RADAR CTI

BOLETÍN SEMANAL
DE CIBERSEGURIDAD

4 - 12 Mayo 2026

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

RADAR CTI

Boletínsemanaldeciberseguridad | 4 - 12 mayo2026

ACONTECIMIENTOS CRÍTICOS

EXTORSIÓN | EDUCACIÓN

Canvas LMS: ShinyHunters escala presión con defacement masivo

Instructure ya venía investigando el robo de datos de Canvas. El 7 de mayo, ShinyHunters volvió a presionar: modificó portales de inicio de sesión de cientos de instituciones y dejó mensajes de extorsión con fecha límite del 12 de mayo. Lo delicado no es solo el robo: es que el atacante logró hacer visible su mensaje dentro del flujo normal de acceso de escuelas y universidades.

Impacto: Riesgo alto de phishing personalizado contra alumnos y personal, abuso de mensajes privados y presión reputacional a instituciones educativas si se publica o reutiliza la información.

Qué hacer ahora

- Rotar claves/API tokens de Canvas y de integraciones conectadas
- Revisar cambios no autorizados en portales y cuentas Free-For-Teacher
- Preparar comunicaciones anti-phishing para estudiantes y docentes

URL oficial: www.instructure.com/resources/blog/security-incident-update

Fuentes: BleepingComputer, TechCrunch, Bitdefender, Instructure

RADAR CTI

Boletínsemanaldeciberseguridad | 4 - 12 mayo2026

ACONTECIMIENTOS CRÍTICOS

SUPPLY CHAIN

DAEMON Tools: instalador oficial entregó malware firmado

Kaspersky detectó que el sitio oficial de DAEMON Tools distribuyó instaladores alterados desde el 8 de abril. El problema es grave porque los binarios venían firmados con certificados válidos del desarrollador, así que parecían legítimos. El primer payload recolectaba datos del equipo; en víctimas seleccionadas se desplegaba un backdoor para control remoto.

Impacto: Miles de equipos expuestos en más de 100 países. Kaspersky reportó víctimas en Brasil, Colombia y Chile, además de Europa y Asia.

Qué hacer ahora

- Reinstalar solo la versión limpia publicada por el proveedor
- Buscar versiones 12.5.0.2421 a 12.5.0.2434
- Revisar persistencia y conexiones a dominios de C2 reportados

URL oficial: www.daemon-tools.cc/products/dtLite

Fuentes: Kaspersky, BleepingComputer, The Hacker News, Disc Soft

ACONTECIMIENTOS CRÍTICOS

DEVSECOPS | DARK WEB

Checkmarx: el golpe a la cadena de suministro siguió dejando ruido

Checkmarx confirmó que el acceso no autorizado a repositorios de GitHub estuvo ligado al ataque previo contra Trivy y TeamPCP. Durante la semana, el tema siguió activo por artefactos de desarrollo afectados y menciones en sitios de filtración. El punto clave: herramientas pensadas para revisar seguridad terminaron siendo usadas como puerta de entrada a CI/CD.

Impacto: Exposición de secretos de desarrollo, claves cloud, tokens de repositorios y riesgo de código malicioso en pipelines.

Qué hacer ahora

- Eliminar artefactos Checkmarx/OpenVSX afectados si fueron usados en marzo
- Rotar secretos de GitHub, cloud, CI/CD, npm y Kubernetes
- Revisar Jenkins/GitHub Actions que ejecutaron herramientas Checkmarx o Trivy

URL oficial: checkmarx.com/blog/checkmarx-security-update

Fuentes: Checkmarx, Jenkins Plugin Index, TechRadar, Kaspersky

ACONTECIMIENTOS CRÍTICOS

SEGURIDAD | BRECHA

Trellix: acceso no autorizado a repositorio de código fuente

Trellix informó que un tercero no autorizado accedió a una parte de su repositorio de código. La compañía dijo que no encontró evidencia de manipulación del código, explotación o afectación a la cadena de distribución. Aun así, en una firma de seguridad este tipo de acceso merece atención: el código fuente puede ayudar a descubrir fallas o preparar ataques futuros.

Impacto: Riesgo de análisis ofensivo del código, búsqueda de vulnerabilidades y presión reputacional contra un proveedor usado por equipos de seguridad.

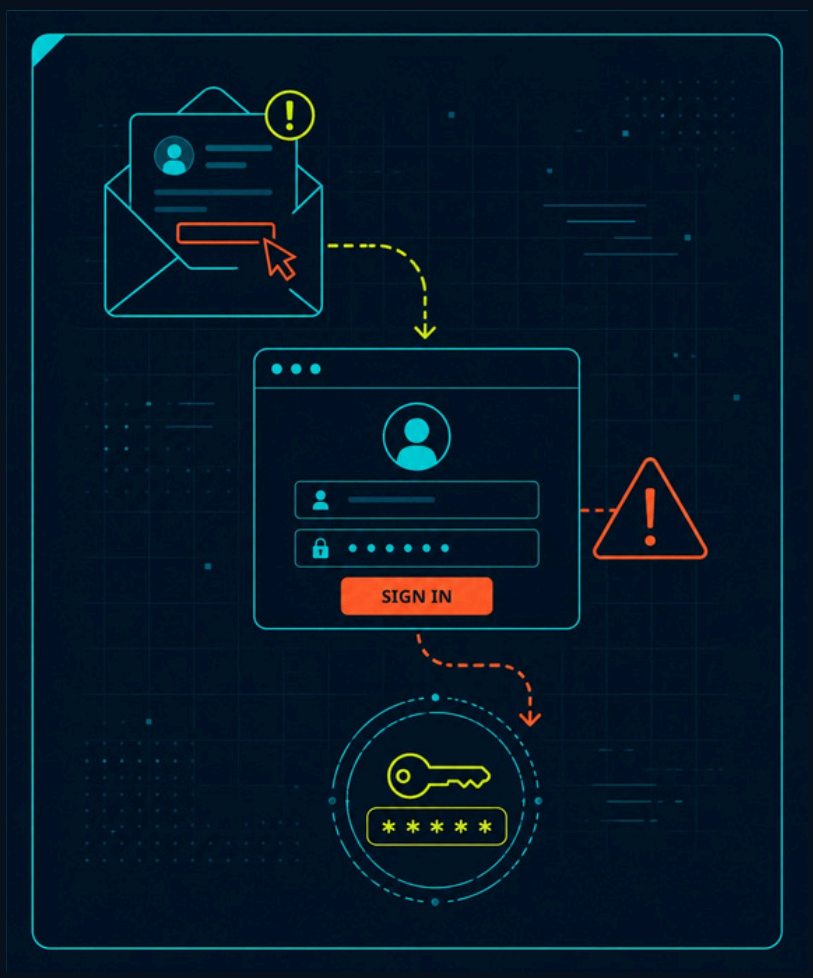
Qué hacer ahora

- Validar integridad de releases y hashes
- Monitorear avisos del fabricante
- Revisar exposición de credenciales en repositorios internos

URL oficial: www.trellix.com

Fuentes: Trellix, BleepingComputer, Infosecurity Magazine

ACONTECIMIENTOS CRÍTICOS



PHISHING GLOBAL

Operation HookedWing: phishing contra 500+ organizaciones

SOCRadar publicó una campaña que llevaba años activa sin estar documentada públicamente. El grupo usó infraestructura rotativa, dominios en GitHub Pages y servidores backend para robar credenciales. Se encontraron más de 2,000 credenciales de usuarios de más de 500 organizaciones.

