# RADAR CTI

BOLETÍN SEMANAL
DE CIBERSEGURIDAD

## INTELIGENCIA PARA ANTICIPARNOS HOY, PROTEGER TU MAÑANA.

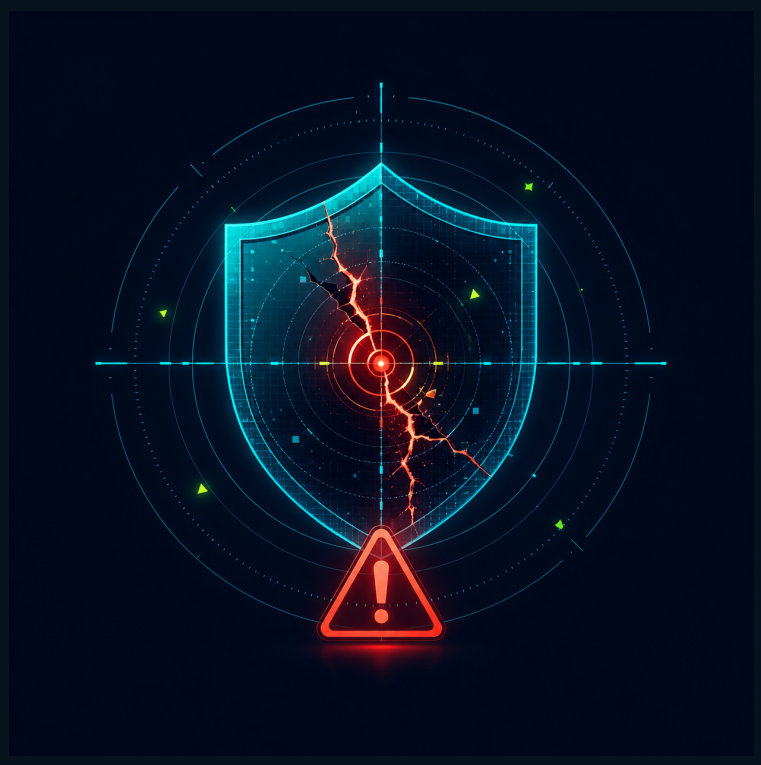
Análisis, contexto y acciones concretas sobre las amenazas más relevantes de la semana.

AMENAZAS EN LA MIRA | VULNERABILIDADES CRÍTICAS | INCIDENTES RELEVANTES | ACCIONES INMEDIATAS

Grupo Smartekh

THREAT INTELLIGENCE | VULNERABILITY MANAGEMENT | NEXT GEN SOC

# ACONTECIMIENTOS CRÍTICOS



0-DAY | VPN | QILIN

## Check Point VPN: explotación activa contra acceso remoto

La semana abrió con un tema sensible para perímetro: CVE-2026-50751 en Check Point Remote Access VPN y Mobile Access. El problema se vio en despliegues con IKEv1 heredado y permite conexiones VPN no autorizadas bajo ciertas condiciones. Check Point lo trató como explotación real y reportes públicos lo vinculan con incidentes donde apareció Qilin ransomware.

**Impacto:** Para una organización mexicana, esto no es solo una falla de VPN. Es una posible puerta de entrada a red interna, movimiento lateral y ransomware. Si el gateway estuvo expuesto, conviene asumir que puede haber habido prueba o abuso antes del parche.

### Qué hacer ahora

- Aplicar el hotfix oficial de Check Point para CVE-2026-50751 en la rama instalada; validar Quantum Security Gateway, CloudGuard y Quantum Spark afectados.
- Deshabilitar IKEv1 heredado donde no sea estrictamente necesario y exigir MFA efectivo en acceso remoto.
- Hacer hunting de accesos VPN anómalos desde el 7 de mayo, nuevas sesiones, cambios de grupos y actividad lateral posterior.

