# Boletín informativo
# Vulnerabilidad de Denegación de Servicio en PAN-OS

**CSIRTSALUD-AV-20260225-31** **TLP: CLEAR**

| | |
|---|---|
| **Incidente ID:** | 031 |
| **Fecha del reporte:** | 25/02/2026 |
| **Entidad:** | Todas las Entidades del Ecosistema Digital |
| **Título:** | Vulnerabilidad de Denegación de Servicio en PAN-OS |
| **Herramienta de detección** | N/A |
| **Activo involucrado:** | Palo Alto Networks |
| **Tipo de incidente:** | Boletín informativo |
| **Nivel de riesgo:** | Medio |

## Objetivo:

Informar a las entidades del Ecosistema sobre la vulnerabilidad crítica CVE-2026-0229, descubierta en el motor de Advanced DNS Security (ADNS) de los sistemas PAN-OS de Palo Alto Networks. Este documento está dirigido a equipos de Centros de Operaciones de Seguridad (SOC), CSIRT y administradores de infraestructura de red para facilitar la detección temprana, comprensión técnica y la remediación inmediata de la amenaza sobre el perímetro de red.


## Descripción:

La vulnerabilidad CVE-2026-0229 cuenta con un puntaje CVSSv4.0 de 6.6 (Severidad Media) y un vector de ataque de red:
**(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)**.
A pesar de su clasificación media, representa un riesgo crítico para la disponibilidad del negocio.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Permite a un atacante remoto y no autenticado forzar el colapso del plano de datos (dataplane) del firewall mediante la inyección de paquetes de red malformados. Si la ráfaga de paquetes manipulados es sostenida, el firewall entra en un ciclo infinito de reinicios (Reboot Loop). Tras múltiples fallos críticos consecutivos en el núcleo de procesamiento, PAN-OS transiciona el dispositivo automáticamente al Modo de Mantenimiento (Maintenance Mode), interrumpiendo el enrutamiento, la inspección de tráfico y desconectando la red de manera indefinida hasta la intervención manual.

Una vez que el ataque tiene éxito y el equipo es forzado a entrar en modo de mantenimiento, la infraestructura y la organización enfrentan los siguientes impactos:

- **Interrupción Total del Perímetro (Downtime):** Pérdida absoluta de conectividad hacia y desde el exterior. Esto paraliza el enrutamiento y la inspección de tráfico, cortando transacciones comerciales, túneles VPN de usuarios remotos (IPSec/SSL) y el acceso a servicios críticos alojados detrás del firewall.

- **Colapso de la Segmentación Interna:** Si el firewall afectado actúa como núcleo para la segmentación de redes internas (arquitecturas *Zero Trust* o enrutamiento inter-VLAN), su caída aísla por completo los diferentes segmentos corporativos, impidiendo la comunicación vital entre servidores de aplicaciones, bases de datos y usuarios locales.

- **Ceguera Operativa para el SOC/CSIRT (Pérdida de Telemetría):** Al colapsar el plano de datos, el dispositivo deja de generar y enviar registros de eventos, tráfico y amenazas (Syslog/NetFlow) hacia el SIEM central. Esta pérdida repentina de visibilidad perimetral puede ser aprovechada por actores de amenazas como cortina de humo para ocultar movimientos laterales u otros ataques simultáneos.

- **Degradación en Clústeres de Alta Disponibilidad (HA):** En topologías Activo-Pasivo o Activo-Activo, los reinicios continuos del plano de datos provocan conmutaciones por

error (*failovers*) caóticas. Si el tráfico malicioso inyectado alcanza o se sincroniza con el resto de los nodos, todo el clúster puede experimentar una caída en cascada, anulando por completo la resiliencia de la arquitectura.

- **Impacto Operacional Prolongado:** A diferencia de una caída de servicio estándar, el estado de *Maintenance Mode* requiere, en la mayoría de los casos, intervención manual por parte de un administrador (a través de acceso de consola fuera de banda o reinicios físicos) para recuperar el equipo, prolongando drásticamente el Tiempo Medio de Recuperación (MTTR).