Impacto: Afecta sectores sensibles: aviación, administración pública, energía, infraestructura crítica, logística y tecnología.

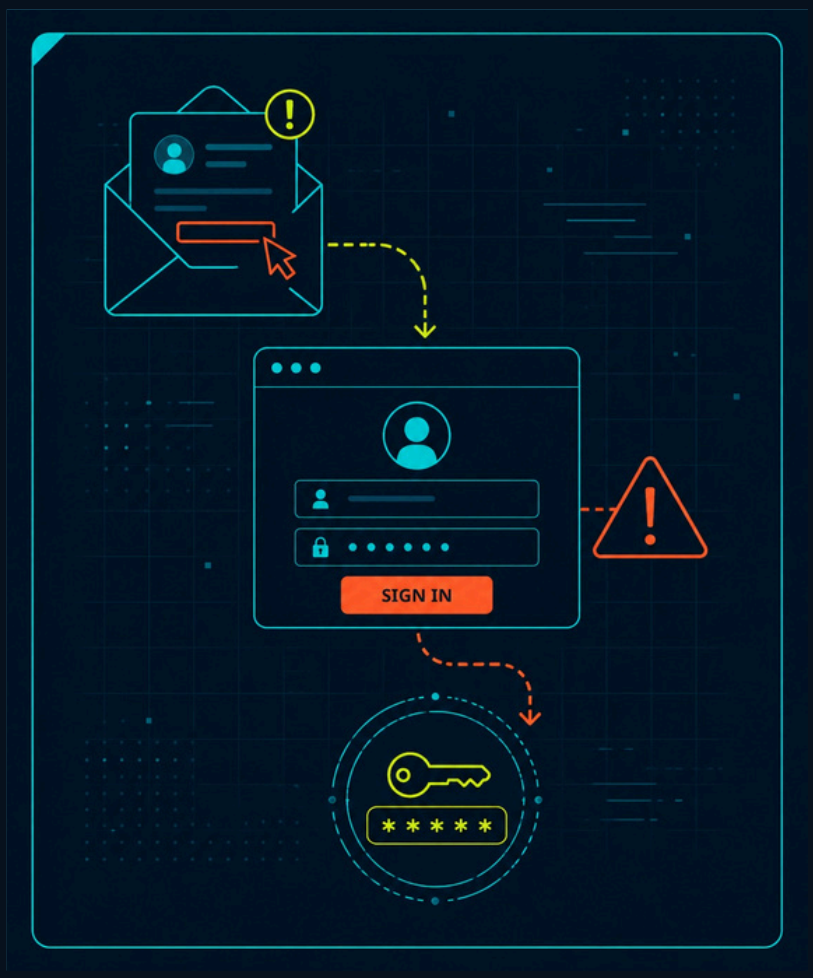
Qué hacer ahora

- Bloquear IOCs y dominios asociados
- Buscar credenciales corporativas filtradas
- Reforzar MFA resistente a phishing y monitoreo de inicios anómalos

URL oficial: socradar.io/blog/operation-hookedwing-4-year-phishing

Fuentes: SOCRadar Threat Research

ACONTECIMIENTOS CRÍTICOS



PHISHING | M365

Microsoft reporta phishing contra 35,000 usuarios en 26 países

Microsoft detalló una campaña que usó correos con apariencia corporativa, PDFs, redirecciones y CAPTCHA para terminar robando credenciales y tokens de sesión. La mayoría de ataques se concentró en EE. UU., pero el patrón es relevante para cualquier organización con Microsoft 365.

Impacto: El robo de tokens puede saltarse MFA tradicional y dar acceso directo a correo, SharePoint, Teams y datos internos.

Qué hacer ahora

- Activar MFA resistente a phishing
- Bloquear reenvíos externos y revisar OAuth apps sospechosas
- Alertar por inicios de sesión imposibles y cambios de métodos MFA

URL oficial: www.microsoft.com/en-us/security/blog

Fuentes: Microsoft, The Hacker News, TechRadar

ACONTECIMIENTOS CRÍTICOS

APT | FALSE FLAG

MuddyWater usa Teams y simula ransomware para tapar espionaje

Rapid7 vinculó una intrusión a MuddyWater, grupo asociado a Irán. El acceso inició con ingeniería social por Microsoft Teams: supuestos técnicos guiaron a la víctima para instalar herramientas remotas, manipular MFA y robar credenciales. Después apareció una narrativa de Chaos ransomware, pero el comportamiento apuntó más a espionaje y exfiltración.

Impacto: El riesgo principal es que una intrusión de espionaje parezca ransomware común y se investigue por el camino equivocado.

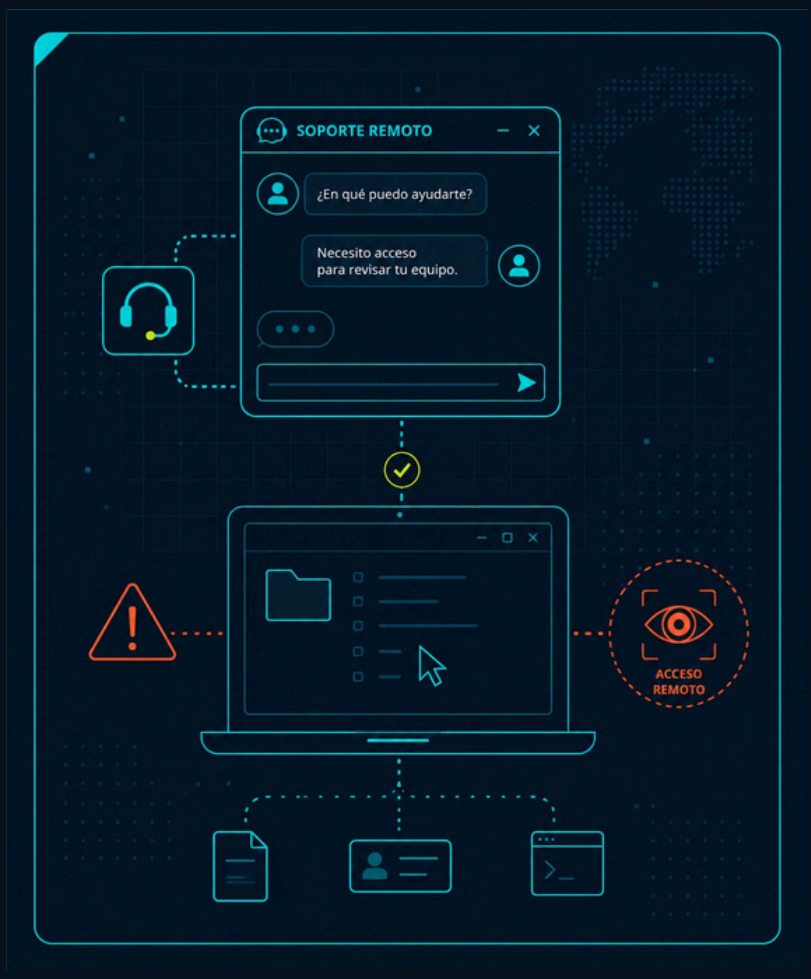
Qué hacer ahora

- Restringir comunicaciones externas en Teams
- Controlar AnyDesk, DWAgent y RMM no autorizados
- Auditar cambios de MFA y sesiones compartidas por soporte