**URL oficial:** checkpoint.com / cisa.gov

Fuentes: Check Point, CISA, TechRadar

# VULNERABILIDADES ALTAS

CRITICAL | IVANTI | ROOT

## Ivanti Sentry: RCE como root en appliance expuesto

Ivanti publicó parches para fallas críticas en Sentry, entre ellas CVE-2026-10520 y CVE-2026-10523. El caso más delicado permite ejecución remota de comandos como root en versiones vulnerables. CISA llevó al menos una de ellas a KEV y después se observó actividad en honeypots, así que no conviene dejarla como pendiente.

**Impacto:** Sentry suele estar cerca de correo, móviles, autenticación y tráfico corporativo. Un appliance comprometido puede convertirse en pivote silencioso, no solo en un equipo aislado que se reinstala y listo.

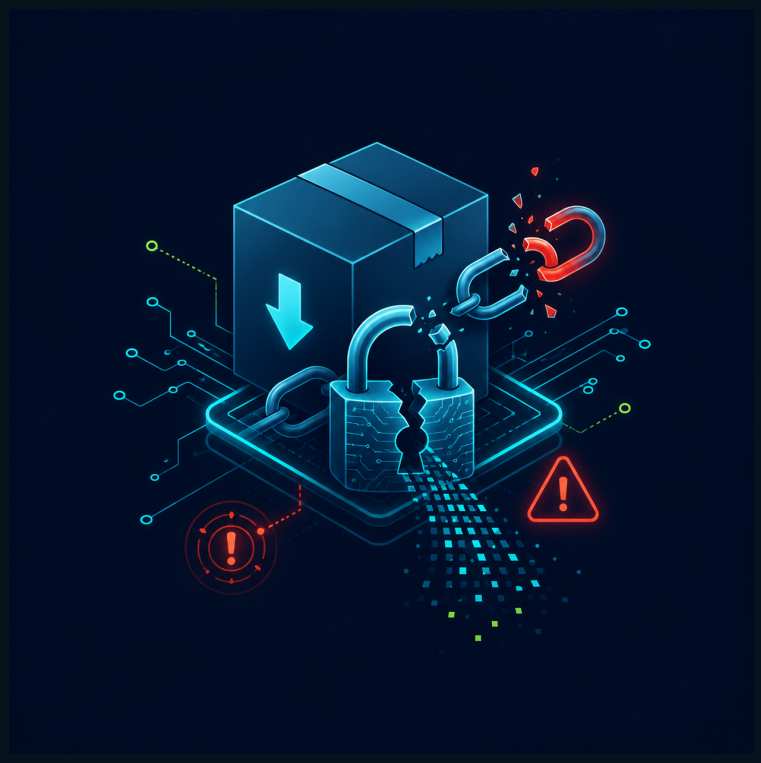
### Qué hacer ahora

- Actualizar Ivanti Sentry al release corregido por Ivanti para CVE-2026-10520 y CVE-2026-10523; confirmar build exacto contra la rama instalada.
- Restringir administración del appliance a segmentos confiables y revisar shells, procesos, cambios de configuración y conexiones salientes.
- Conservar logs antes de reiniciar o reinstalar; buscar actividad desde el 8 de junio en adelante.

**URL oficial:** ivanti.com / cisa.gov

Fuentes: Ivanti, CISA, BleepingComputer, honeypot reports

# ACONTECIMIENTOS CRÍTICOS



PEOPLESOFT | EXTORSIÓN

## PeopleSoft: explotación y extorsión sobre infraestructura enterprise

Oracle publicó una alerta fuera de ciclo para CVE-2026-35273 en PeopleSoft PeopleTools. La falla, con CVSS 9.8, es explotable sin autenticación y puede terminar en ejecución remota de código. Mandiant vinculó la campaña activa con UNC6240 / ShinyHunters, con extorsión y organizaciones de educación superior entre los blancos más visibles.

**Impacto:** PeopleSoft aparece en universidades, corporativos y entidades grandes. Si está expuesto a internet, el riesgo no se queda en la aplicación: puede incluir datos personales, cuentas internas, integraciones y servidores conectados.

