I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Ejecución remota de código (RCE)
Nivel de riesgo: Alta

II. ALERTA

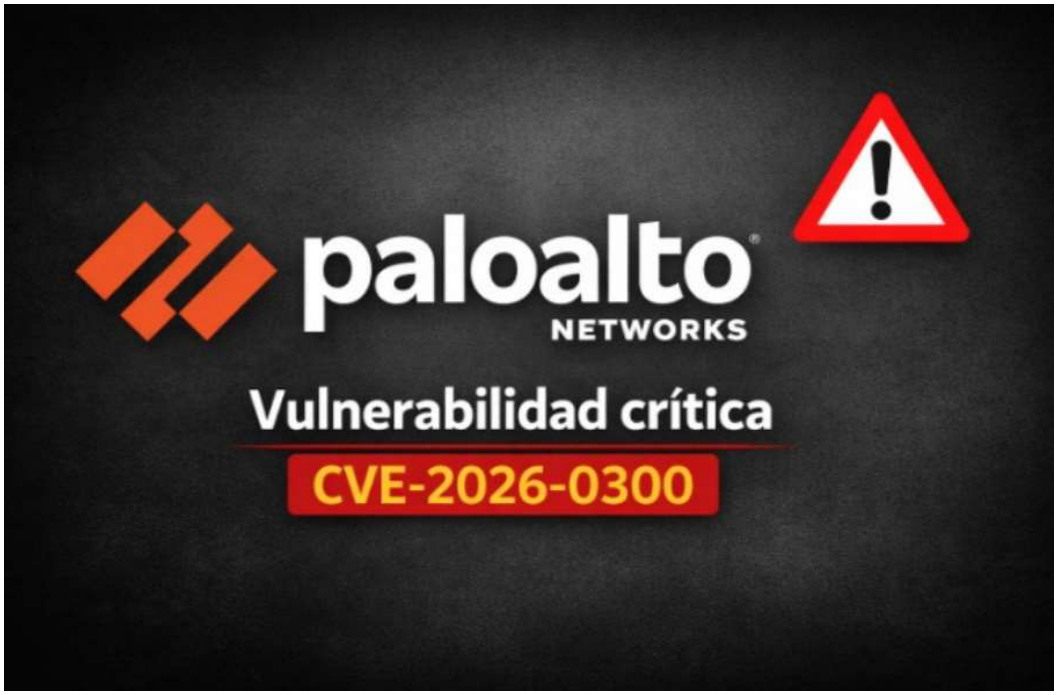

Figura 1.- Vulnerabilidad crítica en PAN-OS permite ejecución remota de código sin autenticación (CVE-2026-0300) - figura referencial

Palo Alto Network ha anunciado sobre una vulnerabilidad critica de 0-day en su PAN-OS, denominada como CVE-2026-0300, la falla se debe al desbordamiento de búfer en el servicio User-IDTM Authentication Portal que permite a un atacante no autenticado ejecute código arbitrario con privilegios de root en los firewalls de las series PA-Series y VM-Series al enviar paquetes especialmente diseñados.

III. INTRODUCCIÓN

El gigante de la ciberseguridad Palo Alto Networks informó sobre una vulnerabilidad 0-day clasificada como crítica, originada por un desbordamiento de búfer que afecta al

servicio Portal de Autenticación de User-ID (Captive Portal) en PAN-OS, el sistema operativo de sus firewalls de próxima generación (NGFW).

En concreto, CVE-2026-0300 impacta únicamente a los firewalls de las series PA y VM que tienen habilitado el Captive Portal. Cuando este servicio está expuesto a internet u otras redes no confiables, queda susceptible a explotación sin necesidad de autenticación, ni interacción del usuario. Un atacante puede aprovechar esta condición para lograr la ejecución remota de código (RCE) con privilegios de root, tras esta explotación exitosa, el atacante fue capaz de inyectar shellcode mediante el envío de paquetes de red especialmente diseñados en un proceso de trabajo de nginx.

La actividad posterior a la explotación incluye la implementación de herramientas de túneles disponibles públicamente (EarthWorm, ReverseSocks5), la enumeración de Active Directory utilizando credenciales probablemente obtenidas del firewall y la destrucción sistemática de registros y otras pruebas de compromiso.

Con esto Palo Alto reporta la explotación, limitada en entornos y dirigida principalmente a portales expuestos a internet y redes no confiables. Como medida preventiva, recomiendan deshabilitar este portal si no es estrictamente necesario. Asimismo, la compañía prevé la publicación de una primera ronda de parches el 13 de mayo, seguida de una segunda actualización programada para el 28 de mayo.

