configuración puede permitir que un atacante remoto no autenticado obtenga la clave pública del certificado y la utilice para falsificar cookies de autenticación, eludiendo así los mecanismos de autenticación.

Para examinar el aspecto de una cookie de anulación de autenticación y cómo se genera, Rapid7 MDR analizó la implementación del binario /usr/local/bin/gpsvc, que implementa el servicio GlobalProtect.

Obteniendo que una de las funciones internas del binario toma el valor de la cookie cifrada recibida, almacenado en portal-userauthcookie o portal-prelogonuserauthcookie, lo descifra y extrae los siguientes datos contenidos en ella:

- Nombre de usuario.
- Nombre del dominio.
- Identificador del equipo (Host ID).
- Sistema operativo del cliente.
- Dirección remota.
- Marca de tiempo (timestamp).

Concluyendo, así que, si un portal o gateway de GlobalProtect reutiliza el certificado empleado para cifrar y descifrar las cookies de anulación de autenticación en el servicio HTTPS del propio portal o gateway, un atacante remoto no autenticado puede obtener la clave pública asociada a dicho certificado. Así, un atacante podrá falsificar y cifrar correctamente cookies de anulación de autenticación arbitrarias y como estas cookies falsificadas podrán descifrarse correctamente en el servidor, serán consideradas confiables y se logrará eludir la autenticación para iniciar sesión y establecer una conexión VPN.

CVE-2026-0257 también ha sido identificado como un vector de acceso inicial utilizado en operaciones atribuidas al grupo de ransomware Qilin. Arctic Wolf documentó la cadena de ataque asociada a esta actividad.

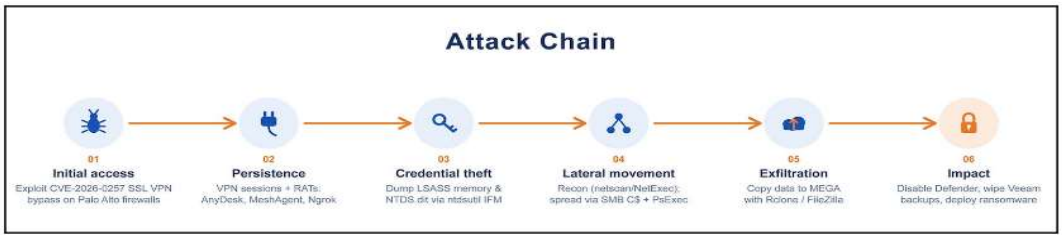

Figura 4.- Cadena de ataque observada por Qilin ransomware.

V. IMPACTO

Producto	Versión
PAN-OS 12.1	< 12.1.4-h6
	< 12.1.7
PAN-OS 11.2	< 11.2.4-h17
	< 11.2.7-h14
	< 11.2.10-h7
	< 11.2.12
PAN-OS 11.1	< 11.1.4-h33
	< 11.1.6-h32
	< 11.1.7-h6
	< 11.1.10-h25
	< 11.1.13-h5
	< 11.1.15
PAN-OS 10.2	< 10.2.7-h34
	< 10.2.10-h36
	< 10.2.13-h21
	< 10.2.16-h7
	< 10.2.18-h6
Prisma Access 11.2.0	< 11.2.7-h13
Prisma Access 10.2.0	< 10.2.10-h36

Tabla 1. - Productos y versiones de PAN-OS y Prisma Access afectados por la vulnerabilidad CVE-2026-0257

VI. INDICADORES DE COMPROMISO

Host Names y Direcciones MAC
aa:bb:cc:dd:ee:ff
00:11:22:33:44:55
WINDOWS-LAPTOP-001
DESKTOP-GP01
GP-CLIENT

Tabla 2.- Nombres de host y direcciones MAC asociados a la actividad de explotación de la vulnerabilidad CVE-2026-0257

Direcciones Ips
23.128.228[.]6
104.207.144[.]154
146.19.216[.]119
146.19.216[.]120
146.19.216[.]125
179.43.172[.]213
185.195.232[.]139
198.12.106[.]60
202.144.192[.]47
216.245.184[.]150
216.245.184[.]47
216.245.184[.]110
216.245.184.0

Tabla 3.- Direcciones IP identificadas como indicadores de compromiso (IoC) relacionados con la explotación de CVE-2026-0257.

VII. RECOMENDACIONES:

- Aplicar el parche CVE-2026-0257 a todas las implementaciones de PAN-OS y Prisma Access con acceso a Internet.
- Deshabilitar las cookies de anulación de autenticación donde no sean necesarias.
- Generar un certificado nuevo dedicado exclusivamente a las cookies de anulación de autenticación.
- Los administradores no deben reutilizar un certificado de portal o gateway GlobalProtect, ni un certificado utilizado previamente para otro servicio.
- Finalice todas las sesiones activas de GlobalProtect después de aplicar el parche.
- Supervisar y restringir la ejecución desde C:\PerfLogs.
- Vigilar conexiones salientes inusuales o a direcciones IP sospechosas que puedan indicar comunicación con servidores de comando y control operadas por ransomware.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

PALO ALTO NETWORKS UNIT 42. (2026). Threat Brief: Active Exploitation of PAN-OS CVE-2026-0257. *https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/*

RAPID7. (2026). Rapid7 Observed Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability (CVE-2026-0257). *https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/*

PALO ALTO NETWORKS. (2026). CVE-2026-0257. *https://security.paloaltonetworks.com/CVE-2026-0257*

CYBERSECURITY NEWS. (2026). CVE-2026-0257: Qilin Ransomware. *https://cybersecurity-news.com/cve-2026-0257-qilin-ransomware/*

GBHACKERS. (2026). Ransomware Hackers Exploit Palo Alto Networks GlobalProtect. *https://gbhackers.com/ransomware-hackers-exploit-palo-alto-networks-globalprotect*