### Qué hacer ahora

- Aplicar la alerta Oracle CVE-2026-35273 para PeopleTools 8.61 y 8.62; validar el parche exacto en Oracle Support.
- Revisar logs de PeopleSoft desde finales de mayo: SSRF/RCE, accesos raros, webshells, cuentas nuevas y extracción de datos.
- Reducir exposición externa, aislar integraciones y rotar credenciales usadas por PeopleSoft si hubo señales de acceso.

**URL oficial:** oracle.com / cloud.google.com

Fuentes: Oracle, Google Cloud/Mandiant, TechRadar

# VULNERABILIDADES ALTAS

WINDOWS | DC | RCE

## Windows Netlogon: controladores de dominio en prioridad...

CVE-2026-41089 vuelve a poner el foco en los domain controllers. Microsoft la clasifica como crítica, con CVSS 9.8, y el riesgo está en Netlogon: tráfico malformado contra servidores que actúan como DC puede derivar en ejecución remota o interrupción del servicio. Aunque la postura de explotación varió entre fuentes, el CCB de Bélgica la marcó como activa.

**Impacto:** En Active Directory, un DC no es un servidor más. Si un atacante toca esa capa, puede afectar autenticación, tickets, cuentas privilegiadas y continuidad operativa de toda la organización.

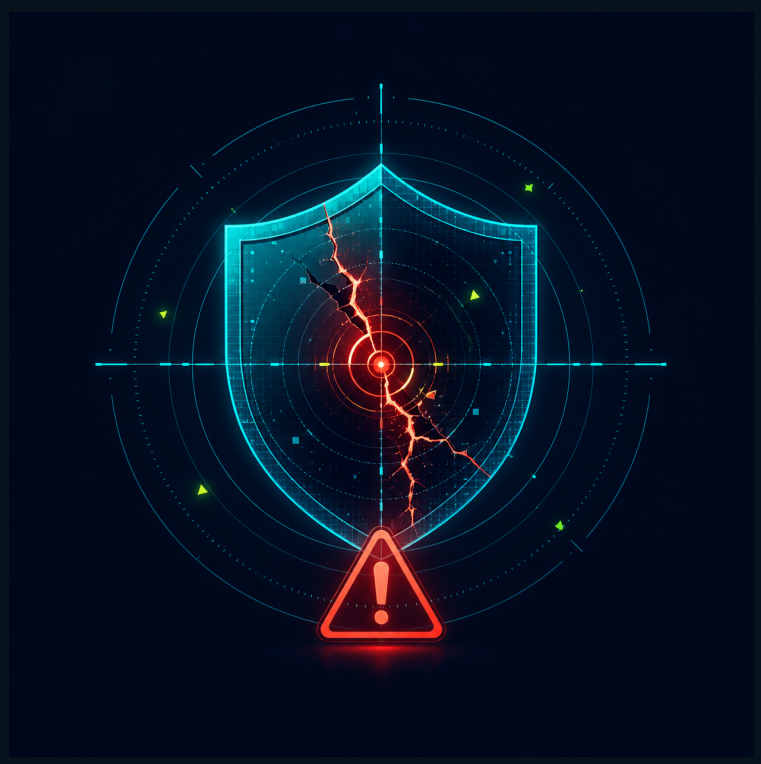
### Qué hacer ahora

- Aplicar actualizaciones Microsoft de mayo 2026 o posteriores en todos los Windows Server/DC afectados por CVE-2026-41089.
- Restringir SMB/RPC/Netlogon a segmentos confiables; no exponer controladores de dominio fuera de redes internas.
- Revisar reinicios inesperados de DC, tráfico RPC/SMB inusual, creación de cuentas y eventos Kerberos anómalos.

**URL oficial:** msrc.microsoft.com / cert.be

Fuentes: Microsoft MSRC, CCB Belgium, Tom’s Hardware

# VULNERABILIDADES ALTAS



PATCH TUESDAY | EXCHANGE

## Microsoft: junio llega con volumen alto y zero-days

El Patch Tuesday de junio corrigió cerca de 200 vulnerabilidades, con varias críticas y fallas públicamente divulgadas. Además de los temas de Windows, Exchange sigue siendo prioridad por escenarios donde un correo especialmente preparado puede ejecutar JavaScript en el navegador de la víctima desde OWA.

