RADAR CTI

BOLETÍN SEMANAL
DE CIBERSEGURIDAD

INTELIGENCIA PARA ANTICIPARNOS HOY, PROTEGER TU MAÑANA.

Análisis, contexto y acciones concretas sobre las amenazas más relevantes de la semana.

AMENAZAS EN LA MIRA

VULNERABILIDADES CRÍTICAS

INCIDENTES RELEVANTES

ACCIONES INMEDIATAS

Grupo Smartekh

THREAT INTELLIGENCE | VULNERABILITY MANAGEMENT | NEXT GEN SOC

RADARCTI

Boletín semanal de ciberseguridad | 26 mayo - 1 junio 2026

VULNERABILIDADES CRÍTICAS

CRITICAL | WINDOWS | NETLOGON

Windows Netlogon: RCE crítico en controladores de dominio

Lo delicado de CVE-2026-41089 no es solo su CVSS 9.8, sino dónde pega: servidores que funcionan como controladores de dominio. Microsoft la clasifica como crítica y el escenario relevante es ejecución remota por red contra Netlogon, sin que el atacante tenga que partir de una cuenta válida.

Impacto: En Active Directory, un DC vulnerable cambia la prioridad del parcheo: comprometer Netlogon puede derivar en ejecución de código sobre el sistema que sostiene identidad, autenticación y políticas del dominio.

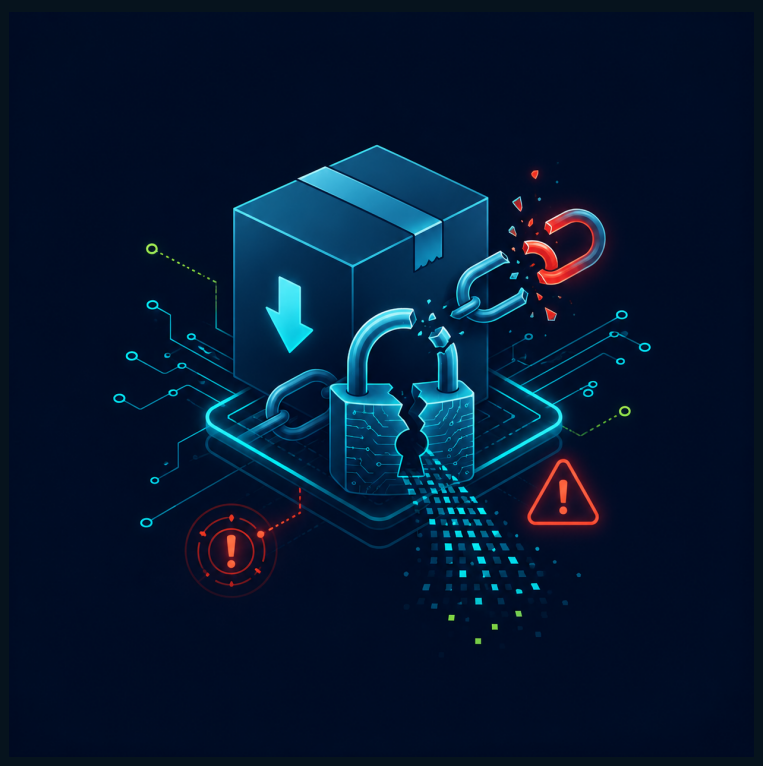
Qué hacer ahora

- Aplicar la actualización de seguridad Microsoft mayo 2026 o posterior en Windows Server/DC afectados por CVE-2026-41089.
- Restringir SMB, RPC y Netlogon a segmentos confiables y no exponerlos a redes no controladas.
- Revisar eventos de DC, reinicios anómalos, fallos Netlogon y tráfico RPC/SMB fuera de patrón.

URL oficial: api.msrc.microsoft.com / msrc.microsoft.com

Fuentes: Microsoft MSRC, referencia del insumo compartido

ACONTECIMIENTOS CRÍTICOS



CISA KEV | SUPPLY CHAIN

CISA KEV: DAEMON Tools, TanStack y Nx Console

CISA sumó a KEV tres casos que apuntan al mismo problema: piezas de software confiables usadas como canal de ataque. DAEMON Tools Lite tuvo instaladores comprometidos, TanStack enfrentó paquetes npm con robo de credenciales y Nx Console distribuyó por poco tiempo una versión maliciosa en marketplaces de VS Code.

