GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1826

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

CVE-2026-0300 – PALO ALTO NETWORKS (EJECUCIÓN REMOTA DE CÓDIGO CRÍTICA - RCE)

Palo Alto Networks ha revelado una vulnerabilidad crítica de desbordamiento de búfer en el software PAN-OS que afecta a los servicios de autenticación de usuario. El fallo está siendo explotado activamente en entornos donde los portales de acceso están expuestos a redes no confiables.

Resumen técnico:

Identificador principal: CVE-2026-0300.

- Severidad: 9.3 (Crítica) según la escala CVSS v4.0.
- Causa raíz: Una escritura fuera de límites (CWE-787) en el servicio User-ID™ Authentication Portal (también conocido como Captive Portal).
- Mecanismo de falla: Un atacante remoto no autenticado puede enviar paquetes de red especialmente diseñados para provocar un desbordamiento de búfer. Esto permite la ejecución de código arbitrario con privilegios de administrador (root) sin requerir interacción del usuario.
- Estado de explotación: Explotación activa detectada en la naturaleza (Día Cero) confirmada el 5 de mayo de 2026.
- Versiones afectadas: Firewalls de las series PA y VM con versiones de PAN-OS 12.1, 11.2, 11.1 y 10.2. Los dispositivos Prisma Access y Panorama no se encuentran afectados.

Impacto potencial:

- Control total del dispositivo (Root): La ejecución exitosa de código otorga privilegios máximos sobre el firewall, permitiendo modificar cualquier configuración de seguridad.
- Movimiento lateral en la red: Al comprometer el perímetro, el atacante puede utilizar el firewall como puente para acceder a segmentos internos de la organización.
- Interceptación y manipulación de tráfico: Capacidad para monitorear, desviar o alterar el flujo de datos que transita a través del dispositivo afectado.
- Exfiltración de credenciales: Acceso a secretos, certificados y datos de autenticación de usuarios gestionados por el portal de identificación.

Recomendaciones de mitigación:

1. Restricción de acceso perimetral: Limitar el acceso al Portal de Autenticación de User-ID únicamente a direcciones IP internas de confianza y evitar su exposición directa a Internet.
2. Deshabilitar el portal si no es requerido: Desactivar completamente el servicio de Captive Portal en la configuración de PAN-OS si no es esencial para la operación del negocio.
3. Aplicación de firmas de seguridad: Para organizaciones con licencia de Prevención de Amenazas, habilitar de inmediato la firma Threat ID 510019 para bloquear intentos de explotación.
4. Planificación de parches urgentes: Preparar la actualización de los sistemas a las versiones remediadas (disponibles entre el 13 y el 28 de mayo de 2026 según la rama de software).

Prioridad: Crítica.

Ampliar información:

- https://security.paloaltonetworks.com/CVE-2026-0300
- https://blog.segu-info.com.ar/2026/05/vulnerabilidad-critica-en-palo-alto.html
- https://cybersecuritynews.com/palo-alto-firewalls-vulnerability-exploited/
- https://socprime.com/es/blog/latest-threats/cve-2026-0300-analisis/
- https://www.wiz.io/blog/critical-vulnerability-in-pan-os-exploited-in-the-wild-cve-2026-0300
- https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-048/
- https://www.helpnetsecurity.com/2026/05/06/palo-alto-firewalls-vulnerability-exploited-cve-2026-0300/

CVE-2026-23918 – APACHE HTTP SERVER (CORRUPCIÓN DE MEMORIA Y RCE POTENCIAL EN HTTP/2)

Se ha identificado una vulnerabilidad de liberación doble (double-free) en la implementación del protocolo HTTP/2 dentro del servidor Apache. El fallo permite a un atacante remoto provocar la caída del proceso de trabajo (worker) o, en condiciones específicas de configuración de memoria, ejecutar código arbitrario en el servidor.

Resumen técnico:

- Identificador principal: CVE-2026-23918.
- Severidad: 8.8 (Alta) según la escala CVSS v4.0.
- Causa raíz: Un error de liberación doble de memoria en la ruta de limpieza de flujos (streams) dentro del componente mod_http2.
- Mecanismo de falla: Se activa durante una secuencia de "reinicio temprano", cuando un cliente envía una trama HEADERS seguida inmediatamente por una trama RST_STREAM. Esto provoca que el puntero del flujo se procese dos veces en el ciclo de limpieza, corrompiendo los metadatos del heap.
- Estado de explotación: No se ha reportado explotación masiva en la naturaleza al momento de esta publicación, pero existe una prueba de concepto (PoC) funcional para ejecución de código.
- Versiones afectadas: Específicamente la versión 2.4.66 de Apache HTTP Server.