URL oficial: www.rapid7.com/blog

Fuentes: Rapid7, The Hacker News, TechRadar

ACONTECIMIENTOS CRÍTICOS



RMM | PHISHING

VENOMOUS#HELPER: phishing con SimpleHelp y ScreenConnect

Securonix reportó una campaña activa desde 2025 que usa software legítimo de soporte remoto para quedarse dentro de los equipos. Los correos suplantan a la administración pública y convencen a usuarios de descargar herramientas como SimpleHelp o ScreenConnect.

Impacto: Los RMM legítimos pueden evadir controles básicos y dar persistencia, movimiento lateral y acceso humano directo al atacante.

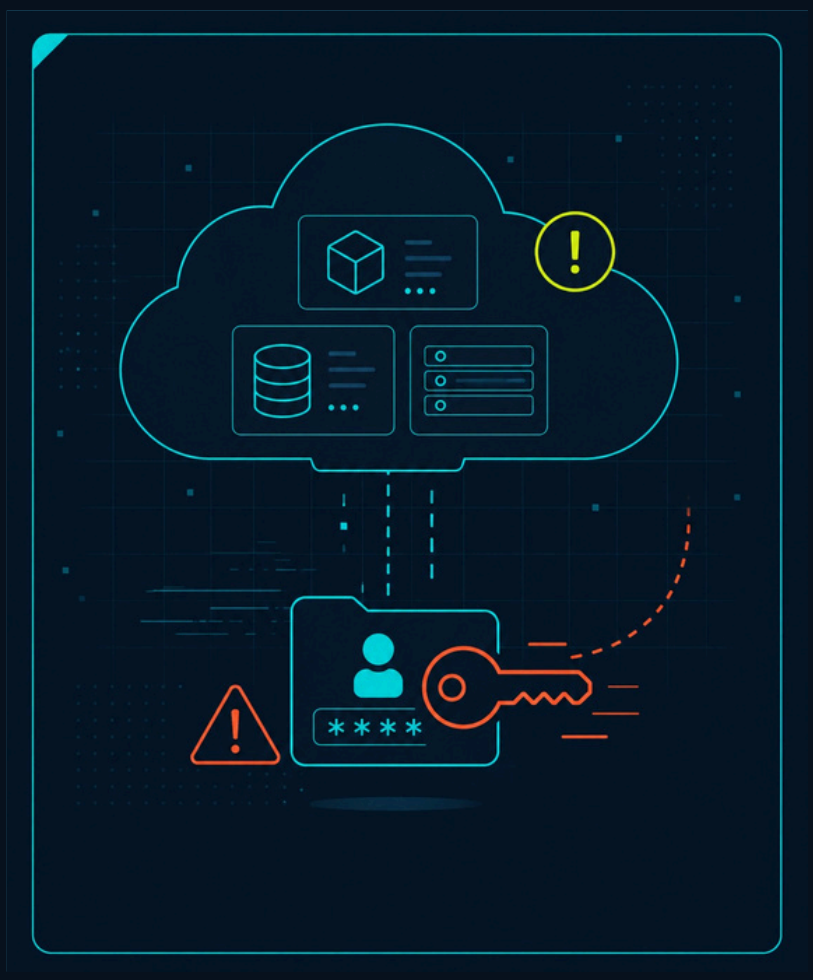
Qué hacer ahora

- Mantener una lista permitida de RMM aprobados
- Alertar instalaciones nuevas de SimpleHelp o ScreenConnect
- Bloquear correos que usen señuelos gubernamentales fuera de canales oficiales

URL oficial: Sin enlace oficial público específico al cierre

Fuentes: Securonix, The Hacker News, Network Security Magazine

ACONTECIMIENTOS CRÍTICOS



CLOUD | CREDENCIALES

PCPJack: nuevo malware roba credenciales en nubes expuestas

SentinelLabs describió PCPJack, un framework que busca servicios expuestos como Docker, Kubernetes, Redis, MongoDB, RayML y aplicaciones web vulnerables. Además de robar credenciales, intenta eliminar accesos de TeamPCP, lo que sugiere disputa entre actores por la misma infraestructura comprometida.

Impacto: Robo de secretos cloud, acceso lateral, abuso de infraestructura para fraude, spam, venta de credenciales o extorsión.

Qué hacer ahora

- Cerrar servicios cloud expuestos sin autenticación fuerte
- Rotar secretos hallados en contenedores y variables de entorno
- Revisar conexiones anómalas a Docker, Kubernetes, Redis y MongoDB

URL oficial: www.sentinelone.com/labs

Fuentes: SentinelLabs, BleepingComputer

LATINOAMÉRICA

BRASIL | BANKING TROJAN

TCLBanker: troyano bancario se propaga por WhatsApp y Outlook

Elastic reportó un nuevo troyano bancario enfocado en Brasil. Llega como instalador MSI falso de Logitech AI Prompt Builder y apunta a 59 plataformas bancarias, fintech y cripto. Su diferenciador es la propagación: usa módulos de gusano para enviar mensajes por WhatsApp y Outlook.

Impacto: Robo de credenciales financieras y expansión rápida dentro de contactos personales o corporativos.