Impacto: El patrón es común: software o paquetes confiables se convierten en vehículo para robo de secretos, tokens, llaves SSH y credenciales cloud. El foco no es solo el endpoint, sino los entornos de desarrollo y pipelines que consumieron esas piezas.

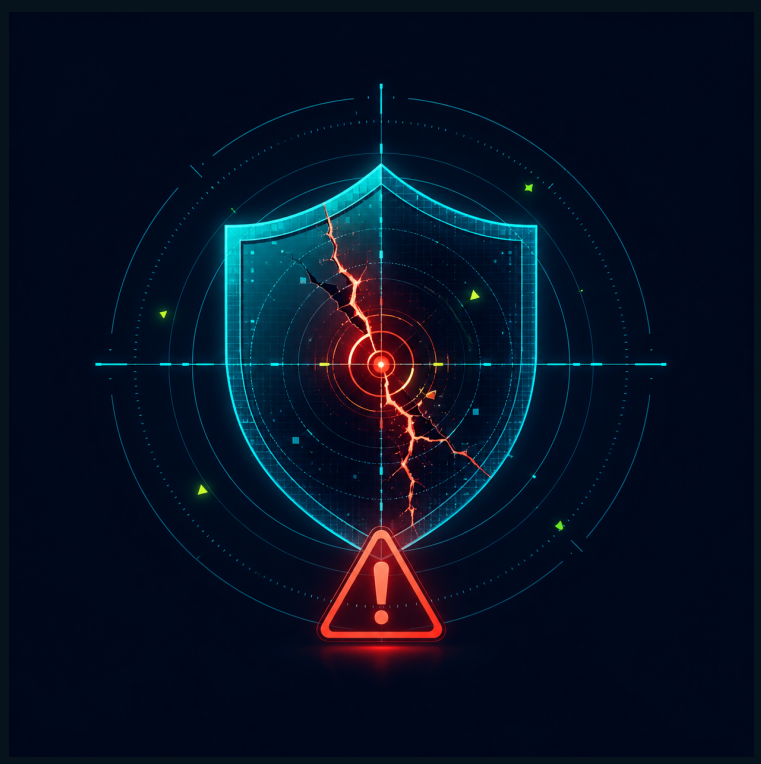
Qué hacer ahora

- DAEMON Tools Lite: retirar instaladores del 8-abr al 5-may y reinstalar solo el build oficial vigente posterior al 5-may.
- TanStack: actualizar paquetes @tanstack/* a releases limpios posteriores al 11-may; rotar tokens GitHub, npm y cloud.
- Nx Console: eliminar la versión maliciosa y actualizar desde VS Marketplace/OpenVSX oficial ya saneado.

URL oficial: cisa.gov / nvd.nist.gov / tanstack.com

Fuentes: CISA KEV, NVD, TanStack, referencia del insumo compartido

VULNERABILIDADES ALTAS



VPN | GLOBALPROTECT | ATTACKED

Palo Alto PAN-OS: bypass de autenticación en GlobalProtect

Palo Alto actualizó CVE-2026-0257 el 29 de mayo y la marcó como ATTACKED. El caso aplica a portales o gateways GlobalProtect con configuraciones específicas de cookies de Authentication Override; bajo esas condiciones, un atacante podría establecer una conexión VPN sin pasar por el flujo esperado de autenticación.

Impacto: Una VPN expuesta suele ser puerta de entrada al entorno interno. Aunque requiere una configuración específica, el estado ATTACKED obliga a revisar versiones, certificados y registros de acceso sin esperar señales internas claras.

Qué hacer ahora

- PAN-OS 12.1: subir a 12.1.7+ o 12.1.4-h6+; PAN-OS 11.2: 11.2.12+ o 11.2.10-h7/11.2.7-h14/11.2.4-h17+.
- PAN-OS 11.1: subir a 11.1.15+ o hotfix 11.1.13-h5, 11.1.10-h25, 11.1.7-h6, 11.1.6-h32 o 11.1.4-h33+.
- PAN-OS 10.2: subir a 10.2.18-h6+ o hotfix 10.2.16-h7, 10.2.13-h21, 10.2.10-h36 o 10.2.7-h34+.