**Impacto:** El volumen importa porque muchos equipos aplican parches por lotes y dejan servidores para después. En este corte, los activos de administración, Exchange, endpoints de usuarios sensibles y servidores Windows deberían ir antes que el resto.

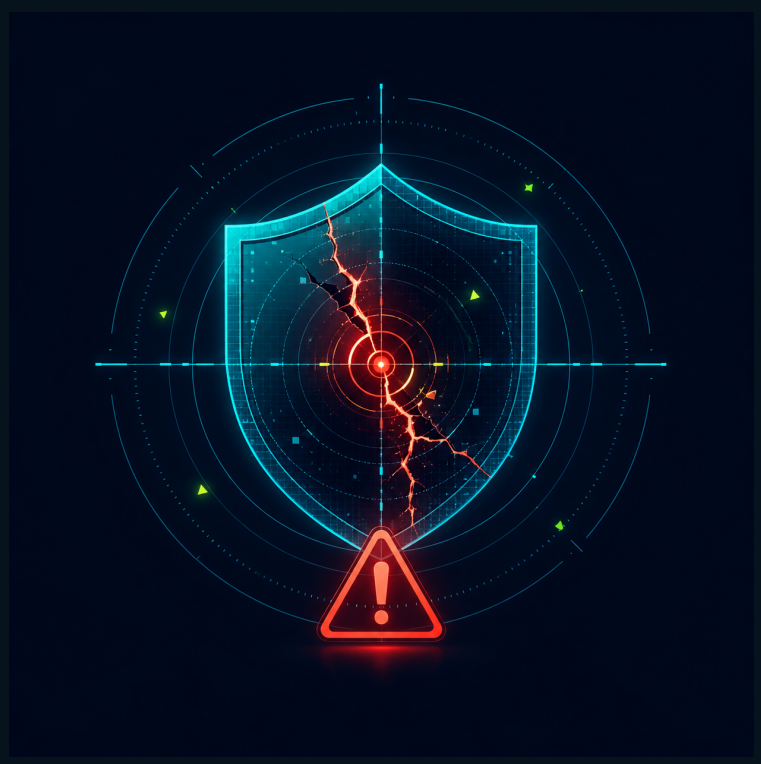
### Qué hacer ahora

- Aplicar las actualizaciones Microsoft de junio 2026 en Windows Server, Windows endpoints, Office/Exchange y equipos de administración.
- En Exchange Server 2016, 2019 y SE, validar EEMS habilitado, Health Checker limpio y mitigaciones vigentes para CVE-2026-42897.
- Priorizar equipos con OWA expuesto, administradores, finanzas, soporte y usuarios de alto riesgo.

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

Fuentes: Microsoft, BleepingComputer, TechRadar

# VULNERABILIDADES ALTAS



CHROME | V8 | KEV

## Chrome V8: explotación activa desde páginas maliciosas

Google corrigió CVE-2026-11645 en V8 y confirmó explotación en la naturaleza. El escenario no requiere mucho ruido: basta con llevar al usuario a una página preparada para ejecutar código dentro del sandbox del navegador. Por herencia, también conviene vigilar navegadores basados en Chromium.

**Impacto:** El navegador sigue siendo una puerta de entrada muy efectiva para phishing, robo de sesión y primer acceso. El riesgo sube en áreas que abren enlaces todo el día: compras, cobranza, soporte, finanzas, ejecutivos y mesa de ayuda.

### Qué hacer ahora

- Forzar Chrome 149.0.7827.102 o superior en Windows/Linux y 149.0.7827.103 o superior en macOS.
- Validar Edge, Brave, Opera y otros Chromium contra sus releases equivalentes corregidos.
- Usar EDR/MDM para confirmar versión real, no solo política de actualización aplicada.

