Boletín de alerta

Boletín Nro.: 47
Fecha de publicación: 07/05/2026
Tema: Alerta 2026-47 Vulnerabilidad Crítica Zero Day en Palo Alto PAN-OS
Traffic Light Protocol (TLP): White

Actualización: 14/05/2026

Producto(s) afectado(s):

La vulnerabilidad afecta a los firewalls PA-Series y VM-Series que ejecutan PAN-OS con el servicio **User-ID Authentication Portal (Captive Portal)** habilitado y expuesto a redes no confiables o a Internet.

Versiones afectadas reportadas:

- PAN-OS 12.1 anteriores a:
  - **12.1.4-h5**
  - **12.1.7**
- PAN-OS 11.2 anteriores a:
  - **11.2.4-h17**
  - **11.2.7-h13**
  - **11.2.10-h6**
  - **11.2.12**
- PAN-OS 11.1 anteriores a:
  - **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 anteriores a:
  - 10.2.7-h34
  - 10.2.10-h36
  - 10.2.13-h21
  - 10.2.16-h7

Descripción

Se reporto una vulnerabilidad crítica identificada como CVE-2026-0300, la cual afecta al componente User-ID Authentication Portal (Captive Portal) de PAN-OS, sistema operativo utilizado en sus firewalls empresariales PA-Series y VM-Series. La falla posee un puntaje CVSS v4 de 9.3, siendo clasificada como crítica, y ya se encuentra siendo explotada activamente en ataques reales limitados.

La vulnerabilidad corresponde a un buffer overflow / out-of-bounds write (CWE-787) que puede ser explotado remotamente por un atacante no autenticado mediante el envío de paquetes especialmente diseñados hacia el portal de autenticación. La explotación exitosa permite ejecutar código arbitrario con privilegios root, otorgando control total sobre el firewall comprometido.

De acuerdo con los análisis publicados por diversos investigadores y organismos de ciberseguridad, el riesgo es considerablemente mayor cuando el servicio Captive Portal está expuesto directamente a Internet o accesible desde redes no confiables. Debido a que la explotación no requiere autenticación ni interacción del usuario, el vector de ataque resulta especialmente atractivo para actores maliciosos y grupos de ransomware.

Adicionalmente, la vulnerabilidad ya fue catalogada con estado “ATTACKED” por el fabricante, indicando evidencia de explotación activa en entornos reales. Organizaciones con firewalls expuestos podrían ser vulnerables a compromisos completos del perímetro de red, movimiento lateral y despliegue de malware o ransomware.

Solución:

Palo Alto Networks publicó actualizaciones de seguridad para corregir la vulnerabilidad y recomienda aplicar los parches inmediatamente en todos los dispositivos afectados.

Las principales recomendaciones incluyen:

- Actualizar PAN-OS a una versión corregida lo antes posible.
- Restringir el acceso al servicio **User-ID Authentication Portal** únicamente a direcciones IP confiables.
- Evitar exponer el Captive Portal directamente a Internet.
- Deshabilitar temporalmente el servicio si no es estrictamente necesario.
- Monitorear logs y actividad sospechosa relacionada con autenticaciones o tráfico anómalo hacia el portal.

El advisory oficial y los parches pueden consultarse en:

- **Advisory oficial de Palo Alto Networks**

Compartimos a continuación una guía oficial para el actualizar los sistemas PAN-OS

- **https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/pan-os-software-updates**

Se ha hecho pública una vulnerabilidad crítica identificada como **CVE-2026-0300** en el **User-ID Authentication Portal (Captive Portal) de PAN-OS**, que permite ejecución remota de código como **root** en firewalls PA-Series y VM-Series sin credenciales ni interacción del usuario, mediante paquetes

especialmente construidos. Palo Alto Networks y varios CERT han confirmado que esta vulnerabilidad se encuentra **bajo explotación activa en el mundo real**, con campañas atribuidas a un cluster probablemente patrocinado por estados (CL□STA□132), incluyendo intentos y compromisos exitosos desde el 9 de abril de 2026, limpieza de logs, inyección de shellcode en procesos `nginx` y movimientos laterales posteriores.

Información adicional:

- **Critical Palo Alto Firewalls Vulnerability Exploited in the Wild to Gain Root Access**
- **https://security.paloaltonetworks.com/CVE-2026-0300**
- **https://thehackernews.com/2026/05/palo-alto-pan-os-flaw-under-active.html**