Boletín informativo
“Vulnerabilidad “Palo Alto Networks PAN-OS GlobalProtect Authentication Bypass.

CSIRTSALUD-AV- 20260601-50 **TLP: CLEAR**

Alerta ID:	050
Fecha del reporte:	01/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Palo Alto Networks PAN-OS GlobalProtect Authentication Bypass
Herramienta de detección	N/A
Activo involucrado:	Palo Alto Networks
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una vulnerabilidad crítica denominada **CVE-2026-0257** en Palo Alto Networks PAN-OS y GlobalProtect, que permite **bypassear la autenticación en VPN**, otorgando acceso no autorizado a redes corporativas. Esta falla podría comprometer la confidencialidad, integridad y disponibilidad de los sistemas y datos de pacientes, afectando operaciones críticas de la infraestructura sanitaria.

El propósito de esta alerta es que las organizaciones del sector salud **valide si utilizan versiones afectadas de PAN-OS o GlobalProtect**, tanto en infraestructura propia como en

servicios en la nube o soluciones gestionadas por terceros, revisando inventarios de sistemas críticos, portales VPN, acceso remoto y plataformas de integración de datos clínicos.

Descripción:

CVE-2026-0257 es una vulnerabilidad crítica en **Palo Alto Networks PAN-OS y GlobalProtect** que permite **bypassear la autenticación en VPN**, otorgando acceso remoto no autorizado a redes corporativas. Esta vulnerabilidad fue identificada y reportada por equipos de seguridad y por la propia Palo Alto Networks, siendo catalogada como de **alto riesgo** debido a su explotación activa en entornos reales.

La característica distintiva de esta falla es que permite a un atacante **eludir los mecanismos de autenticación de GlobalProtect**, estableciendo sesiones VPN como si fueran usuarios legítimos sin necesidad de credenciales válidas. Esto permite comprometer la integridad de la red, acceder a recursos internos críticos y dificultar la detección por parte de sistemas de monitoreo o equipos de SOC, ya que el acceso parece provenir de usuarios autorizados.

La explotación exitosa de CVE-2026-0257 permite a los atacantes acceder a información sensible y controlar sesiones VPN, pudiendo realizar movimientos laterales dentro de la infraestructura corporativa. La vulnerabilidad afecta tanto a conexiones de usuarios locales como remotas a través de GlobalProtect Portal y Gateway, y puede comprometer sistemas críticos utilizados en entornos del sector salud, incluyendo servidores de aplicaciones, bases de datos y servicios de acceso remoto.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-0257** puede generar impactos críticos tanto a nivel técnico como operativo en las organizaciones del sector salud. Entre las principales consecuencias se destacan:

Acceso no autorizado a la red: el atacante puede establecer sesiones VPN como usuario legítimo, accediendo a recursos internos críticos.

Evasión de controles de seguridad: las sesiones parecen provenir de usuarios autorizados, dificultando la detección por sistemas de monitoreo o equipos SOC.

Persistencia y escalamiento: el atacante puede mantener acceso prolongado a la red, habilitando movimientos laterales y escalamiento de privilegios hacia sistemas adicionales.

Exfiltración de información sensible: posibilidad de acceder a datos críticos, incluyendo información de pacientes, credenciales, bases de datos clínicas y otros sistemas internos.

Impacto operacional: compromete servicios críticos de infraestructura, pudiendo afectar portales de acceso remoto, sistemas de información hospitalaria (SIH), bases de datos clínicas o plataformas de atención al usuario.

Riesgo regulatorio y reputacional: la exposición de datos de pacientes puede derivar en incumplimiento de la Ley 1581 de 2012 y otras regulaciones de protección de datos, generando daños reputacionales significativos.