Impacto potencial:

- Denegación de Servicio (DoS): Un atacante puede colapsar los procesos de trabajo de forma trivial mediante una secuencia diseñada de tramas HTTP/2, afectando la disponibilidad del servicio.
- Ejecución Remota de Código (RCE): En sistemas donde la biblioteca APR utiliza el asignador mmap (común en distribuciones basadas en Debian y contenedores oficiales), es posible redirigir el flujo de ejecución.
- Evasión de ASLR: La utilización de la memoria del "scoreboard" de Apache como contenedor estable facilita la ejecución de comandos de forma persistente a pesar de las protecciones de aleatorización.
- Interrupción de conexiones activas: La caída de los procesos worker resulta en el cierre inesperado de todas las solicitudes legítimas que estén siendo procesadas en ese momento.

Recomendaciones de mitigación:

1. Actualización inmediata del servidor: Migrar a la versión 2.4.67 de Apache HTTP Server, la cual corrige la gestión de limpieza de flujos en el multiplexor.
2. Deshabilitar el soporte HTTP/2: Como medida de mitigación temporal si la actualización no es posible, deshabilitar o comentar el módulo mod_http2 en la configuración global del servidor.
3. Auditoría de versiones instaladas: Identificar de forma prioritaria cualquier instancia que ejecute específicamente la versión 2.4.66, dado que es la rama confirmada como vulnerable por cambios recientes en el asignador de memoria.
4. Monitoreo de fallos de segmentación: Supervisar los registros de errores de Apache en busca de señales de inestabilidad o fallos críticos (Segmentation Fault) que coincidan con patrones inusuales de reinicio de flujos HTTP/2.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/05/critical-apache-http2-flaw-cve-2026.html
- https://socradar.io/blog/cve-2026-23918-apache-http-server-http-2/
- https://hadrian.io/blog/cve-2026-23918-apache-http-server-double-free-rce-in-http-2-implementation
- https://socradar.io/blog/cve-2026-23918-apache-http-server-http-2/
- https://securityaffairs.com/191759/security/apache-fixes-critical-http-2-double-free-flaw-cve-2026-23918-enabling-rce.html
- https://www.securityweek.com/critical-high-severity-vulnerabilities-patched-in-apache-mina-http-server/

CVE-2026-31431 – KERNEL DE LINUX (ESCALAMIENTO DE PRIVILEGIOS LOCALES - "COPY FAIL")

Se ha divulgado una vulnerabilidad crítica de escalamiento de privilegios (LPE) en el kernel de Linux que permite a un usuario local sin privilegios obtener acceso total como root. A diferencia de otros fallos históricos, este no depende de condiciones de carrera y es altamente determinista y confiable.

Resumen técnico:

- Identificador principal: CVE-2026-31431.
- Severidad: 7.8 (Alta) / 9.3 (Crítica en entornos compartidos) según CVSS.
- Causa raíz: Una falla lógica en el módulo algif_aead del subsistema criptográfico del kernel (interfaz AF_ALG).
- Mecanismo de falla: El vector aprovecha una optimización defectuosa de 2017 para realizar una sobreescritura controlada de 4 bytes en la caché de páginas del sistema mediante la llamada splice(). Esto permite modificar la copia en memoria de binarios privilegiados (como /usr/bin/su) mientras el archivo en disco permanece intacto.
- Estado de explotación: Existe un exploit público (PoC) en Python de solo 732 bytes que funciona de manera universal en múltiples distribuciones.
- Versiones afectadas: Prácticamente todas las distribuciones con kernels compilados desde 2017 (versiones 4.14 hasta 6.19.12), incluyendo Ubuntu, RHEL, Debian, Amazon Linux y SUSE.

Impacto potencial:

- Escalamiento total a Root: Permite que cualquier proceso con bajos privilegios ejecute código con los máximos permisos del sistema (UID 0).
- Evasión de contenedores (Container Escape): Debido a que el kernel y la caché de páginas se comparten entre el host y los contenedores, un atacante puede saltar del contenedor al nodo físico o afectar cargas de trabajo vecinas.
- Ataque sigiloso persistente: Al corromper la memoria y no el disco, el ataque evade las herramientas tradicionales de monitoreo de integridad de archivos (FIM) y auditorías de sumas de verificación.
- Compromiso de infraestructura crítica: Representa un riesgo extremo para granjas de compilación de código, nodos de Kubernetes y entornos de ejecución de CI/CD multi-inquilino.