**URL oficial:** chromereleases.googleblog.com / cisa.gov

Fuentes: Google, CISA, TechRadar

# VULNERABILIDADES ALTAS

BACKUP | RCE | VEEAM

## Veeam B&R: RCE crítica en servidor de respaldos

Veeam publicó corrección para CVE-2026-44963 en Backup & Replication. La falla permite ejecución remota de código en el servidor de backup por un usuario autenticado de dominio. Aunque requiere credenciales, el activo afectado es de los más sensibles en un escenario de ransomware.

**Impacto:** Los respaldos son la última línea de recuperación. Si el servidor Veeam cae, el atacante puede tocar repositorios, borrar tareas, preparar cifrado o impedir una restauración limpia.

### Qué hacer ahora

- Actualizar Veeam Backup & Replication a 12.3.2.4854 o superior; Veeam indica que 13.x no está afectado por esta arquitectura.
- Aislar servidores de backup, limitar usuarios de dominio con acceso y revisar sesiones remotas recientes.
- Validar tareas nuevas, cambios en repositorios, borrados, credenciales almacenadas y ejecución de comandos.

**URL oficial:** veeam.com/kb4869

Fuentes: Veeam KB4869, WatchTowr, CISA context

# VULNERABILIDADES ALTAS

SAP | SAML | PATCH DAY

## SAP Patch Day: NetWeaver y SAML al frente

SAP publicó sus notas de seguridad de junio con varias correcciones relevantes en NetWeaver, Commerce y Data Hub. Una de las más severas es CVE-2026-44748, CVSS 9.9, relacionada con XML Signature Wrapping en autenticación SAML de NetWeaver AS ABAP / ABAP Platform.

**Impacto:** SAP suele estar conectado a procesos financieros, ventas, inventario y B2B. Una falla en autenticación SAML no solo afecta login: puede tocar identidad, integraciones y flujos críticos de negocio.

### Qué hacer ahora

- Aplicar SAP Security Notes de junio 2026; priorizar CVE-2026-44748 en NetWeaver AS ABAP / ABAP Platform.
- Validar SAML, IdP, certificados, trust relationships y sistemas expuestos a usuarios externos o integraciones B2B.
- Revisar logs de autenticación, sesiones anómalas y cambios recientes en roles o perfiles SAP.

**URL oficial:** support.sap.com

Fuentes: SAP Security Patch Day June 2026

# VULNERABILIDADES ALTAS

SD-WAN | ARISTA | KEV

## Cisco y Arista: KEV empuja revisión de red

CISA agregó a KEV CVE-2026-20245 en Cisco Catalyst SD-WAN Manager y CVE-2026-7473 en Arista EOS. En Cisco, el abuso requiere privilegios netadmin o acceso previo, pero puede terminar en cambios de configuración hacia equipos edge. En Arista, el riesgo aparece en equipos usados como endpoints de túneles.

**Impacto:** Cuando el plano de administración de red cambia, el impacto se vuelve silencioso: rutas, túneles, políticas y segmentación pueden quedar alteradas sin que el usuario final note algo inmediato.