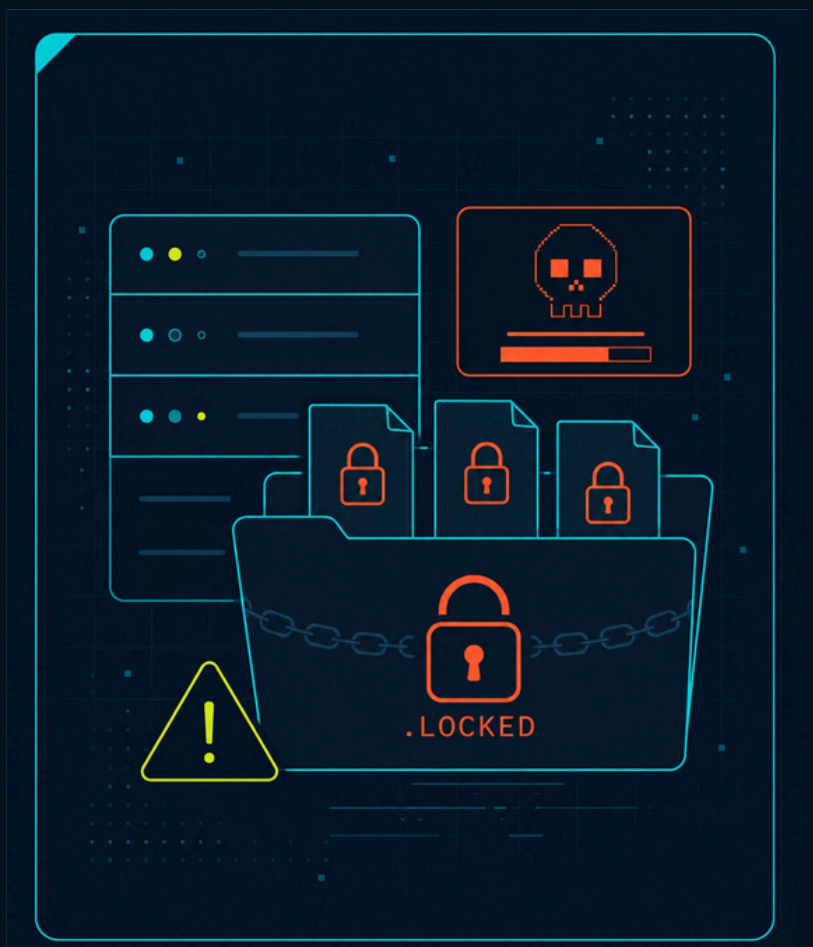
Qué hacer ahora

- Bloquear instaladores no autorizados y MSI desde descargas no confiables
- Revisar automatización de Outlook o WhatsApp inusual
- Monitorear endpoints con locale/teclado brasileño y alertas de Elastic/EDR

URL oficial: www.elastic.co/security-labs

Fuentes: Elastic Security Labs, BleepingComputer

LATINOAMÉRICA



TENDENCIA | RANSOMWARE

Brasil y México vuelven a liderar exposición regional a ransomware

ESET publicó un corte del primer trimestre de 2026 con más de 2,200 ataques de ransomware rastreados globalmente. En Latinoamérica, Brasil y México aparecen como los países con mayor presencia en el conteo regional. Los grupos más activos del trimestre fueron Qilin, The Gentlemen y Akira.

Impacto: Los sectores con más presión fueron manufactura, tecnología y salud; todos con alto costo operativo si se detienen.

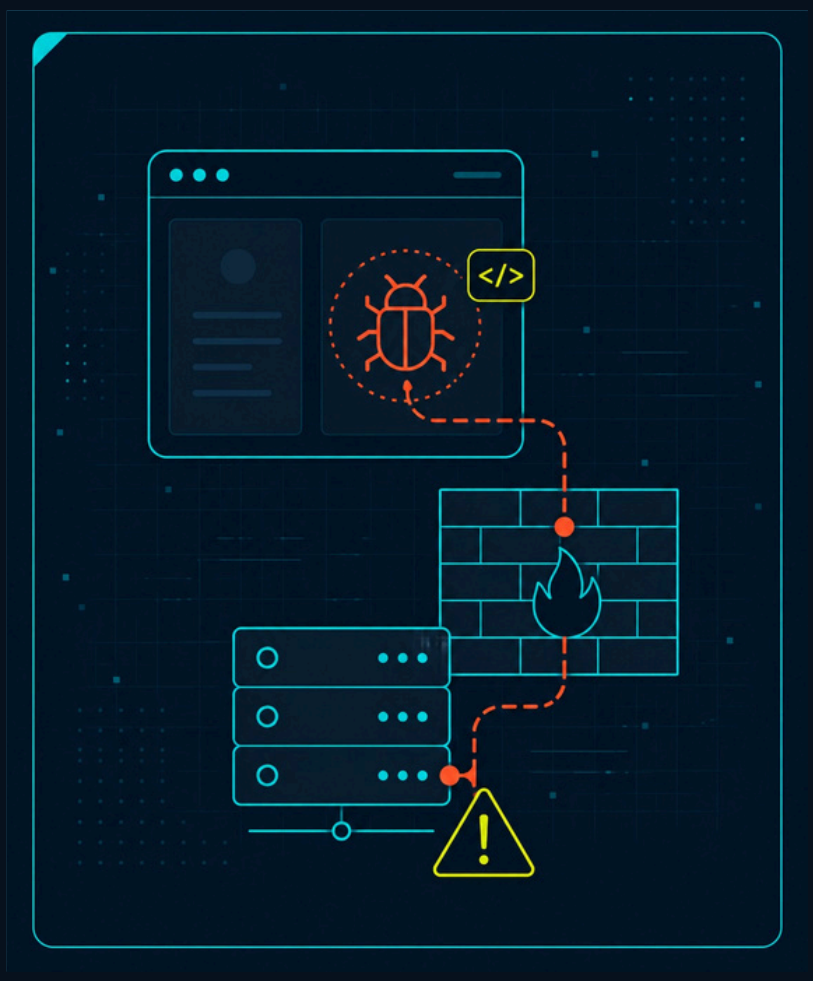
Qué hacer ahora

- Probar restauración de respaldos, no solo existencia de backups
- Separar credenciales privilegiadas y monitorear RDP/VPN
- Preparar playbook de extorsión y comunicación a clientes

URL oficial: www.eset.com/latam

Fuentes: ESET, ransomware.live, Revista Mercado

VULNERABILIDADES CRÍTICAS



KEV | EXPLOTACIÓN ACTIVA

Palo Alto PAN-OS: RCE pre-auth en User-ID Authentication Portal

CVE-2026-0300 permite ejecución remota de código como root en firewalls PA-Series y VM-Series cuando el portal está expuesto a redes no confiables o internet. Palo Alto confirmó explotación limitada y CISA lo agregó a KEV el 6 de mayo.

Impacto: Compromiso completo del firewall: control del perímetro, visibilidad de tráfico y posible pivote hacia la red interna.

