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

Smartekh®

THREAT INTELLIGENCE | VULNERABILITY MANAGEMENT | NEXT GEN SOC

INFRAESTRUCTURA DE RED

FSB ruso: routers vulnerables como punto de vigilancia

FSB | ROUTERS | SNMP

El perímetro de red puede convertirse en punto de reconocimiento, persistencia y captura de configuraciones.

QUÉ ESTÁ PASANDO

NSA, CISA, FBI y aliados alertaron que el Centro 16 del FSB ruso mantiene actividad contra routers vulnerables o mal configurados. Los operadores buscan equipos expuestos, extraen configuraciones y abusan de SNMP, TFTP, credenciales débiles y fallas antiguas para ganar visibilidad de redes críticas.

POR QUÉ IMPORTA

Un router comprometido no es solo un equipo de red: puede revelar rutas internas, tráfico, credenciales y facilitar accesos posteriores sin tocar primero los endpoints.

FUENTES SUGERIDAS

NSA/CISA/FBI · IC3 · BleepingComputer

QUÉ REVISAR AHORA

- Inventariar routers expuestos y fuera de soporte.
- Restringir administración, SNMP y TFTP.
- Rotar credenciales y comunidades SNMP.
- Buscar cambios de configuración y accesos anómalos.

VULNERABILIDAD CRÍTICA

Adobe ColdFusion: RCE crítica ya explotada en campo

COLDFUSION | RCE | KEV

Servidores web heredados pueden convertirse rápidamente en acceso a sistema y datos.

QUÉ ESTÁ PASANDO

Adobe confirmó explotación limitada de CVE-2026-48282 en ColdFusion 2025 y 2023. La falla puede permitir ejecución de código en el servidor, por lo que CISA la agregó a KEV y Adobe publicó los updates 2025 Update 10 y 2023 Update 21.

POR QUÉ IMPORTA

ColdFusion suele sostener portales y aplicaciones conectadas a bases de datos. Si está expuesto, el atacante puede pasar de una falla web a control del servidor y extracción de información.

FUENTES SUGERIDAS

Adobe PSIRT · CISA KEV

QUÉ REVISAR AHORA

- Confirmar versiones 2025/2023 y aplicar updates.
- Priorizar servidores expuestos a Internet.
- Revisar webshells, procesos hijos y cargas inusuales.
- Aislar temporalmente si no se puede parchear.

EXPLOTACIÓN MASIVA

CMS y extensiones Joomla bajo explotación activa

CMS JOOMLA KEV

El riesgo no está solo en el CMS principal: plugins y plantillas viejas abren la puerta.

QUÉ ESTÁ PASANDO

ACSC alertó una campaña global contra sitios hechos con WordPress, Joomla, Craft CMS y otros CMS. La actividad explota cargas de archivos, RCE, SSRF y deserialización; en paralelo, CISA agregó a KEV fallas explotadas en extensiones Joomla.

POR QUÉ IMPORTA

Un sitio comprometido puede alojar webshells, redirigir visitantes, robar datos o servir como puente hacia sistemas internos. El plugin olvidado puede ser el eslabón débil.

FUENTES SUGERIDAS

ACSC · CISA KEV

QUÉ REVISAR AHORA

- Inventariar WordPress, Joomla, Craft CMS y plugins.
- Actualizar o retirar extensiones sin soporte.
- Buscar webshells, uploads raros y redirecciones.
- Separar hosting web de redes internas.

IA / KEV

Langflow: falla de autorización explotada en flujos de IA

LANGFLOW | IA | KEV

Los flujos de IA pueden contener secretos, conectores y acceso indirecto a datos del negocio.

QUÉ ESTÁ PASANDO

CISA agregó a KEV una falla en Langflow anterior a 1.9.1. El problema permite que un usuario autenticado ejecute flujos de otra persona si obtiene el identificador del flujo, incluso cuando esos flujos conectan datos, modelos o servicios internos.

FUENTES SUGERIDAS

GitHub Advisory · CISA KEV

POR QUÉ IMPORTA

Las plataformas de IA concentran conectores y secretos. Una falla de autorización puede ejecutar acciones con permisos ajenos y exponer información sin explotar un servidor tradicional.

QUÉ REVISAR AHORA

- Actualizar Langflow a 1.9.1 o superior.
- Restringir acceso a entornos de IA internos.
- Revisar ejecución de flujos entre usuarios.
- Rotar secretos usados por conectores.

DEVOPS / ACCESO

Gitea Docker: auth bypass amenaza repositorios internos

GITEA DOCKER CI/CD

Un repositorio comprometido puede exponer código, secretos, webhooks y pipelines.

QUÉ ESTÁ PASANDO

Investigadores observaron intentos de explotación de CVE-2026-20896 en Gitea desplegado con imágenes Docker. En configuraciones con autenticación por reverse proxy, un atacante puede falsificar un encabezado confiado y entrar como otro usuario, incluso administrador.