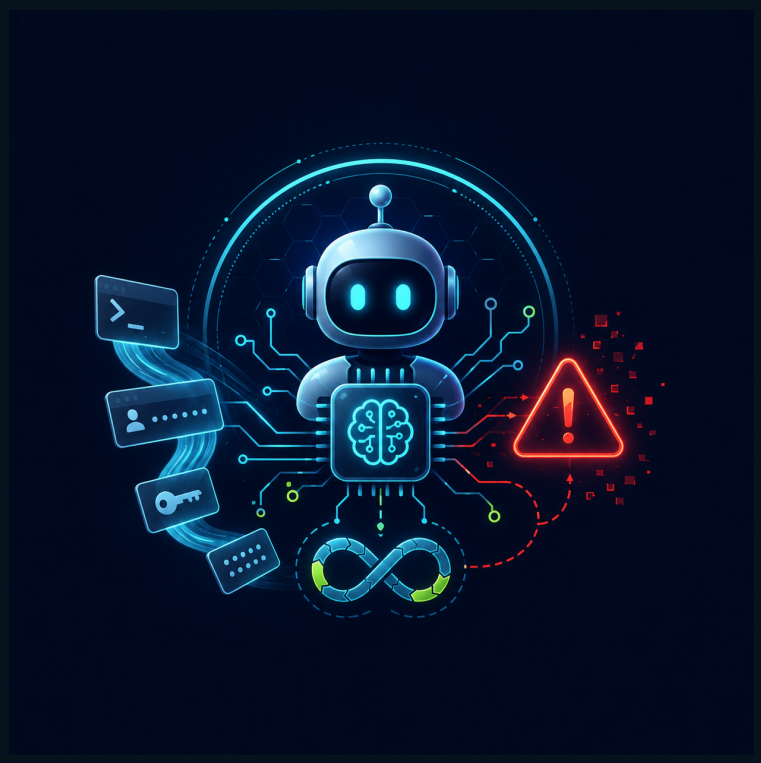
### Qué hacer ahora

- Actualizar Cisco Catalyst SD-WAN Manager al fixed software de Cisco para CVE-2026-20245 y revisar usuarios netadmin.
- Actualizar Arista EOS al fixed release aplicable para CVE-2026-7473; validar VTEP, GRE e ip decap-group.
- Comparar backups de configuración, pushes recientes, peers nuevos, túneles inesperados y cambios de ACL.

**URL oficial:** cisco.com / arista.com / cisa.gov

Fuentes: Cisco, Arista, CISA KEV

# ACONTECIMIENTOS CRÍTICOS



AI | MCP | LLM GATEWAY

## LiteLLM y Starlette: riesgo real en stacks de IA

LiteLLM CVE-2026-42271 entró a KEV y Starlette BadHost sigue siendo relevante para APIs, proxies y MCP servers. El problema no es solo una librería vulnerable: muchos equipos están exponiendo gateways LLM, dashboards y herramientas agenticas con secretos y permisos reales.

**Impacto:** Un servidor de IA comprometido puede abrir API keys, tokens cloud, secretos en .env, datos de prompts o herramientas conectadas. Si además hay MCP o automatización, el daño puede salir del servidor y tocar sistemas internos.

### Qué hacer ahora

- Actualizar Starlette a 1.0.1 o superior; revisar dependencias de FastAPI, LiteLLM, vLLM, MCP servers y proxies OpenAI-compatible.
- Actualizar LiteLLM a la release corregida para CVE-2026-42271; si no se tiene build confirmado, pasar a la última versión estable de la rama.
- Restringir endpoints MCP/REST, rotar API keys y revisar tráfico saliente desde servidores de IA o inferencia.

**URL oficial:** github.com / ostif.org / cisa.gov

Fuentes: CISA, OSTIF, TechRadar

# VULNERABILIDADES ALTAS

RMM | SIMPLEHELP | OIDC

## SimpleHelp: bypass OIDC puede abrir sesión de técnico

CVE-2026-48558 afecta SimpleHelp por un problema de verificación en OIDC: tokens sin firma válida podían ser aceptados. En una plataforma de soporte remoto, eso cambia la gravedad, porque una sesión de técnico puede convertirse en acceso directo a equipos de clientes.

**Impacto:** El riesgo es especialmente alto para proveedores de TI, mesas de ayuda y organizaciones que usan RMM para soporte masivo. Un acceso de técnico falso puede saltar rápido de una consola a muchos endpoints.