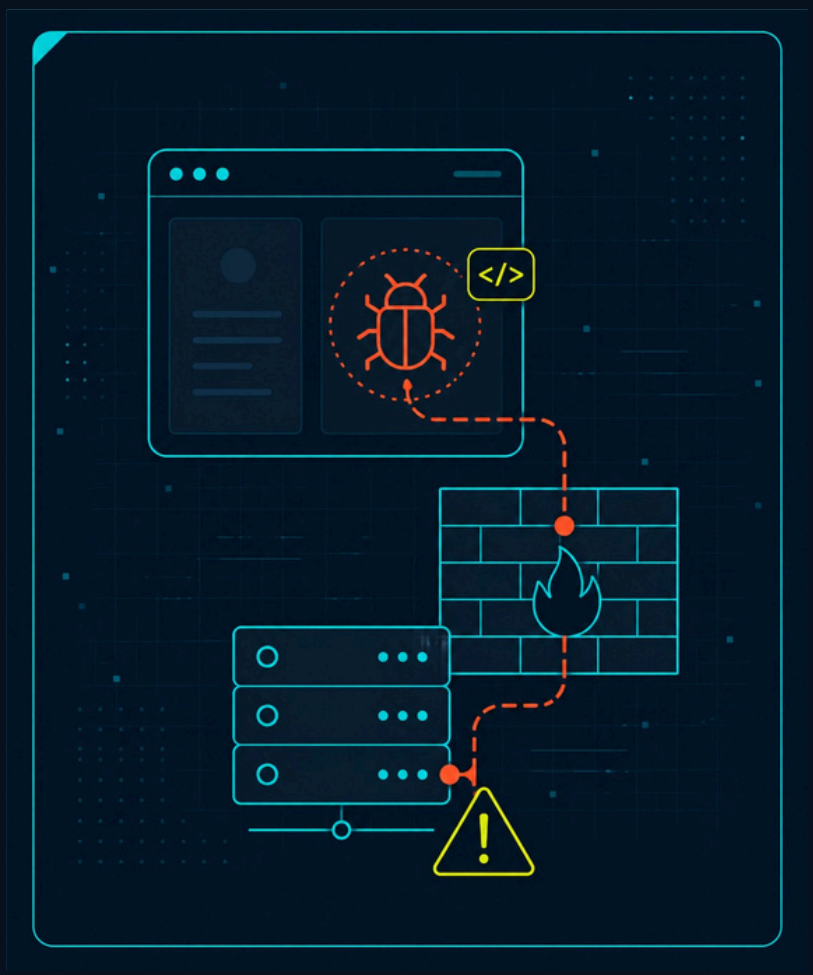
Qué hacer ahora

- Restringir el portal User-ID a zonas/IPs confiables
- Deshabilitar el portal si no se usa
- Monitorear accesos anómalos hasta aplicar los builds corregidos

URL oficial: security.paloaltonetworks.com/CVE-2026-0300

Fuentes: Palo Alto Networks, CISA KEV, NVD

VULNERABILIDADES CRÍTICAS



KEV | EXPLOTACIÓN ACTIVA

Ivanti EPMM: RCE autenticado con privilegios administrativos

CVE-2026-6973 afecta Ivanti Endpoint Manager Mobile antes de 12.6.1.1, 12.7.0.1 y 12.8.0.1. Requiere una cuenta administrativa, pero permite ejecutar código remotamente. Ivanti confirmó explotación limitada y CISA dio plazos cortos para remediar.

Impacto: Riesgo alto para plataformas MDM: acceso a administración móvil, políticas, usuarios y posible movimiento lateral.

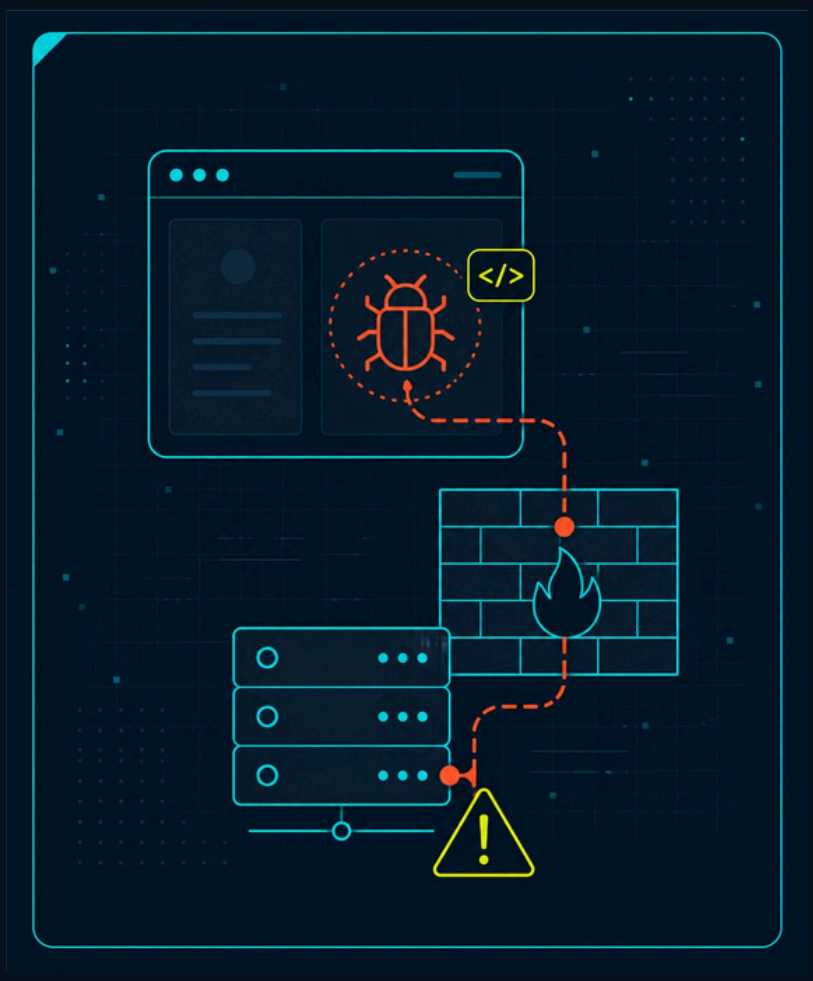
Qué hacer ahora

- Actualizar a 12.6.1.1, 12.7.0.1 o 12.8.0.1
- Revisar cuentas admin y rotar credenciales
- Buscar accesos administrativos fuera de horario o desde IPs inusuales

URL oficial: hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-EPMM

Fuentes: Ivanti, CISA KEV, NVD, BleepingComputer

VULNERABILIDADES CRÍTICAS



CRÍTICO | MFT

MOVEit Automation: bypass de autenticación y escalamiento

Progress corrigió CVE-2026-4670 y CVE-2026-5174. La primera permite saltarse autenticación; la segunda eleva privilegios. En una plataforma de transferencia automatizada, el valor para atacantes es claro: archivos sensibles, credenciales de flujos y movimiento entre sistemas.

Impacto: Exposición de transferencias empresariales y posible acceso a información financiera, legal, RH o datos de clientes.