Modo de explotación del ataque

La explotación de la vulnerabilidad **CVE-2026-0257** en **Palo Alto Networks PAN-OS y GlobalProtect** puede dividirse en varias fases claramente identificables:

Fase 1 – Acceso inicial al endpoint o red expuesta:

El atacante identifica un portal GlobalProtect o Gateway vulnerable y envía solicitudes específicamente diseñadas para aprovechar la falla de autenticación. Esta fase no requiere credenciales válidas ni interacción del usuario legítimo.

Fase 2 – Bypass de autenticación:

Se manipulan las cookies de override o tokens de sesión de GlobalProtect para eludir la autenticación del portal VPN, permitiendo al atacante establecer una sesión como si fuera un usuario legítimo. Esta técnica permite que el acceso parezca autorizado, dificultando la detección por los sistemas de monitoreo.

Fase 3 – Acceso a la red interna:

Una vez establecida la sesión VPN, el atacante obtiene acceso a la red interna de la organización, incluyendo recursos críticos y sistemas sensibles. Este acceso puede usarse para movimiento lateral y exploración de activos internos.

Fase 4 – Escalamiento y persistencia:

Aunque la vulnerabilidad no concede privilegios de administrador en sí misma, permite al atacante establecer conexiones persistentes y preparar vectores de escalamiento adicionales dentro de la red corporativa.

Fase 5 – Operaciones sobre sistemas internos:

Con el acceso VPN, el atacante puede:

- Enumerar y acceder a servidores, bases de datos y sistemas críticos.
- Exfiltrar información sensible, incluyendo datos de pacientes y credenciales.
- Alterar configuraciones de seguridad o herramientas de monitorización.
- Realizar movimientos laterales a otros sistemas dentro de la infraestructura

Categoría	Capacidades soportadas
Gestión de sesión	Establecimiento de conexiones VPN como usuario autorizado aparente; persistencia de sesión.
Ejecución remota	Acceso no autorizado a la red interna, posibilidad de mover lateralmente.
Operaciones sobre archivos	Posible acceso a recursos compartidos, bases de datos y archivos críticos según permisos de red.
Control de procesos	Acceso a servicios internos y aplicaciones corporativas mediante credenciales comprometidas o sesiones establecidas.
Inventario de software	Posible reconocimiento de servicios y aplicaciones dentro de la red corporativa para planificación de ataques posteriores.

Boletín informativo
“Vulnerabilidad “Palo Alto Networks PAN-OS GlobalProtect Authentication Bypass.

CSIRTSALUD-AV- 20260601-50 **TLP: CLEAR**

Vulnerabilidades asociadas

La vulnerabilidad CVE-2026-0257 se centra en la elusión de autenticación en GlobalProtect VPN, pero su explotación combina varias debilidades y vectores de seguridad que facilitan el acceso no autorizado. Entre los mecanismos más importantes se incluyen:

Bypass de autenticación en VPN: Explotación de un fallo en la validación de cookies o tokens de sesión en GlobalProtect, permitiendo establecer conexiones como usuario legítimo sin credenciales válidas.

Exposición de servicios VPN expuestos a Internet: La vulnerabilidad puede ser aprovechada si los portales GlobalProtect o Gateways no están protegidos por controles adicionales como MFA, restricciones de IP o segmentación de red.

Ausencia de monitoreo de sesiones anómalas: La falta de alertas sobre sesiones inusuales o sobre acceso desde IPs externas permite al atacante mantener el acceso sin ser detectado.

Persistencia y movimiento lateral: La sesión VPN comprometida puede utilizarse para pivotar a otros sistemas internos, acceder a datos sensibles o comprometer servidores y aplicaciones críticas.

Mapeo MITRE ATT&CK:

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Initial Access (TA0001)	T1078	Uso de credenciales o bypass de autenticación en VPN para establecer sesión inicial.