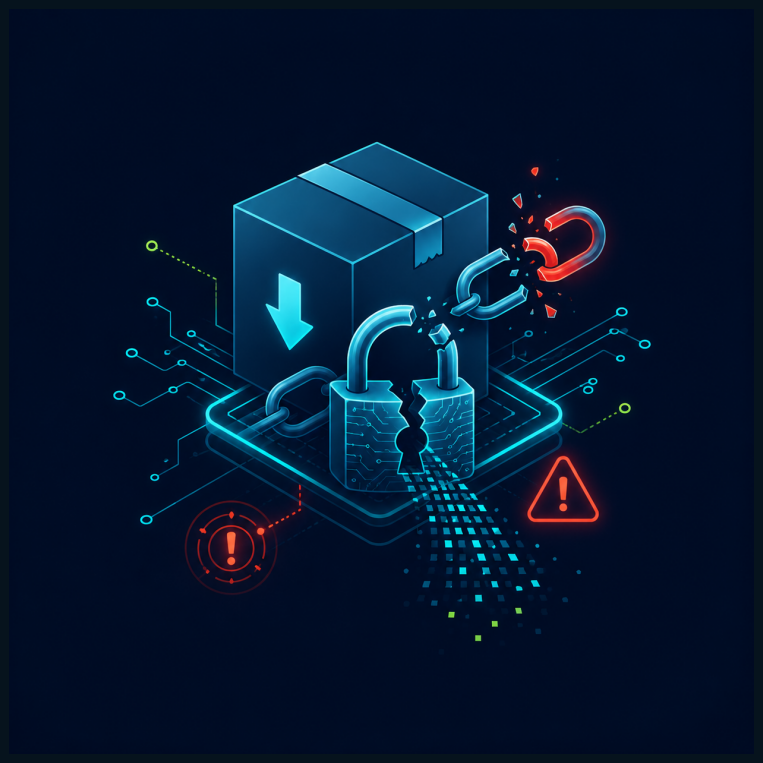
### Qué hacer ahora

- Actualizar SimpleHelp al build corregido publicado para CVE-2026-48558; si no se puede, restringir acceso de técnicos por IP/VPN.
- Revisar sesiones de técnico, inicios OIDC, bypass de MFA, nuevas conexiones remotas y acciones ejecutadas desde la consola.
- Rotar credenciales de integración y revisar equipos gestionados si hubo sesiones fuera de horario o desde ASN inusuales.

**URL oficial:** simple-help.com / horizon3.ai / opencve.io

Fuentes: SimpleHelp, Horizon3, OpenCVE

# ACONTECIMIENTOS CRÍTICOS



WORDPRESS | SUPPLY CHAIN

## WordPress: JS de plugins sirvió cuentas admin y backdoors

Sansec reportó una cadena de suministro web que involucró JavaScript servido a sitios WordPress mediante ecosistemas como OptinMonster, PushEngage y TrustPulse. El abuso permitió crear cuentas administradoras maliciosas y preparar persistencia, con exposición potencial para un volumen muy alto de sitios.

**Impacto:** No hace falta comprometer cada WordPress por separado. Si el script confiable que muchos sitios cargan cambia, el atacante hereda alcance, reputación y tráfico legítimo.

### Qué hacer ahora

- Auditar sitios WordPress que carguen scripts de OptinMonster, PushEngage o TrustPulse; revisar cuentas admin creadas en junio.
- Buscar backdoors, plugins modificados, redirecciones SEO/phishing y JavaScript extraño en temas o headers.
- Forzar rotación de credenciales admin y revisar logs de wp-admin, REST API y cambios de archivos.

**URL oficial:** sansec.io

Fuentes: Sansec, BleepingComputer, medios especializados

# LATINOAMÉRICA

**MÉXICO | FINANZAS | MUNDIAL**

## México: ransomware financiero y fraude por Mundial 2026

No apareció una brecha nueva confirmada públicamente de una empresa mexicana durante el corte. Lo que sí pesa para México es doble: Banxico actualizó su documento de incidentes cibernéticos 2026 del sistema financiero, y varios reportes alertan fraude, dominios falsos, phishing, boletaje y malware alrededor del Mundial 2026.

**Impacto:** El riesgo local no siempre llega como un titular de “empresa hackeada”. Esta semana se ve en superficie financiera, bancos, adquirentes, hospitality, entretenimiento, marcas, call centers y comercios que van a recibir tráfico y presión por el Mundial.