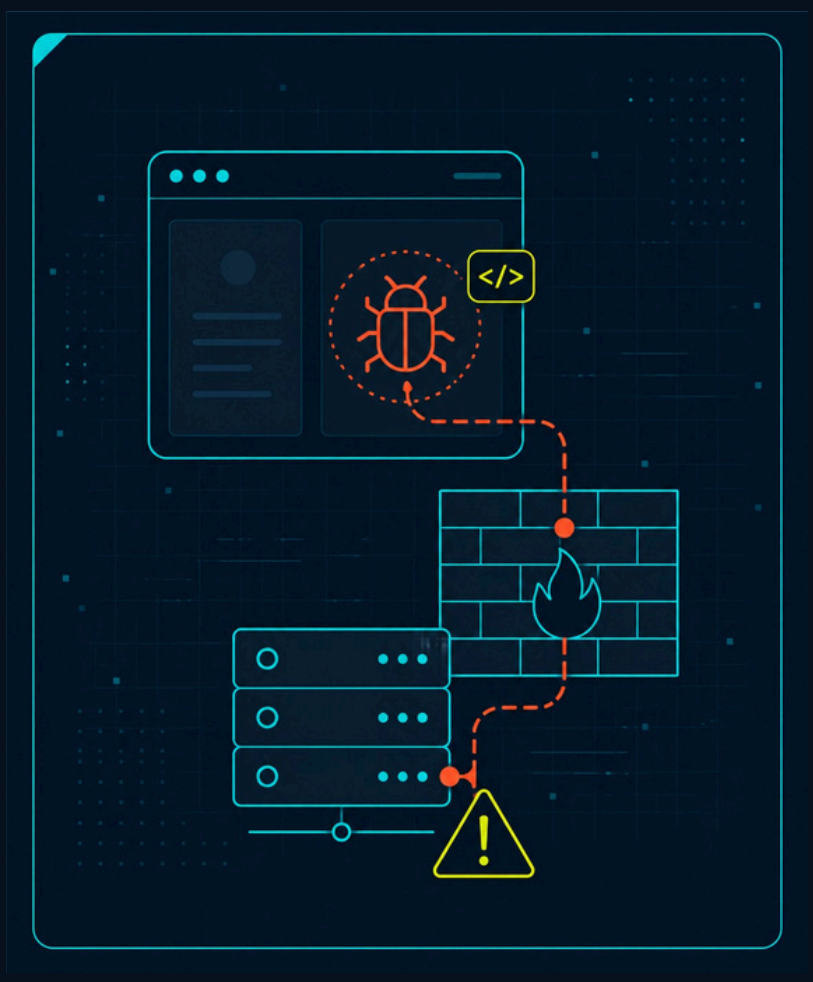
Qué hacer ahora

- Actualizar a 2025.1.5, 2025.0.9 o 2024.1.8 según rama
- Reducir exposición a internet
- Auditar tareas, credenciales guardadas y transferencias recientes

URL oficial: community.progress.com/s/article/MOVEit-Automation-Critical-Security-Alert

Fuentes: Progress, NVD, SOCRadar

VULNERABILIDADES CRÍTICAS



WEB | RCE

Apache HTTP Server y MINA: parches para RCE y deserialización

Apache HTTP Server 2.4.67 corrigió varias fallas, incluida una de HTTP/2 con posible RCE. Apache MINA publicó 2.1.12 y 2.2.7 para cerrar fallas críticas de deserialización incompletamente corregidas que podían derivar en ejecución de código.

Impacto: Riesgo en servidores web y aplicaciones Java que procesan objetos serializados con MINA.

Qué hacer ahora

- Actualizar Apache HTTP Server a 2.4.67
- Actualizar Apache MINA a 2.1.12 o 2.2.7
- Revisar exposición de HTTP/2, AJP y uso de IoBuffer.getObject()

URL oficial: httpd.apache.org/security/vulnerabilities_24.html

Fuentes: Apache HTTP Server, Apache MINA, SecurityWeek

VULNERABILIDADES CRÍTICAS

NPM | SANDBOX ESCAPE

vm2: escapes críticos permiten ejecutar código fuera del sandbox

Durante la semana se publicaron avisos críticos para vm2, una librería npm usada para ejecutar código no confiable en un entorno aislado. En la práctica, un escape de sandbox rompe esa promesa: el código del atacante puede salir del contenedor lógico y correr comandos en el host.

Impacto: Riesgo directo en plataformas que ejecutan scripts de usuarios, automatizaciones, plugins o evaluadores de código.

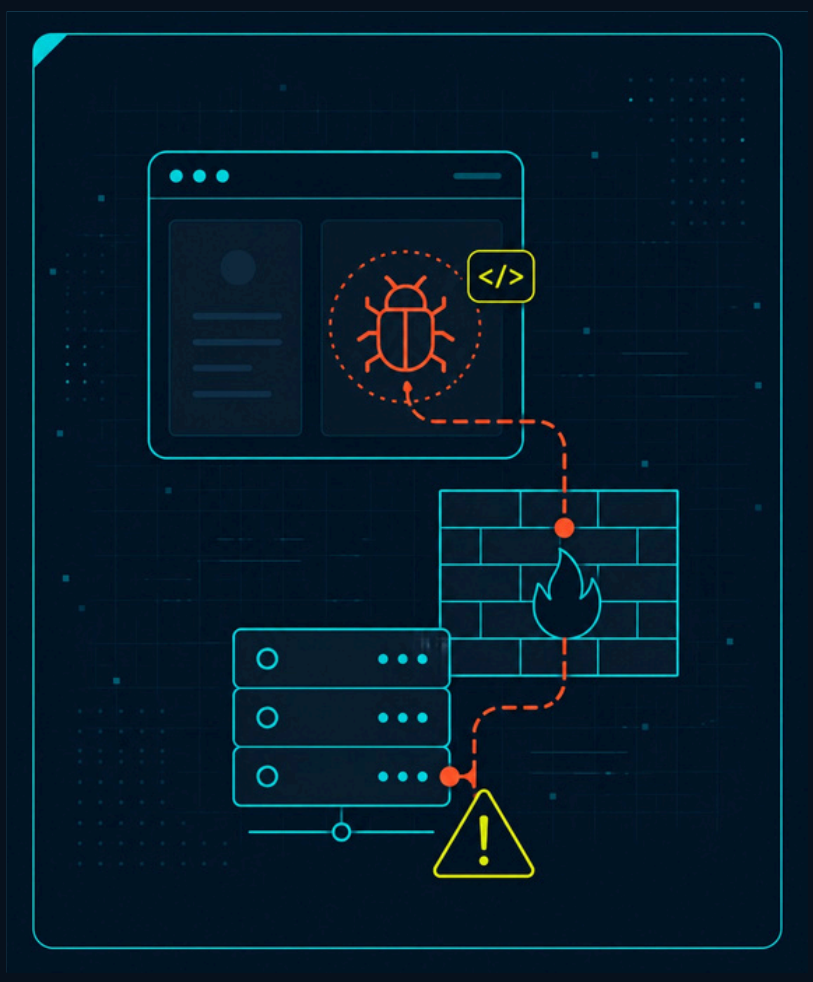
Qué hacer ahora

- Actualizar vm2 a 3.11.0 o superior
- Evitar ejecutar código no confiable en el mismo host de producción
- Revisar dependencias transitivas y locks de npm

URL oficial: github.com/advisories/GHSA-55hx-c926-fr95

Fuentes: GitHub Advisory, GitLab Advisory, Snyk, OSV

VULNERABILIDADES CRÍTICAS



ANDROID | RCE

Android May 2026: fallo crítico en System con RCE cercano

El boletín de Android del 4 de mayo corrigió vulnerabilidades del parche 2026-05-01. La más grave está en el componente System y puede permitir ejecución remota o cercana como usuario shell, sin interacción del usuario bajo ciertas condiciones.