## Productos afectados:

La vulnerabilidad afecta a las siguientes versiones de PAN-OS:

**Vulnerables:** PAN-OS 12.1 (versiones 12.1.0 hasta 12.1.3) y PAN-OS 11.2 (versiones 11.2.0 hasta 11.2.9).

**No Afectados:** PAN-OS 11.1, PAN-OS 10.2, Cloud NGFW, y Prisma Access.

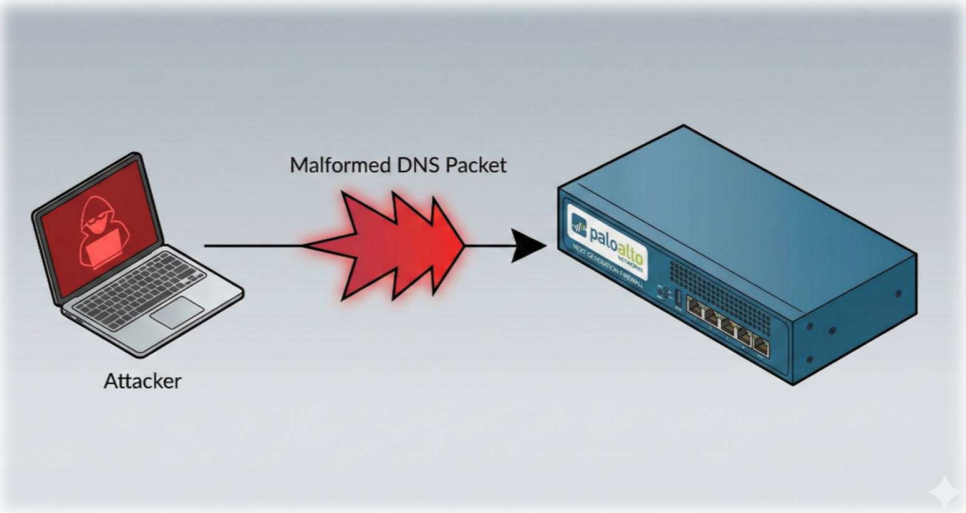
## Modo de explotación y cadena de infección

La vulnerabilidad radica en un fallo crítico de manejo de excepciones (CWE-754) dentro del subsistema de inspección de Capa 7 (Content-ID) de PAN-OS, específicamente en las rutinas de memoria que gestionan la función de **Advanced DNS Security (ADNS)**.

Para que la explotación sea exitosa, la topología lógica y el flujo de procesamiento de paquetes (*packet flow*) deben alinearse con la siguiente secuencia técnica:

**Fase 1: Precondiciones lógicas en el Motor de Políticas** El vector de ataque requiere que el firewall receptor tenga una configuración específica en su plano de control (*control plane*) que instruya al plano de datos (*dataplane*) a inspeccionar el tráfico entrante de una manera particular:

- El tráfico inyectado debe coincidir con una regla de seguridad (*Security Policy*) que tenga adjunto un **Perfil Antispyware**.
- Dicho perfil debe tener configurada una acción de inspección activa (block, sinkhole o alert).
- La licencia y funcionalidad de **Advanced DNS Security** deben estar operativas y enlazadas a ese motor de inspección.




**Fase 2: Inyección y Análisis de Flujo (Ingress & Flow Logic)** El adversario envía un paquete de red malformado (típicamente manipulando cabeceras o payloads de protocolos que el firewall intenta interpretar como tráfico DNS para su análisis).

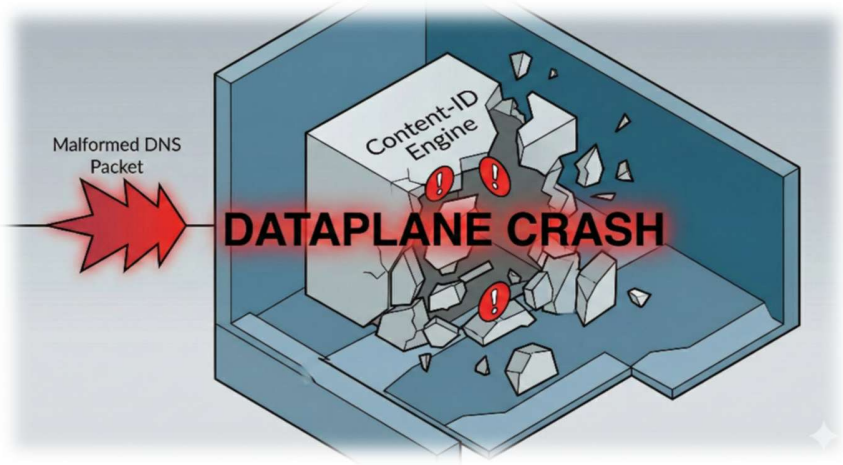
1. El paquete ingresa por una interfaz perimetral.