POR QUÉ IMPORTA

Una cuenta admin de Gitea puede abrir código privado, webhooks, tokens y secretos usados por CI/CD. El impacto puede saltar de repositorios a nube o producción.

FUENTES SUGERIDAS

Gitea · SecurityWeek · BleepingComputer

QUÉ REVISAR AHORA

- Actualizar directamente a Gitea 1.26.4.
- Validar configuración de reverse proxy.
- Revisar altas, tokens y actividad admin.
- Rotar secretos de webhooks y pipelines.

SUPPLY CHAIN

Jscrambler npm: paquete legítimo distribuyó infostealer

NPM | SECRETOS | CI/CD

Una dependencia confiable puede llegar a estaciones de desarrollo y pipelines sin levantar sospechas.

QUÉ ESTÁ PASANDO

Jscrambler confirmó que una credencial de publicación npm fue comprometida. Durante una ventana corta, versiones legítimas del paquete ejecutaban código al instalarse y buscaban secretos de nube, repositorios, Kubernetes, navegadores, CI/CD y herramientas de IA.

FUENTES SUGERIDAS

Jscrambler · Socket · BleepingComputer

POR QUÉ IMPORTA

La víctima no descarga un paquete extraño: instala una dependencia confiable. Los secretos robados pueden habilitar una segunda fase contra repositorios, nube o producción.

QUÉ REVISAR AHORA

- Identificar instalaciones durante la ventana afectada.
- Rotar llaves cloud, tokens y credenciales CI/CD.
- Revisar endpoints de desarrollo y runners.
- Reinstalar desde versiones seguras verificadas.

ACCESO PRIVILEGIADO

BeyondTrust: fallas críticas en soporte remoto y PRA

PAM REMOTE CRÍTICO

La capa de soporte remoto concentra privilegios y acceso de terceros.

QUÉ ESTÁ PASANDO

BeyondTrust publicó BT26-03 para corregir cuatro vulnerabilidades en Remote Support y Privileged Remote Access. Dos son críticas y, bajo configuraciones específicas, podrían omitir autenticación. El fabricante indicó que no observó explotación activa.

FUENTES SUGERIDAS

BeyondTrust · BleepingComputer

POR QUÉ IMPORTA

PAM y soporte remoto concentran sesiones administrativas, proveedores y accesos de emergencia. Un fallo aquí puede tener impacto mayor que una vulnerabilidad en una app aislada.

QUÉ REVISAR AHORA

- Confirmar versión 25.3.3 o superior.
- Validar appliances autogestionadas expuestas.
- Revisar autenticación, proveedores y sesiones.
- Auditar accesos privilegiados recientes.

OAUTH / MIDDLEWARE

RabbitMQ: secreto OAuth expuesto por plugin de administración

RABBITMQ | OAUTH | TOKENS

Un secreto de cliente puede convertirse en suplantación o tokens con privilegios.

QUÉ ESTÁ PASANDO

RabbitMQ corrigió CVE-2026-57219 en el management plugin. Si el plugin usa OAuth 2.0 como cliente confidencial, un endpoint obsoleto podía exponer el secreto OAuth sin iniciar sesión, dependiendo de la configuración.

POR QUÉ IMPORTA

RabbitMQ sostiene procesos y microservicios críticos. Si se compromete su identidad OAuth, puede afectarse la administración del broker, mensajes y aplicaciones conectadas.

FUENTES SUGERIDAS

GitHub Advisory · Miggo · SecurityWeek

QUÉ REVISAR AHORA

- Actualizar a versiones corregidas del fabricante.
- Confirmar si OAuth confidencial estuvo habilitado.
- Rotar el secreto después de actualizar.
- Revisar accesos al management plugin.

LATAM / TENDENCIA

Latinoamérica: mayor volumen regional de ataques y riesgo GenAI

LATAM GENAI RIESGO

La presión regional combina ataques sostenidos y exposición de datos en herramientas de IA.

QUÉ ESTÁ PASANDO

Check Point reportó que en junio de 2026 Latinoamérica registró 3,501 ataques semanales por organización, 27% más interanual y el mayor volumen entre regiones comparadas. También observó 5.2% de prompts GenAI de alto riesgo, por encima del promedio global.

POR QUÉ IMPORTA

La señal une dos frentes: infraestructura regional bajo presión y datos sensibles ingresados en herramientas de IA. No es una campaña única, pero sí un indicador ejecutivo de exposición.

FUENTES SUGERIDAS

Check Point Research

QUÉ REVISAR AHORA

- Priorizar exposición externa y vulnerabilidades KEV.
- Revisar gobierno de datos en herramientas GenAI.
- Reforzar identidad, MFA y segmentación.
- Enfocar educación, gobierno, salud y telecom.

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

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