BOLETÍN INFORMATIVO

Mainsoft

N°168

ENERO 2025

Los cibercriminales atacan a los desarrolladores de Ethereum con paquetes npm de Hardhat falsos

Investigadores de ciberseguridad han revelado varios paquetes maliciosos en el registro npm que se han hecho pasar por la herramienta Hardhat de Nomic Foundation para robar datos confidenciales de los sistemas de los desarrolladores.

El malware FireScam para Android se hace pasar por Telegram Premium para robar datos y controlar dispositivos

Se ha descubierto un malware que roba información de Android llamado FireScam, que se hace pasar por una versión premium de la aplicación de mensajería Telegram para robar datos y mantener un control remoto persistente sobre los dispositivos comprometidos.

El nuevo método de inteligencia artificial para jailbreak, 'Bad Likert Judge', aumenta las tasas de éxito de los ataques en más del 60 %

Los investigadores en ciberseguridad han arrojado luz sobre una nueva técnica de jailbreak que podría utilizarse para superar las barreras de seguridad de un modelo de lenguaje grande (LLM) y producir respuestas potencialmente dañinas o maliciosas.

Fecha límite crítica: actualice los dominios .NET antiguos antes del 7 de enero de 2025 para evitar la interrupción del servicio

Microsoft ha anunciado que está realizando un "cambio inesperado" en la forma en que se distribuyen los instaladores y archivos .NET, lo que requiere que los desarrolladores actualicen su infraestructura de producción y DevOps.

Microsoft® .NET

INCIDENTES DE

SISTEMAS

Se publica un exploit PoC para la vulnerabilidad de ejecución de código arbitrario en OpenSSH

Se ha publicado un exploit de prueba de concepto (PoC) para la vulnerabilidad crítica de OpenSSH CVE-2024-6387, también conocida como "regreSSHion", lo que ha generado alarma en toda la comunidad de ciberseguridad.

Se publica un exploit PoC para la vulnerabilidad de elevación de privilegios del Registro de Windows

Una vulnerabilidad crítica de elevación de privilegios del Registro de Windows, identificada como CVE-2024-43641. Esta falla, que afecta a varias ediciones de Windows Server 2025, Windows 10 y Windows 11, ha recibido una puntuación CVSS v3.1 de 7,8, lo que indica una gravedad alta

AWS repite la misma vulnerabilidad crítica de RCE 3 veces en 4 años

Amazon Web Services (AWS) ha introducido la misma vulnerabilidad de ejecución remota de código (RCE) tres veces en los últimos cuatro años a través de su SDK Neuron, lo que pone de relieve fallas críticas en la seguridad de sus procesos de instalación de paquetes Python

RECOMENDACIONES

LECTURA DE SEGURIDAD

Estafas más comunes en Discord y cómo evitarlas

Phishing, malware y fraudes con criptomonedas son algunas formas en que los ciberdelincuentes aprovechan Discord. Infórmate sobre estas tácticas y protege tu seguridad

Mejores prácticas para garantizar un entorno de navegación seguro

En esta entrevista de Help Net Security, Devin Ertel, CISO de Menlo Security, analiza cómo las innovaciones como la IA y una colaboración más estrecha entre los proveedores de navegadores y los proveedores de seguridad darán forma al futuro de la seguridad del navegador

Estados Unidos sanciona a empresa de seguridad china responsable de la amenaza del tifón Flax

Una empresa de ciberseguridad con sede en Beijing, presuntamente detrás del grupo de amenaza Flax Typhoon patrocinado por el estado chino, fue sancionada por el Departamento del Tesoro de Estados Unidos el viernes.

NOTICIAS DE

NUESTROS PARTNERS

Replanteamiento de la seguridad de los endpoints: el papel de la IA en la detección de amenazas

Descubra cómo las empresas pueden aprovechar la IA para mejorar la inteligencia ante amenazas y los mecanismos de respuesta para proteger los puntos finales. También analizaremos los aspectos éticos y prácticos de la implementación de la IA en un entorno de seguridad y la necesidad de sistemas con intervención humana que proporcionen control y responsabilidad y, al mismo tiempo, puedan adaptarse a las amenazas en constante evolución

Los monitores HTTP en la última plataforma Dynatrace amplían los conocimientos sobre el estado de sus puntos finales de API y simplifican la gestión de pruebas

Los monitores HTTP sintéticos brindan visibilidad las 24 horas, los 7 días de la semana y en todo el mundo sobre el estado de sus aplicaciones web y puntos finales de API críticos para el negocio. Ahora, al aprovechar toda la potencia del último SaaS Dynatrace, los monitores HTTP ofrecen un conjunto mejorado de datos, lo que permite un análisis más rápido y preciso de la causa raíz de los problemas descubiertos y acorta el tiempo medio de reparación (MTTR).

CEM Top 10: Cómo BlackBerry AtHoc supera a sus competidores

Cuando se enfrenta a eventos disruptivos, desde desastres naturales hasta disturbios civiles y ciberataques , su organización necesita una herramienta sólida de gestión de eventos críticos (CEM) para proteger sus operaciones, sus empleados y su reputación.

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

CYLANCE — Más Información

IBM Gold Partner — Más Información