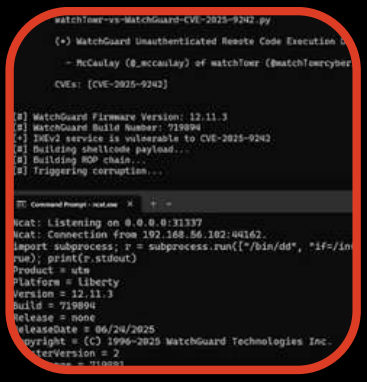
BOLETÍN INFORMATIVO N°204

OCTUBRE 2025



Investigadores descubren un fallo en la VPN de WatchGuard que podría permitir a los atacantes tomar el control de los dispositivos

Los investigadores de ciberseguridad han revelado detalles de una falla de seguridad crítica recientemente parcheada en WatchGuard Fireware que podría permitir a atacantes no autenticados ejecutar código arbitrario.

Nueva puerta trasera .NET CAPI ataca a empresas rusas de automóviles y comercio electrónico mediante ZIP de phishing

Los investigadores de ciberseguridad han arrojado luz sobre una nueva campaña que probablemente se ha dirigido a los sectores automovilístico y de comercio electrónico rusos con un malware .NET previamente no documentado denominado CAPI Backdoor.

LinkPro Linux Rootkit utiliza eBPF para ocultarse y activarse mediante paquetes TCP mágicos

Una investigación sobre la vulneración de una infraestructura alojada en Amazon Web Services (AWS) ha llevado al descubrimiento de un nuevo rootkit GNU/Linux denominado LinkPro , según los hallazgos de Synacktiv.

Microsoft revoca 200 certificados fraudulentos utilizados en la campaña de ransomware Rhysida

Microsoft reveló el jueves que revocó más de 200 certificados utilizados por un actor de amenazas que rastrea como Vanilla Tempest para firmar fraudulentamente binarios maliciosos en ataques de ransomware.

Una filtración de F5 expone el código fuente de BIG-IP: hackers de estados nacionales responsables de una intrusión masiva

La empresa estadounidense de ciberseguridad F5 reveló el miércoles que actores de amenazas no identificados irrumpieron en sus sistemas y robaron archivos que contenían parte del código fuente de BIG-IP e información relacionada con vulnerabilidades no reveladas en el producto.

Exploit PoC para vulnerabilidades de 7-Zip que permite la ejecución remota de código

Una prueba de concepto de explotación para dos vulnerabilidades críticas en el popular archivador de archivos 7-Zip, que potencialmente permite a los atacantes ejecutar código arbitrario de forma remota a través de archivos ZIP maliciosos.

RECOMENDACIONES

LECTURA DE SEGURIDAD

La mayoría de las investigaciones sobre privacidad de la IA apuntan en la dirección equivocada

La mayoría de las investigaciones sobre la privacidad de los LLM se han centrado en el problema equivocado, según un nuevo artículo de investigadores de la Universidad Carnegie Mellon y la Universidad Northeastern.

Resumen semanal: F5 vulnerado, rootkits de Linux, ataque Pixnapping, EtherHiding y más

Es fácil creer que tus defensas son sólidas, hasta que te das cuenta de que los atacantes han estado dentro de ellas todo el tiempo. Los últimos incidentes demuestran que las brechas silenciosas y a largo plazo se están convirtiendo en la norma. La mejor defensa ahora no es solo aplicar parches rápidamente, sino ser más inteligente y estar alerta ante lo inesperado.

NOTICIAS DE

NUESTROS PARTNERS

Cómo una importante empresa de ingeniería civil redujo el MTTR en la red, el correo electrónico y la nube con Darktrace

Esta empresa de ingeniería civil mantiene gran parte de la infraestructura vial del Reino Unido. Tras el fracaso de las herramientas tradicionales para detener las amenazas avanzadas por correo electrónico, la empresa adoptó la IA de Darktrace, que detectó y neutralizó los ataques de forma autónoma, lo que demostró su valor e impulsó una implementación más amplia.

Recomendaciones de seguridad de la identidad para abordar las deficiencias en la higiene de la ciberseguridad

El Aviso AA25-212A de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) revela deficiencias críticas en la higiene de la ciberseguridad en el registro, la segmentación y la gestión de credenciales en una organización de infraestructura crítica estadounidense

IBM y Groq se asocian para acelerar la implementación de IA empresarial con velocidad y escala

IBM (NYSE: IBM) y Groq anunciaron hoy una alianza estratégica de comercialización y tecnología diseñada para brindar a los clientes acceso inmediato a la tecnología de inferencia de Groq, GroqCloud , en Watsonx Orchestrate.

BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

HAZ CLICK

EVENTOS CERCANOS DE

NUESTROS PARTNERS

DARKTRACE

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información