Impacto: Riesgo en flotas Android no parcheadas, especialmente equipos corporativos con demora de actualizaciones por fabricante.

Qué hacer ahora

- Aplicar nivel de parche Android 2026-05-01 o posterior
- Priorizar equipos con acceso a correo, VPN o apps corporativas
- Aislar dispositivos que no reciban parches del fabricante

URL oficial: source.android.com/docs/security/bulletin/2026/2026-05-01

Fuentes: Android Security Bulletin

VULNERABILIDADES CRÍTICAS

LINUX | SIN PARCHE GENERAL

Dirty Frag: nuevo LPE en Linux con PoC público

Dirty Frag es una cadena de fallas en subsistemas de red del kernel Linux. Permite que un usuario local sin privilegios pueda escalar a root. A diferencia de un RCE, no entra solo desde internet; el riesgo aparece cuando el atacante ya tiene una shell, un contenedor, un runner o una cuenta limitada.

Impacto: Alto impacto en servidores multiusuario, CI/CD, Kubernetes, hosting compartido y equipos donde usuarios no confiables pueden ejecutar código local. También eleva el riesgo de movimiento lateral y control total del sistema.

Qué hacer ahora

- Aplicar kernel actualizado cuando el proveedor lo publique
- Restringir acceso local y shells no necesarias
- Mitigar módulos esp4, esp6 y rxrpc solo si no se usan IPsec/AFS

URL oficial: access.redhat.com/security/vulnerabilities/RHSB-2026-003

Fuentes: Red Hat, NHS England Digital, Phoronix

ACONTECIMIENTOS CRÍTICOS

SUPPLY CHAIN | NPM

TanStack: ataque a npm con 84 versiones maliciosas

El 11 de mayo, TanStack confirmó una cadena de suministro muy rápida: 84 versiones maliciosas en 42 paquetes @tanstack/* durante una ventana de seis minutos. El atacante combinó pull_request_target, envenenamiento de cache en GitHub Actions y extracción de un token OIDC del runner. No fue un robo clásico de token npm: fue abuso del flujo de CI/CD para publicar paquetes legítimos con malware.

Impacto: Robo de secretos de AWS, GCP, Kubernetes, Vault, GitHub, npm y SSH desde estaciones de desarrollo o runners. Si el host instaló una versión afectada, hay que tratarlo como comprometido.

Qué hacer ahora

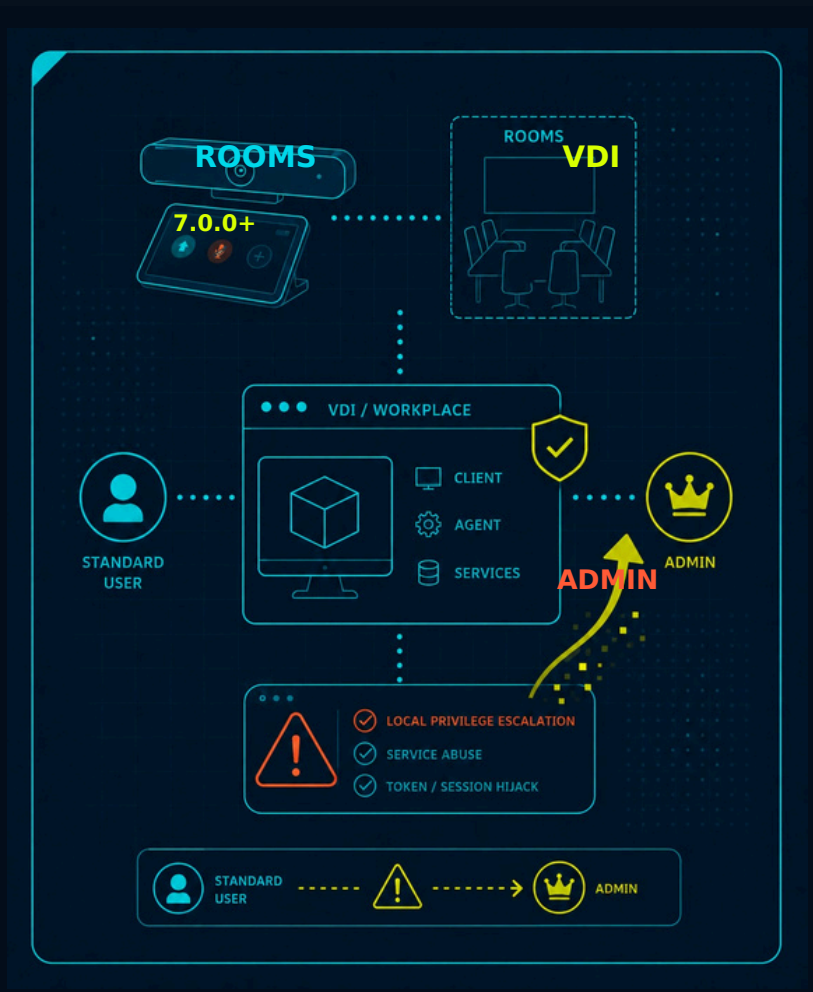
- Identificar builds que instalaron paquetes @tanstack/* afectados el 11 de mayo
- Rotar secretos accesibles desde hosts o runners que ejecutaron npm, pnpm o yarn
- Auditar pull_request_target, caches compartidos y permisos id-token: write en GitHub Actions

URL oficial: tanstack.com/blog/npm-supply-chain-compromise-postmortem

Fuentes: TanStack, GitHub Security Advisory, StepSecurity, Socket.dev

VULNERABILIDADES ALTAS

HIGH | ELEVACIÓN DE PRIVILEGIOS



Zoom Rooms y Workplace: fallas permiten elevar privilegios

Zoom publicó actualizaciones para tres fallas reportadas el 12 de mayo. Las más relevantes para empresa son CVE-2026-30906 en Zoom Rooms para Windows, por ruta de búsqueda no confiable en el instalador, y CVE-2026-30905 en Zoom Workplace VDI Plugin para Windows, por control externo de nombre o ruta. Ambas tienen CVSS 7.8 y requieren acceso local autenticado, pero sirven para convertir una cuenta estándar en una posición mucchhoo m másá sp eplieglriogsrao.sa.

Impacto: Una escalada local enequiposde sala o VDI puede facilitar desactivación de controles, robo de datoscorporativos y preparación de ransomware o movimiento lateral.