URL oficial: security.paloaltonetworks.com/CVE-2026-0257

Fuentes: Palo Alto Networks Security Advisory

VULNERABILIDADES CRÍTICAS

CMS | DRUPAL | SQLI

Drupal: SQL injection explotada en sitios PostgreSQL

Drupal corrigió CVE-2026-9082 después de reportes de explotación activa. La falla toca la capa de base de datos y se vuelve crítica en sitios que usan PostgreSQL, porque una solicitud especialmente armada puede abrir SQL injection sin autenticación. En ciertos entornos, esto puede terminar en exposición de datos o algo peor.

Impacto: Drupal suele sostener portales gubernamentales, universidades, medios y servicios financieros. La combinación de explotación real, CMS público y base de datos expuesta cambia la prioridad para sitios institucionales y de alto tráfico.

Qué hacer ahora

- Actualizar Drupal según rama: 11.3.x, 11.2.x, 10.6.x o 10.5.x corregida; si se usa 11.1 o 10.4, subir a 11.1.9 o 10.4.9.
- Si aún existe Drupal 9.5.11 u 8.9.20 EOL, aplicar hotfix temporal y planear migración; no hay parche completo para 8/9.
- Revisar logs de web y base de datos por consultas anómalas, errores SQL y cadenas de explotación repetidas.

URL oficial: drupal.org / cisa.gov / bleepingcomputer.com

Fuentes: Drupal, CISA, BleepingComputer, Imperva

VULNERABILIDADES CRÍTICAS

WORDPRESS | ADMIN TAKEOVER

WP Maps Pro: creación de administradores sin autenticación

En WP Maps Pro, el problema es directo: hasta la versión 6.1.0, una función AJAX expuesta podía abusarse para crear usuarios administradores sin iniciar sesión. Wordfence lo calificó con CVSS 9.8 porque el atacante no necesita credenciales y, una vez dentro, controla el sitio como administrador.

Impacto: El riesgo no es solo acceso a WordPress: un administrador malicioso puede instalar plugins, modificar temas, colocar webshells, redirigir tráfico o usar el sitio para phishing y campañas SEO maliciosas.

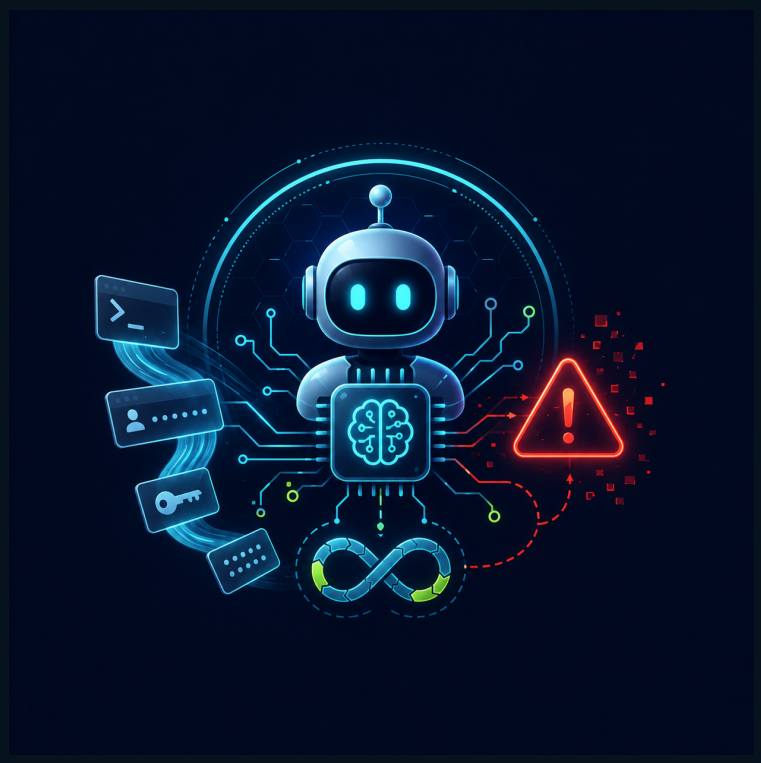
Qué hacer ahora

- Actualizar WP Maps Pro a 6.1.1 o superior en sitios WordPress.
- Auditar usuarios administradores creados recientemente y cuentas con correos o nombres sospechosos.
- Revisar plugins, temas, archivos modificados, webshells, redirecciones y cambios SEO.