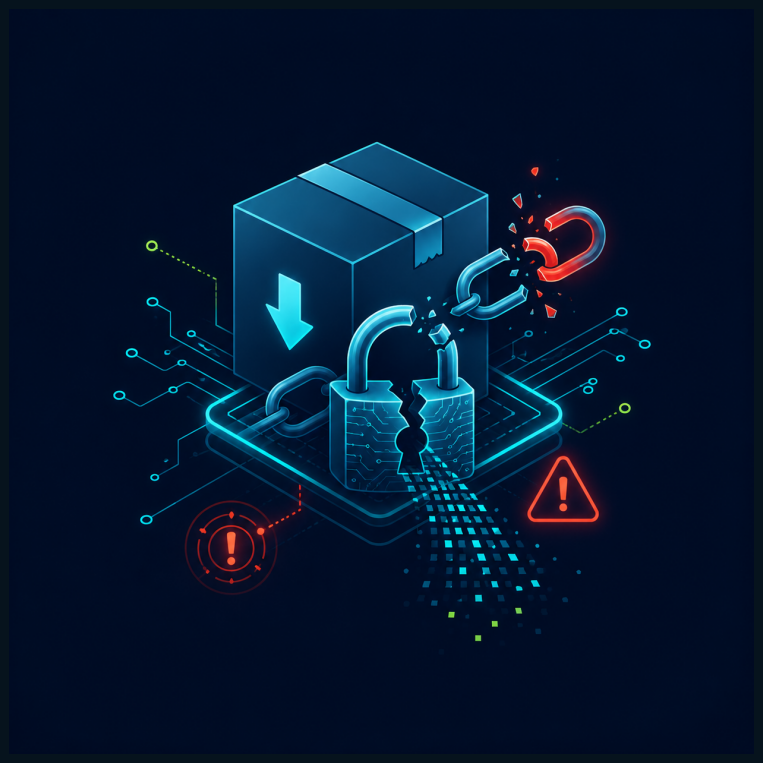
### Qué hacer ahora

- Monitorear dominios similares a FIFA, bancos, boletaje, hoteles, cines, transporte y marcas mexicanas; preparar takedown temprano.
- Usar alertas antifraude para usuarios: boletos solo en canales oficiales, cuidado con QR, anuncios patrocinados y “promociones” de último minuto.
- Revisar exposición de ransomware en sector financiero: MFA real, backups, RMM, VPN y cuentas privilegiadas.

**URL oficial:** banxico.org.mx / fortinet.com / group-ib.com

Fuentes: Banxico, Fortinet, Group-IB, FBI IC3

# ACONTECIMIENTOS CRÍTICOS



RANSOMWARE | MALWARE

## Ransomware y malware: Qilin, Gentlemen y fast-flux

Qilin vuelve a aparecer por su posible relación con explotación de Check Point VPN. The Gentlemen ganó visibilidad como RaaS activo, Silent Ransom Group fue observado usando DNS fast-flux y Huntress reportó malspam que abusa de redirecciones tipo DoubleClick para mover HTML, JScript, PowerShell y cargas .NET.

**Impacto:** La tendencia es clara: menos campañas ruidosas y más abuso de infraestructura confiable, acceso remoto, DNS dinámico y herramientas legítimas. Eso complica bloquear por IP o por hash y exige más contexto de comportamiento.

### Qué hacer ahora

- Ajustar detección por comportamiento: DNS fast-flux, RMM anómalo, PowerShell/JScript desde adjuntos HTML y conexiones a dominios nuevos.
- Cruzar hunting de VPN/RMM con señales de ransomware: enumeración, desactivación de defensas, borrado de backups y compresión/exfiltración.
- Revisar si proveedores, despachos legales o terceros críticos tienen exposición de DNS, correo o acceso remoto débil.

**URL oficial:** securityweek.com / huntress.com / thehackernews.com

Fuentes: SecurityWeek, Huntress, The Hacker News, TechRadar

# 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