2. El procesador de red (NPU) o los hilos de trabajo del plano de datos (pan_task) realizan el análisis de las capas 2 a 4.
3. El motor de App-ID identifica el flujo y lo transfiere al motor de Content-ID para la inspección de amenazas.

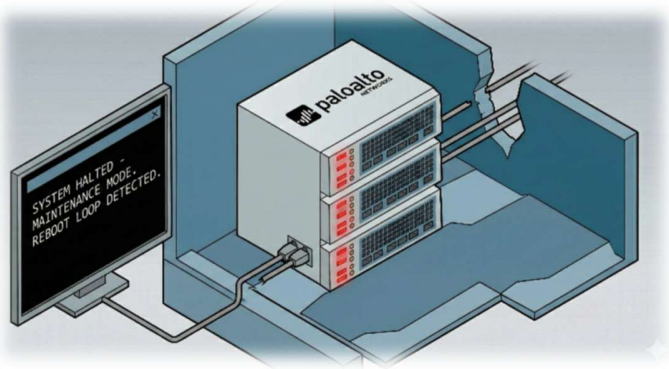
**Fase 3: Trigger de la Vulnerabilidad (Excepción no Controlada)** Al llegar al módulo de ADNS, el código base de PAN-OS (escrito típicamente en C/C++) intenta analizar (hacer *parsing*) de la estructura del paquete malformado. Debido a la debilidad **CWE-754**, el desarrollador no incluyó rutinas de validación exhaustivas (como comprobación de límites de memoria o desreferenciación de punteros nulos) para las condiciones anómalas presentes en este payload específico. Al intentar procesar campos inválidos, el hilo de ejecución genera una excepción fatal (por ejemplo, un *Segmentation Fault* o SIGSEGV) a nivel de memoria del sistema operativo.

**Fase 4: Caída del Hilo y Condición de Carrera (Reboot Loop)**

1. La excepción no controlada provoca el colapso inmediato del proceso principal del plano de datos que estaba inspeccionando ese tráfico.
2. El demonio de supervisión del sistema operativo (watchdog del *control plane*) detecta que el proceso del *dataplane* ha muerto de forma abrupta e intenta reiniciarlo para recuperar el enrutamiento y la inspección.
3. Si el atacante envía un flujo constante de estos paquetes (ataque volumétrico o sostenido), en el momento exacto en que el *dataplane* vuelve a levantarse e intenta procesar el búfer de entrada, el nuevo paquete vuelve a causar un *crash*.




**Fase 5: Aislamiento por Hardware/Software (Maintenance Mode)** Los sistemas integrados de alta disponibilidad y gestión de fallos de PAN-OS tienen umbrales de tolerancia. Si el proceso del *dataplane* (o el propio *kernel*) colapsa un número predeterminado de veces dentro de una ventana de tiempo corta (ciclo de pánico del kernel), el sistema operativo asume que existe una falla crítica e irrecuperable. Para evitar daños a nivel de corrupción de estado o envíos de tráfico anómalo, el sistema aborta el arranque normal y transiciona la unidad completa a **Maintenance Mode**, aislando el equipo de la red y requiriendo intervención técnica directa.




**Relación con las Tácticas según MITRE ATT&CK**

El comportamiento explotatorio de esta vulnerabilidad se encuadra dentro de las siguientes categorías del marco MITRE ATT&CK:

- **Táctica:** Impacto (TA0040) - El adversario interrumpe la disponibilidad operacional para afectar directamente la productividad o aislar servicios de red.
- **Técnica:** Network Denial of Service (T1498) / Service Exhaustion Flood (T1498.001) - Uso de tráfico especialmente diseñado para agotar la capacidad de procesamiento del dispositivo, degradándolo hasta la inhabilitación total del perímetro y provocando disrupción corporativa.