URL oficial: wordfence.com / codecanyon.net

Fuentes: Wordfence, WP Maps Pro

VULNERABILIDADES ALTAS



AI DEV | STARLETTE | BADHOST

Starlette BadHost: riesgo en APIs y stacks de IA

BadHost, identificado como CVE-2026-48710, nace de una validación débil del Host header en Starlette. El detalle parece pequeño, pero en frameworks y servicios que reconstruyen URLs para tomar decisiones de seguridad, un header malformado puede alterar rutas, queries o fragmentos y romper supuestos de control de acceso.

Impacto: El efecto downstream puede ser serio en FastAPI, LiteLLM, vLLM, proxies OpenAI-compatible, MCP servers y dashboards de IA. Si el control de acceso vive en middleware, endpoints internos pueden quedar alcanzables.

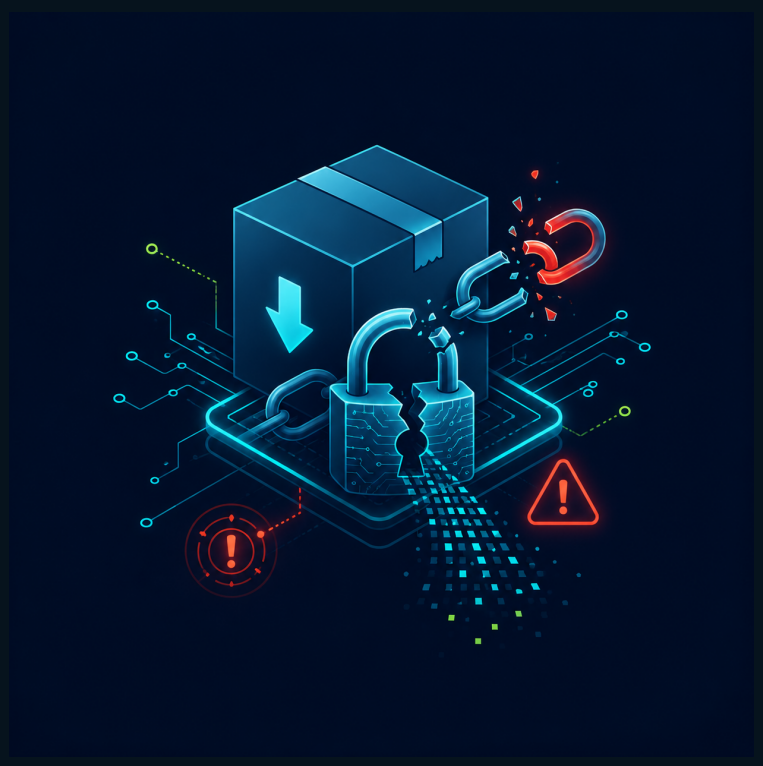
Qué hacer ahora

- Actualizar Starlette a 1.0.1 y reconstruir imágenes, virtualenvs y artefactos que la empaqueten.
- Revisar middleware que use request.url o request.url.path para decisiones de seguridad.
- Colocar reverse proxy que rechace Host headers malformados y validar APIs de IA expuestas.

URL oficial: ostif.org / github.com/Kludex/starlette

Fuentes: OSTIF, X41-Dsec, Starlette advisory

ACONTECIMIENTOS CRÍTICOS



SUPPLY CHAIN | DESARROLLADORES

Glassworm: botnet contra desarrolladores fue desmantelado

Glassworm volvió a mostrar que los desarrolladores ya son objetivo de primer nivel. La operación coordinada de CrowdStrike, Google y Shadowserver cortó parte de su infraestructura de mando, pero la campaña ya había abusado de extensiones de VSCode, paquetes npm/Python y repositorios GitHub para buscar tokens, llaves SSH y credenciales de publicación.

Impacto: La afectación no se limita al equipo infectado: los secretos de desarrollo pueden abrir acceso a CI/CD, nube, registros de paquetes y repositorios privados. Aunque la operación redujo el control del botnet, los hosts tocados deben tratarse como comprometidos.