Recomendaciones de mitigación:

1. Actualización urgente del Kernel: Aplicar de inmediato los parches de seguridad distribuidos por su proveedor de sistema operativo y realizar el reinicio correspondiente para cargar la versión remediada.
2. Deshabilitar el módulo vulnerable: Bloquear la carga del módulo algif_aead creando el archivo /etc/modprobe.d/disable-algif.conf con el contenido install algif_aead /bin/false y ejecutando rmmod algif_aead.
3. Mitigación específica para RHEL/Red Hat: En sistemas donde el módulo está integrado, utilizar grubby para añadir initcall_blacklist=algif_aead_init a los argumentos del kernel y reiniciar el sistema.
4. Implementación de políticas de Seccomp: En entornos de contenedores (Docker/Kubernetes), configurar perfiles de seccomp que bloqueen la creación de sockets de la familia AF_ALG para neutralizar el vector de entrada del exploit.

Prioridad: Crítica.

Ampliar información:

- https://almalinux.org/blog/2026-05-01-cve-2026-31431-copy-fail/
- https://www.microsoft.com/en-us/security/blog/2026/05/01/cve-2026-31431-copy-fail-vulnerability-enables-linux-root-privilege-escalation/
- https://unit42.paloaltonetworks.com/cve-2026-31431-copy-fail/
- https://support.plesk.com/hc/en-us/articles/40124635047319-Vulnerability-CVE-2026-31431
- https://cert.europa.eu/publications/security-advisories/2026-005/
- https://blog.segu-info.com.ar/2026/04/copy-fail-vulnerabilidad-critica.html

MALWARE

xlabs_v1 – BOTNET DERIVADA DE MIRAI (DDoS-FOR-HIRE SOBRE DISPOSITIVOS ANDROID)

Se ha identificado una nueva variante de la familia Mirai, denominada xlabs_v1, la cual está diseñada para reclutar dispositivos Android e IoT con el fin de realizar ataques de denegación de servicio distribuido (DDoS). Esta operación se comercializa bajo un modelo de "DDoS-for-hire", especializándose en la interrupción de servidores.

Resumen técnico:

- Tipo de amenaza: Botnet / Malware de red.
- Vector de infección: Explotación de dispositivos con el puerto del Android Debug Bridge (ADB) (TCP/5555) expuesto a Internet sin autenticación.
- Objetivos principales: Servidores (protocolos RakNet) y servidores OpenVPN.
- Técnicas de evasión: El malware renombra su proceso a /bin/bash para ocultarse en la lista de procesos del sistema y utiliza cifrado ChaCha20 para proteger sus comunicaciones con el servidor de comando y control (C2).
- Funcionalidad distintiva: Realiza un perfilado de ancho de banda mediante la apertura de miles de conexiones simultáneas a servidores de Speedtest, permitiendo al operador categorizar los dispositivos infectados según su capacidad de ataque.
- Infraestructura: La operación centraliza su distribución y control en centros de datos ubicados en los Países Bajos.

Impacto potencial:

- Degradación del ancho de banda: El uso intensivo del canal de subida para pruebas de velocidad y ataques DDoS puede saturar la conexión a Internet del dispositivo afectado, impactando la calidad del servicio para el usuario legítimo.
- Reclutamiento en redes criminales: Los dispositivos comprometidos pasan a formar parte de una infraestructura alquilable para actores de amenazas, facilitando ataques masivos contra terceros.
- Eliminación de software legítimo y competencia: El malware posee un subsistema que identifica y finaliza otros procesos maliciosos competidores para garantizar el uso exclusivo de los recursos del hardware.
- Exposición de red interna: Debido a que muchos de estos dispositivos residen en redes domésticas o corporativas, un acceso mediante ADB podría ser utilizado como punto de partida para una exploración más profunda de la red local.

Recomendaciones de mitigación:

1. Deshabilitar el servicio ADB: Asegúrese de que la función Android Debug Bridge esté desactivada en todos los dispositivos Android TV, routers y hardware IoT, a menos que sea estrictamente necesario para labores de desarrollo controladas.
2. Filtrado de puertos perimetrales: Configurar los cortafuegos de la organización para bloquear cualquier tráfico entrante y saliente a través del puerto TCP/5555 hacia redes no confiables o Internet.
3. Monitoreo de procesos inusuales: Supervisar la aparición de procesos denominados /bin/bash o similares que se ejecuten sin una terminal controladora o que presenten un consumo de CPU y red anómalamente alto.
4. Bloqueo de indicadores de compromiso (IoC): Implementar reglas de bloqueo en las soluciones de seguridad para impedir la comunicación con el dominio de C2 xlabslover[.]lol y las direcciones IP asociadas a la infraestructura detectada.

