BOLETÍN DE CIBERSEGURIDAD

PROTEGIENDO LA PRIVACIDAD DE QUIENES FORJAN NUESTROS VALORES

Mayo | Edición Especial: Día de la Madre

INSTINTO DE MADRE: BLINDANDO SU SEGURIDAD DIGITAL BOLETÍN DE CIBERSEGURIDAD, MAYO DE 2026

1. **Use solo fuentes oficiales para sus descargas:** Evite instalar programas o juegos de sitios desconocidos. Estos archivos suelen esconder virus diseñados para robar sus claves bancarias y personales. Use siempre tiendas oficiales para mantener sus equipos seguros.

2. **Sea prudente con lo que comparte en internet:** No publique detalles de su vida privada en redes sociales o chats de juegos. Los delincuentes usan esa información para crear estafas y suplantar su identidad. Mantener un perfil bajo es su mejor defensa.

3. **Proteja su intimidad: Asegure cámara y micrófono:** Evite ojos y oídos indiscretos tapando la cámara de su equipo cuando no la use. Esto impide que virus maliciosos graben imágenes o conversaciones privadas sin su permiso.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.

ACTUALIZACIÓN CRÍTICA PARA LA INFRAESTRUCTURA APACHE

La Apache Software Foundation lanzó una actualización urgente para corregir un fallo crítico (CVSS 8.8) en la versión 2.4.66. La vulnerabilidad permite ataques de denegación de servicio (DoS) y ejecución remota de código (RCE) mediante la manipulación del protocolo HTTP/2. Entornos basados en Debian y Docker presentan un riesgo mayor debido a su configuración de memoria predeterminada. El ataque DoS es trivial, sin requerir autenticación, lo que compromete la disponibilidad de los servicios. Se insta a los administradores a actualizar inmediatamente a la versión 2.4.67 para mitigar estos riesgos. Esta corrección es prioritaria para garantizar la integridad y continuidad de la infraestructura institucional.

FUENTE: THE HACKER NEWS

ALERTA POR EXPLOTACIÓN ACTIVA EN CMS METINFO

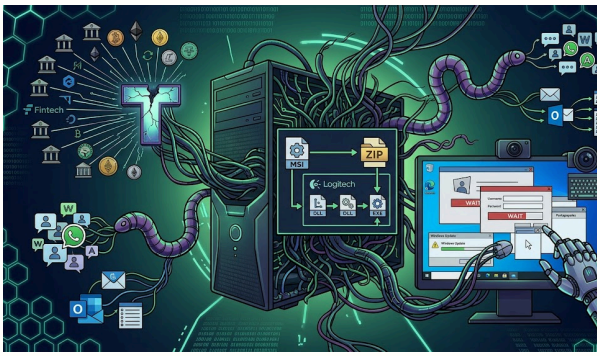
Ciberdelincuentes están explotando una vulnerabilidad crítica de inyección de código (CVE-2026-29014, CVSS 9.8) en el sistema de gestión de contenidos de código abierto MetInfo. El fallo afecta a las versiones 7.9, 8.0 y 8.1, permitiendo a atacantes remotos no autenticados ejecutar código PHP arbitrario y obtener el control total del servidor mediante solicitudes manipuladas.

La vulnerabilidad se origina por una neutralización insuficiente de datos en el script relacionado con la API de WeChat. Aunque los parches fueron publicados el 7 de abril de 2026, se ha detectado un repunte de ataques desde el 1 de mayo, dirigidos principalmente a instancias ubicadas en China y Hong Kong. Se recomienda a los administradores actualizar sus sistemas de inmediato, especialmente si el directorio de caché de WeChat está activo.

FUENTE: THE HACKER NEWS

TCLBANKER: EL NUEVO TROYANO BRASILEÑO QUE USA "LOGITECH" PARA PROPAGARSE

Expertos detectaron TCLBANKER, un malware que ataca 59 plataformas financieras mediante la carga lateral de DLL en la aplicación legítima de Logitech. Su sofisticada cadena de infección incluye potentes medidas anti-análisis y un gusano que secuestra WhatsApp y Outlook para propagarse entre los contactos de la víctima. Al usar cuentas reales, elude filtros de spam tradicionales, permitiendo a los atacantes controlar el equipo remotamente y robar credenciales mediante superposiciones falsas de alta calidad.



Este malware se enfoca principalmente en sistemas configurados en portugués brasileño para asegurar la rentabilidad de sus ataques financieros. Su capacidad para generar llamadas al sistema directas y evadir la telemetría de Windows lo convierte en una de las amenazas regionales más avanzadas.

FUENTE: THE HACKER NEWS

UNA NUEVA PUERTA TRASERA PARA LINUX, PAMDOORA, UTILIZA MÓDULOS PAM PARA ROBAR CREDENCIALES SSH.

Investigadores descubrieron PamDOORa, una herramienta de post-explotación para Linux que se vende en foros rusos y permite acceso persistente mediante SSH. Al integrarse en el marco de trabajo PAM (Módulo de Autenticación Conectable), este malware puede capturar credenciales en texto plano de todos los usuarios legítimos que inicien sesión. Además de su capacidad de robo, incluye funciones antiforenses para borrar registros de actividad y mecanismos anti-depuración, posicionándose como una amenaza de nivel profesional superior a los scripts comunes de código abierto.

FUENTE: THE HACKER NEWS

ALERTA MÁXIMA: DETECTAN VULNERABILIDADES CRÍTICAS DE DÍA CERO EN ADOBE Y MARIMO

La infraestructura digital enfrenta una amenaza severa por la explotación activa de un "Zero-Day" en Adobe Reader, que permite el control total de equipos mediante PDFs maliciosos. Paralelamente, se reportó el CVE-2026-39987 en la plataforma de IA Marimo, explotado apenas 10 horas después de su descubrimiento para ejecutar código remoto.
Junto a fallos críticos en Node.js y sistemas Linux, estas brechas facilitan el despliegue de malware como SNOWLIGHT.
Es urgente actualizar Adobe a la versión de abril 2026 y Marimo a la 0.10.16 para mitigar riesgos de exfiltración masiva.

FUENTE: BOLETÍN DE CIBERSEGURIDAD CSIRT-AMERICA