Qué hacer ahora

- Buscar extensiones de VSCode y paquetes instalados fuera de fuentes confiables.
- Rotar tokens GitHub, npm, PyPI, SSH y secretos expuestos a entornos de desarrollo.
- Revisar repositorios y pipelines por commits, workflows o publicaciones no autorizadas.

URL oficial: crowdstrike.com / shadowserver.org

Fuentes: TechRadar, CrowdStrike, Google, Shadowserver

VULNERABILIDADES ALTAS

HIGH | RCE | 7-ZIP

7-Zip: abrir un archivo puede ejecutar código

La falla en 7-Zip preocupa porque el usuario no tiene que hacer mucho: basta con que la herramienta procese un archivo manipulado. El caso reportado, con CVSS 8.8, aprovecha estructuras tipo NTFS dentro de formatos comunes como ZIP, RAR o 7z, por lo que afecta tanto uso manual como flujos automatizados.

Impacto: La exposición es amplia por el uso de 7-Zip en estaciones, servidores, scripts, herramientas de análisis, antivirus, respaldos y flujos CI/CD. El riesgo sube si procesos automatizados revisan archivos con privilegios altos.

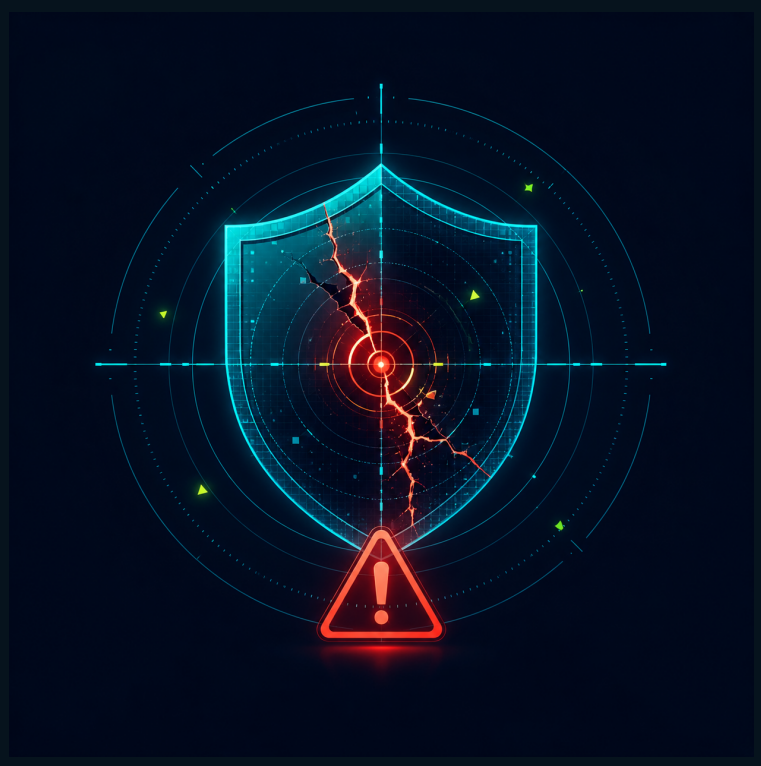
Qué hacer ahora

- Actualizar 7-Zip a 26.01 o superior y revisar forks/p7zip empaquetados por Linux.
- Evitar que procesos privilegiados abran archivos no confiables sin sandbox.
- Inventariar herramientas que llamen 7z de forma indirecta en pipelines y servidores.

URL oficial: 7-zip.org / tomshardware.com

Fuentes: Tom’s Hardware, 7-Zip

VULNERABILIDADES ALTAS



0-DAY | KEV | ENDPOINT

Trend Micro Apex One: explotación activa entra a KEV

CVE-2026-34926 afecta a Apex One on-premise y ya entró al catálogo KEV de CISA. No es una falla de entrada inicial simple, porque requiere acceso administrativo previo al servidor, pero sí es peligrosa: desde la consola central puede inyectarse código que después llega a los agentes administrados.

Impacto: Aunque exige acceso administrativo previo al servidor, el impacto puede extenderse hacia endpoints bajo administración central. Un servidor Apex One comprometido puede convertirse en canal de despliegue confiable para código malicioso.