## Indicadores de compromiso:

El fabricante y las firmas de inteligencia de amenazas reportan que la "Madurez del Exploit" (Exploit Maturity) se encuentra en estado **Unreported**. Actualmente no existen exploits públicos ni evidencia de explotación activa (*in-the-wild*). Por tanto, no hay hashes, IPs o dominios asociados. La detección debe centrarse en la telemetría operativa:

- Patrones en el system log o envío de traps SNMP que alerten sobre caídas del proceso de red en ventanas de tiempo recurrentes (ej. fallos sucesivos cada 10-15 minutos).

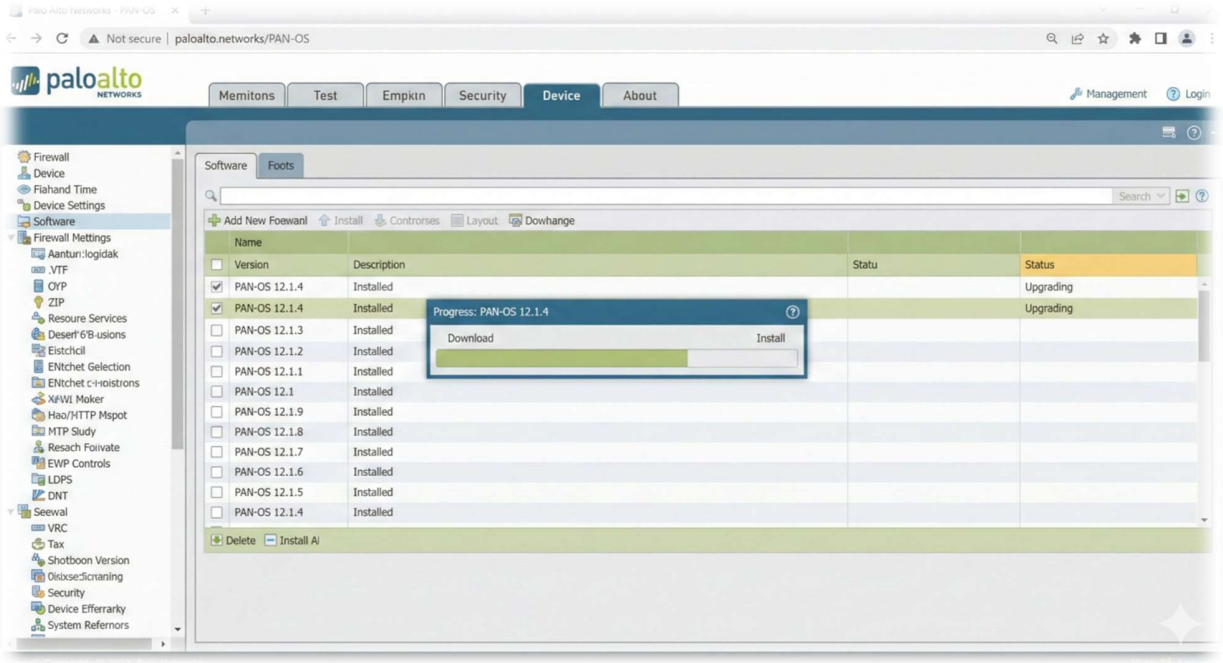
- Alertas del sistema advirtiendo el paso a *Maintenance Mode* fuera de ventanas de mantenimiento aprobadas.

- Flaps y conmutaciones por error (failovers) anormales y continuos entre nodos Activo-Pasivo en configuraciones de Alta Disponibilidad.

## Recomendaciones de mitigación:

La única solución oficial y permanente para mitigar la vulnerabilidad **CVE-2026-0229** es elevar la versión del sistema operativo (PAN-OS) en una ventana de mantenimiento crítica.

- Para la rama **12.1**: Instalar la versión **12.1.4** o superior.
- Para la rama **11.2**: Instalar la versión **11.2.10** o superior.