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Execution (TA0002)	T1059	Ejecución de comandos a través de la sesión VPN para explorar la red interna.
Persistence (TA0003)	T1098	Posibilidad de mantener acceso a la red mediante sesiones VPN persistentes.
Privilege Escalation (TA0004)	T1068	Escalamiento posterior mediante vectores internos, aprovechando el acceso VPN inicial.
Defense Evasion (TA0005)	T1027	La sesión comprometida aparenta tráfico legítimo, evadiendo detección por monitoreo de red.
Defense Evasion (TA0005)	T1018	Reconocimiento de sistemas y servicios internos accesibles a través de la VPN comprometida.
Discovery (TA0007)	T1021	Movimiento lateral a servidores, estaciones de trabajo o aplicaciones internas.
Collection (TA0009)	T1119	Acceso a datos críticos y recursos compartidos a través de la sesión comprometida.
Command and Control (TA0011)	T1071	La sesión VPN sirve como canal de comunicación con el atacante, permitiendo control remoto de la infraestructura.
Impact (TA0040)	T1489	Posibilidad de afectar operaciones internas o servicios críticos, dependiendo del acceso obtenido.

Recomendaciones de detección y mitigación

- Los equipos de operaciones de seguridad (SOC, Blue Team) deben implementar y ajustar reglas de detección en sus plataformas SIEM y EDR/XDR, orientadas a identificar patrones característicos de explotación de CVE 2026 0257. Entre las reglas prioritarias se encuentran:
- Monitoreo de accesos VPN no autorizados: Alertar sobre sesiones establecidas sin autenticación válida, especialmente aquellas que parecen provenir de usuarios legítimos pero desde ubicaciones inusuales.
- Detección de bypass de autenticación: Revisar intentos fallidos y exitosos que utilicen técnicas de cookies o tokens manipulados en GlobalProtect.
- Revisión de logs de GlobalProtect Portal y Gateway: Analizar patrones anómalos de conexión, duración de sesión y frecuencia de reintentos desde IP externas.
- Threat hunting proactivo: Buscar conexiones establecidas mediante bypass de autenticación, acceso a recursos internos críticos y tráfico que no corresponda a usuarios autorizados.
- Alertas por actividad lateral sospechosa: Detectar accesos desde sesiones VPN comprometidas a sistemas internos, bases de datos, aplicaciones críticas o servidores de aplicaciones sanitarias.
- Bloqueo o detección de IoC relacionados con la explotación: Incluir direcciones IP o patrones conocidos de explotación de CVE 2026 0257 según reportes oficiales y feeds de inteligencia.
- Verificación de integridad de configuraciones: Revisar que las configuraciones de GlobalProtect y PAN OS no hayan sido modificadas sin autorización.

- Aplicación de principios de mínimo privilegio: Limitar el acceso de usuarios y cuentas administrativas a lo estrictamente necesario para reducir riesgo de escalamiento.
- Uso de MFA y controles complementarios: Implementar autenticación multifactor en VPNs y controles de acceso de red para detectar y prevenir accesos no autorizados.

Recomendaciones de prevención y mitigación

1. En paralelo a la detección, se recomienda aplicar las siguientes medidas de fortalecimiento y prevención para proteger los sistemas ante la vulnerabilidad CVE-2026-0257:
2. Actualizar PAN-OS y GlobalProtect: Aplicar inmediatamente la versión parcheada distribuida por Palo Alto Networks para cerrar la vulnerabilidad.
3. Restringir accesos administrativos: Limitar el uso de cuentas con privilegios para la administración de GlobalProtect y PAN-OS, asegurando que solo personal autorizado pueda realizar cambios críticos.
4. Implementar autenticación multifactor (MFA): Reforzar la autenticación de usuarios VPN, asegurando que incluso si se aprovecha el bypass de autenticación, la sesión requiera un segundo factor de verificación.
5. Segmentación de red y control de accesos: Limitar el acceso de las sesiones VPN solo a recursos necesarios; separar sistemas críticos y sensibles de accesos generales de usuarios.
6. Monitoreo de sesiones anómalas: Revisar logs de GlobalProtect y PAN-OS para detectar patrones sospechosos, incluyendo sesiones iniciadas desde IPs externas, duración inusual o comportamientos de movimiento lateral.