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2026-0300 tiene un vector de ataque tipo RED CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V con nivel de severidad 9.3 CRITICA.

Palo Alto informa que el payload no es un malware que se descarga en el disco, sino una secuencia de paquetes maliciosos enviada al componente Captive Portal.

A comienzos de abril de 2026, se produjeron intentos fallidos de explotación contra un dispositivo PAN-OS. Una semana más tarde, los atacantes lograron la ejecución remota de código (RCE) en el dispositivo e inyectaron shellcode. Tras el compromiso, los atacantes procedieron inmediatamente a limpiar los registros para evitar la detección, borrando los mensajes de fallo del kernel, eliminando las entradas y los registros de fallos de nginx, así también como la eliminación de los archivos de volcado de memoria de los fallos.

Cuatro días después, los atacantes implementaron varias herramientas con privilegios de root, antes de llevar a cabo una enumeración de Active Directory (AD) utilizando las credenciales de la cuenta de servicio del firewall para acceder al domain root y DomainDnsZones. Tras la enumeración, los atacantes eliminaron del registro de auditoría las pruebas de la inyección ptrace y borraron el binario de escalada de privilegios SetUserID (SUID).

Para finales de abril, los atacantes llevaron a cabo otro ataque, uno de inundación de SAML (Security Assertion Markup Language) contra el dispositivo que había sido previamente atacado, lo que promovió a un segundo dispositivo al estado Activo, heredando el mismo tráfico hacia internet. Luego lograron el RCE en el segundo dispositivo, donde se descargaron las herramientas open source EarthWorm y ReverseSocks5.

Con Earthworm, los atacantes tenían una herramienta de túneles de red escrita en lenguaje C que funciona en Windows, Linux, macOS y plataformas basadas en ARM/MIPS. Actúa como servidor SOCKS v5 y la utilidad de hacer port forwarding, está diseñada para establecer canales de comunicación encubiertos a través de límites de red restringidos. Entre sus capacidades están:

- Inicia un servidor SOCKS5 de reenvío para actuar como proxy de las conexiones entrantes (T1090)
- Establecer túneles SOCKS5 inversos desde hosts internos a puentes externos controlados por el atacante (T1090).
- Conecta datos entre dos puertos de escucha separados para facilitar la gestión de pivotes (T1090).
- Reenvía el tráfico desde un puerto local a un host y puerto de destino remotos (T1090).
- Encadena múltiples modos de transferencia para crear túneles de red en cascada de múltiples saltos (T1572).
- Encapsula el tráfico de protocolos como RDP y SSH dentro de túneles SOCKS (T1572).

En ReverseSocks5, la herramienta de red es utilizada para eludir firewalls o NAT estableciendo una conexión saliente desde un equipo de destino hacia un controlador, y no en sentido contrario.

Una vez que establecían la conexión, crean un túnel proxy SOCKS5 que permite al controlador enrutar el tráfico hacia la red interna del dispositivo víctima. Dado que el

código fuente está disponible públicamente, los administradores de sistemas lo utilizan con frecuencia para la gestión remota y también los atacantes para hacer pivote durante una intrusión.

V. IMPACTO

Versión	Afectado	No afectado / Corregido
NGFW en la nube	No aplica	Todas las versiones
PAN-OS 12.1	< 12.1.4-h5 / < 12.1.7	≥ 12.1.4-h5 (ETA: 13/05/2026) ≥ 12.1.7 (ETA: 28/05/2026)
PAN-OS 11.2	< 11.2.4-h17 / < 11.2.7-h13 / < 11.2.10-h6 / < 11.2.12	≥ 11.2.4-h17 (ETA: 28/05/2026) ≥ 11.2.7-h13 (ETA: 13/05/2026) ≥ 11.2.10-h6 (ETA: 13/05/2026) ≥ 11.2.12 (ETA: 28/05/2026)
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	≥ 11.1.4-h33 (ETA: 13/05/2026) ≥ 11.1.6-h32 (ETA: 13/05/2026) ≥ 11.1.7-h6 (ETA: 28/05/2026) ≥ 11.1.10-h25 (ETA: 13/05/2026) ≥ 11.1.13-h5 (ETA: 13/05/2026) ≥ 11.1.15 (ETA: 28/05/2026)
PAN-OS 10.2	< 10.2.7-h34 / < 10.2.10-h36 / < 10.2.13-h21 / < 10.2.16-h7 / < 10.2.18-h6	≥ 10.2.7-h34 (ETA: 28/05/2026) ≥ 10.2.10-h36 (ETA: 13/05/2026) ≥ 10.2.13-h21 (ETA: 28/05/2026) ≥ 10.2.16-h7 (ETA: 28/05/2026) ≥ 10.2.18-h6 (ETA: 13/05/2026)
Prisma Access	No aplica	Todas las versiones