*(Nota: PAN-OS 11.1, 10.2, Cloud NGFW y Prisma Access no están afectados).*

Antes de iniciar cualquier actualización, **es obligatorio generar y exportar un respaldo de la configuración actual** (Device > Setup > Operations > Export named configuration snapshot). Una vez asegurado el respaldo, proceda con uno de los siguientes métodos:

- **Método 1: Directamente desde la Consola de Administración (Recomendado)** Este método aplica si el firewall tiene conectividad a internet para alcanzar los servidores de actualización de Palo Alto Networks.

1. Ingrese a la interfaz web (GUI) del firewall con credenciales de administrador.
2. Navegue a la pestaña **Device** > **Software**.
3. Haga clic en **Check Now** (Verificar ahora) en la parte inferior para refrescar la lista de versiones disponibles.
4. Localice la versión objetivo (ej. 12.1.4 o 11.2.10).
5. Haga clic en **Download** (Descargar) en la columna de acción.
6. Una vez finalizada la descarga, haga clic en **Install** (Instalar).
7. El sistema requerirá un **Reboot** (reinicio) para aplicar los cambios en el plano de control y plano de datos.

- **Método 2: Descarga Manual desde el Portal de Soporte (Para redes aisladas / Air-gapped)** Este método aplica si el firewall perimetral no tiene resolución DNS externa o políticas que le permitan descargar directamente el software.

1. Ingresar al **Customer Support Portal (CSP)** de Palo Alto Networks (https://www.google.com/search?q=support.paloaltonetworks.com) desde un equipo con acceso a internet.
2. Ir a la sección de **Updates** > **Software Updates** y seleccionar el modelo de su firewall y la versión de PAN-OS requerida.
3. Descargar el archivo de imagen de PAN-OS al equipo local.
4. Ingresar a la consola de administración del firewall vulnerable, ir a **Device** > **Software** y haga clic en **Upload** (Cargar).
5. Seleccionar el archivo descargado. Una vez cargado, hacer clic en **Install from file** (Instalar desde archivo) y proceder con el reinicio.

- **Consideraciones para Alta Disponibilidad (HA):** Si los firewalls operan en un clúster Activo-Pasivo, el proceso debe seguir las mejores prácticas de cero tiempo de inactividad (*Zero Downtime Upgrade*):

    1. Suspender el nodo Activo actual para forzar el *failover*.
    2. Actualizar primero el nodo Pasivo (ahora Activo) y reiniciarlo.
    3. Verificar la estabilidad de la red y proceder a actualizar el nodo restante.

**Mitigaciones y Limitaciones del Entorno:**

- El boletín oficial establece explícitamente que **no existen workarounds oficiales**.
- **No es posible generar firmas IPS:** Debido a que el vector de explotación explota un error en los mecanismos base con los que el equipo captura y analiza el tráfico de amenazas, es arquitectónicamente imposible crear una firma de Prevención de Amenazas (Threat Prevention Signature) para bloquear el ataque perimetralmente antes de que se evalúe.

En escenarios críticos donde un ataque DoS está en curso imposibilitando la operación, y un parcheo no pueda ejecutarse de manera oportuna, la administración técnica podría evaluar el riesgo de cambiar de forma temporal las acciones de block/sinkhole/alert a allow en el perfil de Spyware para la función de DNS Avanzado. Sin embargo, esto reducirá de manera severa la capacidad del firewall para detener intrusiones basadas en DNS, por lo que requiere aprobación del nivel ejecutivo bajo riesgo documentado hasta el momento de su actualización oficial.

## Fuentes:

- https://security.paloaltonetworks.com/CVE-2026-0229
- https://www.csirt.gob.bo/es/alertas-de-seguridad/vulnerabilidad-cve-2026-0229-denegacion-de-servicio-dos-en-el-motor-de

- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-denegacion-de-servicio-en-pan-os-de-palo-alto-networks-2/
- https://blog.elhacker.net/2026/02/vulnerabilidad-en-firewall-de-palo-alto.html
- https://nvd.nist.gov/vuln/detail/CVE-2026-0229
- https://radar.offseq.com/threat/cve-2026-0229-cwe-754-improper-check-for-unusual-o-3f546358

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 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.