7. Inspección de tráfico y políticas de firewall: Configurar inspección profunda de paquetes (DPI) y bloquear accesos a servicios no autorizados o tráfico que indique posibles abusos de la sesión VPN.
8. Auditoría y control de configuraciones: Revisar periódicamente que no se hayan realizado cambios no autorizados en las configuraciones de GlobalProtect y PAN-OS.
9. Fortalecimiento de EDR/XDR: Mantener actualizadas las soluciones de detección con reglas de comportamiento que identifiquen accesos no autorizados o anomalías de VPN.
10. Pruebas de penetración y ejercicios de red team: Simular ataques para evaluar la efectividad de controles, detección de bypass de autenticación y respuesta a incidentes.
11. Aplicar el principio de mínimo privilegio: Limitar que los usuarios finales tengan permisos de administrador en endpoints y accesos innecesarios a la infraestructura de red.

Recomendaciones de respuesta ante compromiso

En caso de confirmarse o sospecharse explotación de CVE-2026-0257, se recomienda ejecutar el siguiente procedimiento de contención y erradicación:

- **Aislar inmediatamente la sesión VPN comprometida**: Desconectar la conexión GlobalProtect afectada de la red corporativa para evitar movimientos laterales, sin cerrar la sesión de manera que se pueda preservar evidencia de la actividad.
- **Captura de registros y artefactos clave:** Recolectar logs de PAN-OS, GlobalProtect Portal y Gateway, registros de firewall, y cualquier alerta o evento inusual registrado en SIEM/EDR para análisis forense.

- **Revocar y restablecer credenciales comprometidas:** Cambiar contraseñas de usuarios afectados y habilitar MFA si no estaba activado, además de revisar tokens o sesiones persistentes.
- **Revisión de configuraciones críticas:** Validar que las políticas de autenticación, certificados y reglas de acceso de GlobalProtect no hayan sido alteradas por el atacante.
- **Monitoreo de accesos y tráfico de red:** Analizar conexiones VPN recientes, patrones de tráfico anómalos y accesos a sistemas internos críticos para detectar actividad lateral o escalamiento.
- **Evaluar sistemas internos potencialmente comprometidos:** Revisar servidores, bases de datos y aplicaciones críticas que pudieron ser accedidos a través de la sesión comprometida.
- **Comunicación y reporte:** Notificar al equipo de seguridad, al CSIRT interno, y según corresponda, a autoridades regulatorias o entidades de cumplimiento, especialmente si la información sensible del sector salud ha sido afectada.
- **Restauración y remediación:** Considerar la revocación de sesiones, reconfiguración de VPN, reinstalación de componentes críticos si no es posible garantizar la integridad de los sistemas afectados, y aplicar parches de seguridad oficiales de PAN-OS.
- **Auditoría post-incidente:** Realizar un análisis posterior al incidente para validar la eficacia de las medidas de contención, detectar vulnerabilidades residuales y fortalecer controles de seguridad para prevenir futuras explotaciones.

Fuentes:

- **Palo Alto Networks Security Advisory**: Boletín oficial de actualización y mitigación de CVE-2026-0257. Disponible en: https://security.paloaltonetworks.com/CVE-2026-0257
- **CISA – Known Exploited Vulnerabilities Catalog**: Inclusión de CVE-2026-0257 como vulnerabilidad explotada. Disponible en: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Threat Intelligence Reports – CVE-2026-0257**: Análisis de explotación activa y vectores de ataque. Disponible en: https://www.threatclaw.ai/cve/CVE-2026-0257
- **MITRE ATT&CK Framework for Enterprise:** Referencias a tácticas y técnicas aplicables a la explotación de autenticación y movimiento lateral. Disponible en: https://attack.mitre.org/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.