Qué hacer ahora

- Actualizar Zoom Rooms para Windows a 7.0.0 o superior
- Actualizar Zoom Workplace VDI Plugin de 6.6.10 a 6.6.11 o superior
- Revisar endpoints de salas, VDI y equipos compartidos donde usuarios no admin tienen acceso local

URL oficial: zoom.com/en/trust/security-bulletin/zsb-26008; zoom.com/en/trust/security-bulletin/zsb-26007

Fuentes: Zoom, GBHackers

VULNERABILIDADES CRÍTICAS

CRÍTICO | ERP / COMMERCE

SAP: S/4HANA y Commerce Cloud reciben parches HotNews

El Patch Day de SAP del 12 de mayo trajo dos notas HotNews con CVSS 9.6. CVE-2026-34260 afecta SAP S/4HANA Enterprise Search for ABAP y permite inyección SQL a un usuario autenticado. CVE-2026-34263 afecta SAP Commerce Cloud por una configuración de Spring Security demasiado permisiva: un usuario no autenticado puede subir configuración maliciosa e inyectar código con ejecución del lado servidor.

Impacto: Riesgo directo sobre datos de negocio, disponibilidad del ERP, comercio digital, integraciones con pagos, CRM y flujos donde SAP actúa como sistema central.

Qué hacer ahora

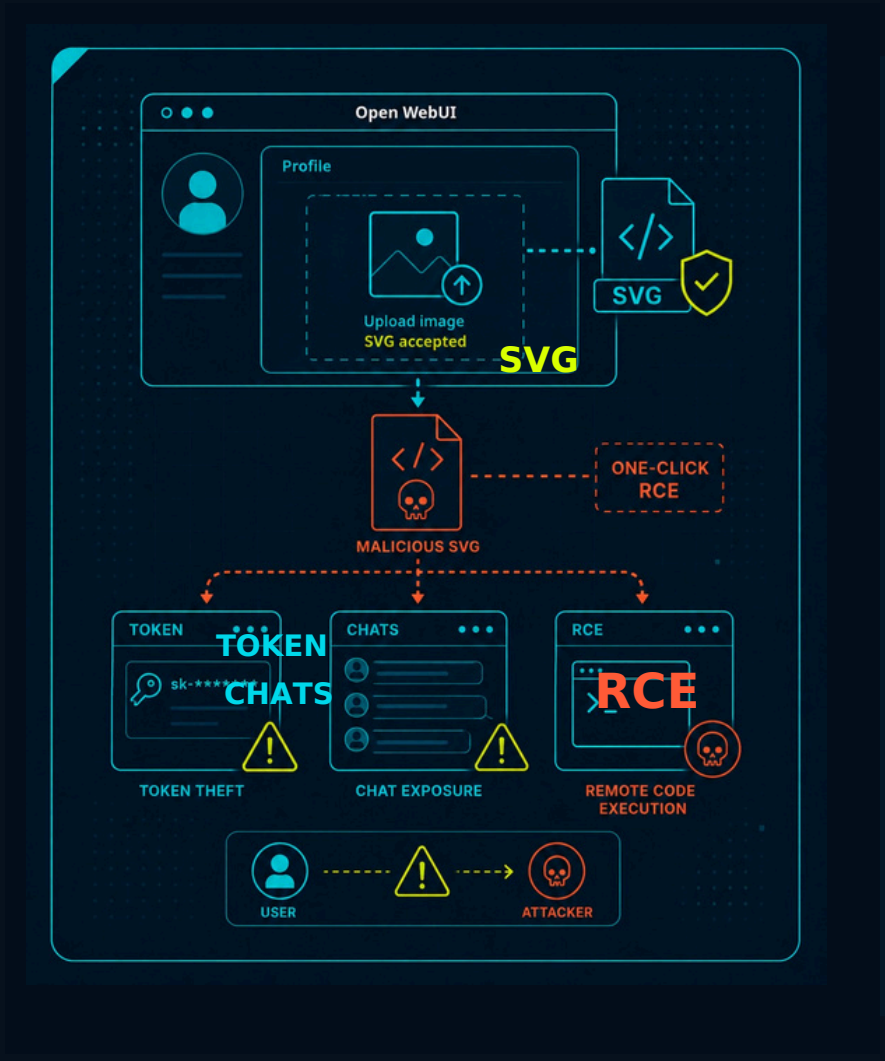
- Aplicar SAP Notes 3724838 y 3733064 del May 2026 Security Patch Day
- Priorizar instancias S/4HANA, Commerce Cloud y ambientes expuestos a internet
- Revisar logs de búsquedas ABAP, cargas de configuración y cambios no planeados

URL oficial: me.sap.com/notes/3724838; me.sap.com/notes/3733064; url.sap/sapsecuritypatchday

Fuentes: SAP, Onapsis, NVD, GBHackers

VULNERABILIDADES CRÍTICAS

0-DAY | SIN PARCHE



Open WebUI: upload de imagen deriva en RCE de 1 clic

Investigadores publicaron una falla almacenada XSS en Open WebUI que convierte una imagen de perfil en vector de ejecución remota. El backend acepta data:image/svg+xml;base64 y devuelve el contenido inline; si un administrador o usuario con permisos workspace.tools abre el enlace, el JavaScript puede crear una herramienta con payload de reverse shell. En usuarios estándar, el mismo flujo roba token y chats.

Impacto: Compromiso de cuentas, lectura de conversaciones, robo de tokens y RCE si la víctima tiene permisos altos. La divulgación incluye PoC y se reporta sin parche en 0.7.2.

Qué hacer ahora

- No abrir enlaces externos que redirijan a la instancia de Open WebUI
- Permitir solo image/png, image/jpeg, image/gif o image/webp en profile_image_url
- Restringir workspace.tools y monitorear /api/v1/tools/create, /api/v1/chats/all y cambios de imagen

URL oficial: usehacker.com/blog/open-webui-one-click-rce; github.com/open-webui/open-webui

Fuentes: UseHacker, GBHackers

VULNERABILIDADES CRÍTICAS

0-DAY | AI AGENT RCE

Cline AI Agent: WebSocket local permite RCE desde un sitio

CVE-2026-44211 afecta al paquete kanban usado por Cline CLI. El servidor WebSocket local en 127.0.0.1:3484 no valida Origin ni autentica endpoints críticos. Cualquier página visitada por el desarrollador puede conectarse al WebSocket, leer rutas, ramas Git y chats del agente; si detecta una sesión activa, puede inyectar entrada al terminal del agente y convertirla en ejecución de comandos.

Impacto: RCE en entornos de desarrollo, fuga de información de proyectos internos y terminación de tareas del agente. GitHub lo califica crítico y lista versiones afectadas menores a v2.13.0, sin versión parchada.

Qué hacer ahora

- No ejecutar Cline kanban mientras se navega por sitios no confiables
- Bloquear o aislar 127.0.0.1:3484 hasta que exista parche
- Monitorear procesos cline/kanban y revisar comandos ejecutados por agentes en endpoints de desarrollo

URL oficial: github.com/cline/cline/security/advisories/GHSA-5c57-rqjx-35g2

Fuentes: GitHub Advisory, GBHackers

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