Tabla 1.- Sistemas afectados y corregidos – Vulnerabilidad crítica en PAN-OS permite ejecución remota de código sin autenticación (CVE-2026-0300)

VI. INDICADORES DE COMPROMISO

Categoría	Indicador de Compromiso (IOC)	Descripción
Hash SHA-1	d60e484f8681bd4ca03c2632d2b9409ccc3e1424	Hash SHA-1 identificado en muestra maliciosa

Categoría	Indicador de Compromiso (IOC)	Descripción
Hash SHA-256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dcd84f97a584	Hash SHA-256 identificado en muestra maliciosa
IP / Infraestructura	67.206.213[.]86	Dirección IP asociada a infraestructura sospechosa
IP / Infraestructura	136.0.8[.]48	Dirección IP asociada a actividad maliciosa
IP / Infraestructura	146.70.100[.]69	Servidor C2 Staging
IP / Infraestructura	149.104.66[.]84	Dirección IP asociada a infraestructura sospechosa
URL maliciosa	hxxp[:]//146.70.100[.]69:8000/php_sess	Descarga de EarthWorm
URL maliciosa	hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz	Descarga de ReverseSocks5
User-Agent	Safari/532.31 Mozilla/5.5 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0	Cadena User-Agent utilizada por el atacante
Ruta / Archivo	/var/tmp/linuxap	Herramienta de túnel
Ruta / Archivo	/var/tmp/linuxda	Herramienta de túnel
Ruta / Archivo	/var/tmp/linuxupdate	Herramienta de túnel
Ruta / Archivo	/tmp/.c	Script Python no identificado
Ruta / Archivo	/tmp/R5	Binario ReverseSocks5
Ruta / Archivo	/var/R	Binario ReverseSocks5

Tabla 2.- Indicadores de compromiso - Vulnerabilidad crítica en PAN-OS permite ejecución remota de código sin autenticación (CVE-2026-0300)

VII. RECOMENDACIONES:

- Aplicar parches de seguridad inmediatamente. Actualizar a las versiones corregidas de PAN-OS tan pronto estén disponibles, según el fabricante.
- Evitar la exposición a Internet de interfaces críticas. Restringir el acceso a portales User-ID y de administración mediante VPN o listas de control de acceso (ACL).

- Implementar segmentación de red para limitar el acceso a los dispositivos desde redes externas o no confiables.
- Monitorear eventos y registros (logs), especialmente accesos a interfaces web, intentos de conexión no autorizados y actividades inusuales en el sistema.
- Aplicar controles de acceso robustos, como autenticación multifactor (MFA) y restricción de accesos administrativos por dirección IP.
- Deshabilitar servicios innecesarios para reducir la superficie de ataque, especialmente aquellos expuestos externamente.
- Realizar auditorías de seguridad en la configuración de PAN-OS y verificar posibles compromisos.
- Implementar mecanismos de detección de intrusiones (IDS/IPS) con firmas actualizadas.
- Aislar los sistemas en caso de sospecha de compromiso y realizar análisis forense.

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 (2026). CVE-2026-0300. *https://security.paloaltonetworks.com/CVE-2026-0300*

THE HACKER NEWS (2026). Palo Alto PAN-OS flaw under active exploitation. *https://thehackernews.com/2026/05/palo-alto-pan-os-flaw-under-active.html*

SOC PRIME (2026). CVE-2026-0300 Analysis. *https://socprime.com/blog/latest-threats/cve-2026-0300-analysis/*

SECURITYWEEK (2026). Palo Alto Networks to patch zero-day exploited to hack firewalls. *https://www.securityweek.com/palo-alto-networks-to-patch-zero-day-exploited-to-hack-firewalls/*

HELP NET SECURITY (2026). Palo Alto firewalls vulnerability exploited (CVE-2026-0300). *https://www.helpnetsecurity.com/2026/05/06/palo-alto-firewalls-vulnerability-exploited-cve-2026-0300/*

HKCERT (2026). Palo Alto PAN-OS remote code execution vulnerability. *https://www.hkcert.org/security-bulletin/palo-alto-pan-os-remote-code-execution-vulnerability_20260506*

WATCHTOWR (2026). Rapid reaction: PAN-OS buffer overflow CVE-2026-0300. *https://watchtowr.com/resources/rapid-reaction-palo-alto-pan-os-buffer-overflow-cve-2026-0300/*