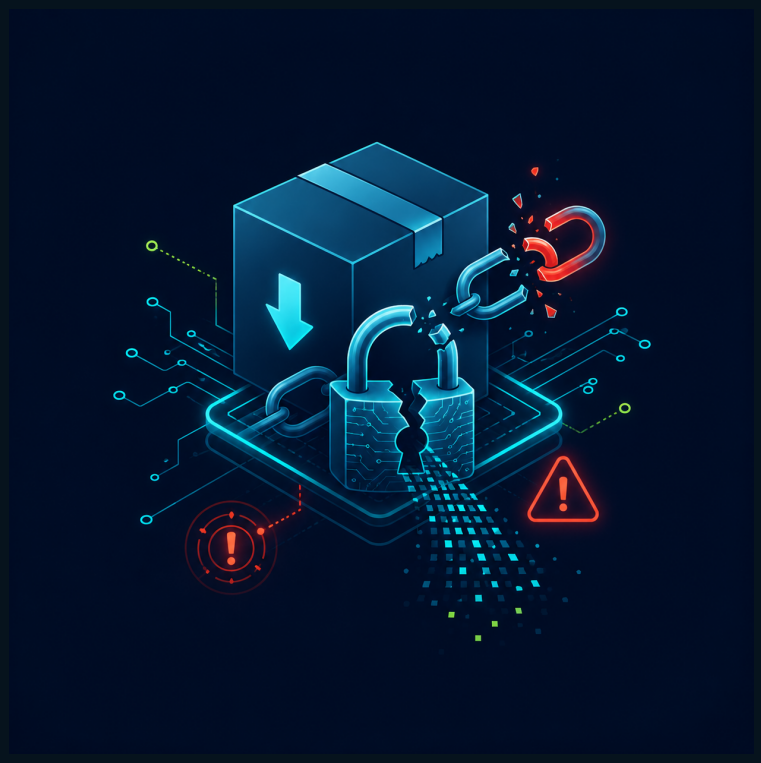
Qué hacer ahora

- Aplicar el patch oficial de Trend Micro para Apex One on-premise que corrige CVE-2026-34926 o discontinuar uso antes del 4-jun.
- Validar en la consola que el servidor Apex One quedó en el build corregido del advisory de CVE-2026-34926.
- Revisar políticas, paquetes desplegados y actividad de cuentas administrativas después de actualizar.

URL oficial: trendmicro.com / cisa.gov

Fuentes: Trend Micro, CISA, TechRadar

ACONTECIMIENTOS CRÍTICOS



IDENTIDAD | M365 | PHAAS

Kali365: phishing roba tokens de Microsoft 365

Kali365 destaca porque no intenta robar la contraseña de forma clásica. El kit guía a la víctima para autorizar un código en una página legítima de Microsoft; al completar ese flujo de device code, el atacante obtiene tokens OAuth con acceso a servicios como Outlook, Teams, OneDrive y otros componentes de Microsoft 365.

Impacto: MFA no bloquea este escenario si el usuario completa el flujo legítimo. El acceso persiste hasta revocar tokens, por lo que puede derivar en robo de correo, exfiltración de documentos y movimiento lateral dentro del tenant.

Qué hacer ahora

- Bloquear o restringir device code flow con Conditional Access cuando no sea necesario.
- Auditar usos recientes de device code, apps autorizadas y refresh tokens sospechosos.
- Revocar sesiones y tokens ante indicios de acceso anómalo a Outlook, Teams o OneDrive.

URL oficial: ic3.gov / fbi.gov / microsoft.com

Fuentes: FBI, TechRadar, ITPro

RADAR CTI

BOLETÍN SEMANAL DE CIBERSEGURIDAD

Las amenazas cambian cada semana.
Tu capacidad de responder define el impacto.

¿Tu organización podría detectar alguno de estos escenarios antes de que afecte la operación?

En Grupo Smartekh ayudamos a equipos de TI y ciberseguridad a:

- Identificar riesgos críticos
- Priorizar vulnerabilidades
- Fortalecer controles
- Responder incidentes con rapidez real

Grupo Smartekh

NEXT GEN SOC
Monitoreo 24/7

THREAT INTELLIGENCE
Inteligencia accionable

VULNERABILITY MANAGEMENT
Visibilidad y remediación

ESCRÍBENOS
informacion@smartekh.com

#SMARTEKH

Canal WhatsApp | Eventos | Blogs | Infografías Awareness