Prioridad: Urgente.

Ampliar información:

- https://www.cryptika.com/new-xlabs_v1-botnet-targets-minecraft-servers-through-adb-exposed-android-devices/
- https://gbhackers.com/adb-exposed-android-devices/#google_vignette
- https://teamwin.in/new-xlabs_v1-botnet-targets-minecraft-servers-through-adb-exposed-android-devices/
- https://cybersecuritynews.com/new-xlabs_v1-botnet-targets-minecraft-servers/
- https://thehackernews.com/2026/05/mirai-based-xlabsv1-botnet-exploits-adb.html

Recomendaciones generales sobre malware:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

ATAQUE A LA CADENA DE SUMINISTRO: INSTALADORES DE DAEMON TOOLS COMPROMETIDOS

Se ha identificado un sofisticado ataque a la cadena de suministro que ha afectado los instaladores oficiales de la herramienta de emulación de discos DAEMON Tools (específicamente la versión Lite). Los atacantes lograron inyectar código malicioso en los archivos distribuidos desde el sitio web legítimo del fabricante, los cuales contaban con una firma digital válida de AVB Disc Soft.

Resumen técnico:

- Periodo de exposición: Del 8 de abril de 2026 hasta el 5 de mayo de 2026 (fecha de divulgación pública).
- Versiones afectadas: Versiones de Windows desde la 12.5.0.2421 hasta la 12.5.0.2434.
- Componentes troyanizados: Los binarios DTHelper.exe, DiscSoftBusServiceLite.exe y DTShellHlp.exe.
- Cadena de infección: El malware establece persistencia al ejecutarse en cada inicio del sistema, contactando a un servidor de comando y control (C2) diseñado para simular el dominio oficial del desarrollador.
- Cargas útiles detectadas: Incluyen un recolector de información (.NET), una puerta trasera minimalista y un implante avanzado denominado QUIC RAT, capaz de inyectar código en procesos legítimos como notepad.exe.
- Estado de remediación: El fabricante ha publicado la versión 12.6.0.2445, la cual se encuentra libre de comportamiento malicioso.

Impacto potencial:

- Recolección masiva de telemetría: El implante inicial extrae datos sensibles como direcciones MAC, nombres de host, dominios DNS, listas de software instalado y procesos activos para perfilar a las víctimas.
- Despliegue selectivo de Backdoors: Los atacantes utilizan la información recopilada para entregar cargas útiles avanzadas de forma dirigida a organizaciones de sectores gubernamentales, científicos e industriales.
- Evasión de controles tradicionales: Al estar firmados con certificados digitales legítimos, los instaladores maliciosos evaden las protecciones basadas en la confianza del editor y el filtrado perimetral estándar.
- Persistencia sigilosa en el sistema: El uso de protocolos de comunicación robustos (QUIC, HTTP/3, WSS) y la inyección en procesos de sistema dificultan significativamente la detección mediante análisis de comportamiento básico.

Recomendaciones para mitigar el riesgo:

1. Aislamiento y análisis de endpoints: Identificar y desconectar de la red cualquier sistema que haya instalado o actualizado DAEMON Tools entre el 8 de abril y el 5 de mayo de 2026.
2. Actualización obligatoria a versión segura: Forzar la transición a la versión 12.6.0.2445 o proceder con la desinstalación completa de las versiones afectadas.
3. Bloqueo de infraestructura C2: Implementar bloqueos perimetrales para el dominio env-check.daemontools[.]cc y la dirección IP 38.180.107[.]76.
4. Auditoría de procesos de sistema: Realizar una búsqueda activa (Threat Hunting) de anomalías en los procesos notepad.exe y conhost.exe, verificando posibles inyecciones de memoria o conexiones de red inusuales.

Prioridad: Importante.

Ampliar Información:

- https://www.rescana.com/post/critical-daemon-tools-supply-chain-attack-malware-compromised-windows-installers-threaten-organizations-and-home-users-v/
- https://www.kaspersky.es/blog/daemon-tools-supply-chain-attack/32085/?srsltid=AfmBOoqG7J183xwbTMNgRGvSt-RCnmSURxa2WlAREDpjX7d9QNS8TXaY
- https://www.safestate.com/post/daemon-tools-installer-backdoored-in-active-supply-chain-attack
- https://securelist.com/tr/daemon-tools-backdoor/119654/
- https://thehackernews.com/2026/05/daemon-tools-supply-chain-attack.html
- https://www.kaspersky.com/blog/daemon-tools-supply-chain-attack/55691/