BOLETÍN INFORMATIVO N°190

JULIO 2025

Fraudes masivos en Android descubiertos: IconAds, Kaleidoscope, malware SMS y estafas NFC

Una operación fraudulenta de publicidad móvil denominada IconAds que constaba de 352 aplicaciones de Android ha sido interrumpida, según un nuevo informe de HUMAN.

Hackers usan archivos PDF para hacerse pasar por Microsoft, DocuSign y otros en campañas de phishing con devolución de llamada

Los investigadores de ciberseguridad están llamando la atención sobre las campañas de phishing que se hacen pasar por marcas populares y engañan a los objetivos para que llamen a números de teléfono operados por actores de amenazas.

Más de 40 extensiones maliciosas de Firefox atacan monederos de criptomonedas y roban activos de los usuarios.

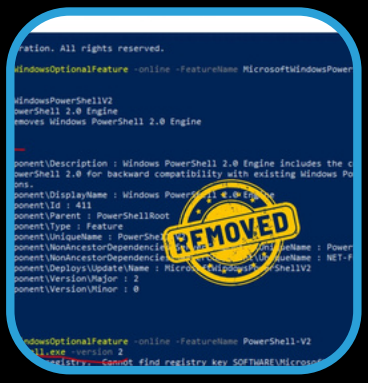
Investigadores de ciberseguridad han descubierto más de 40 extensiones de navegador maliciosas para Mozilla Firefox que están diseñadas para robar secretos de billeteras de criptomonedas, poniendo en riesgo los activos digitales de los usuarios.

Vulnerabilidades críticas de Sudo permiten a usuarios locales obtener acceso root en Linux, lo que afecta a las principales distribuciones.

Investigadores de ciberseguridad han revelado dos fallas de seguridad en la utilidad de línea de comandos Sudo para sistemas operativos Linux y similares a Unix que podrían permitir a atacantes locales escalar sus privilegios de root en máquinas susceptibles.

Microsoft eliminará PowerShell 2.0 de Windows 11 debido a riesgos de seguridad

Microsoft ha eliminado oficialmente Windows PowerShell 2.0 de las últimas compilaciones de Windows 11 Insider Preview, lo que marca una importante actualización centrada en la seguridad en el ciclo de desarrollo del sistema operativo.

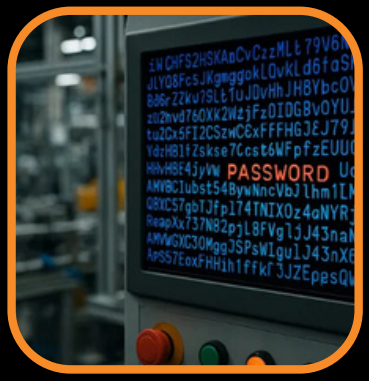


Una nueva falla en IDE como Visual Studio Code permite que extensiones maliciosas omitan el estado verificado

Un nuevo estudio de entornos de desarrollo integrados (IDE) como Microsoft Visual Studio Code, Visual Studio, IntelliJ IDEA y Cursor ha revelado debilidades en la forma en que manejan el proceso de verificación de extensiones, lo que en última instancia permite a los atacantes ejecutar código malicioso en las máquinas de los desarrolladores.

RECOMENDACIONES

LECTURA DE SEGURIDAD



Seguridad en la fabricación: ¿Por qué deben desaparecer las contraseñas predeterminadas?

Si no sabías que hackers iraníes violaron las instalaciones de agua de EE. UU., es porque solo lograron controlar una sola estación de presión que abastecía a 7000 personas. Lo que hizo que este ataque fuera notable no fue su magnitud, sino la facilidad con la que los hackers accedieron, simplemente usando la contraseña predeterminada del fabricante, "1111".

Nueva técnica detecta la manipulación o falsificación de un documento PDF

Investigadores de la Universidad de Pretoria presentaron una nueva técnica para detectar manipulaciones en documentos PDF mediante el análisis de los objetos de página del archivo. La técnica emplea un prototipo capaz de detectar cambios en un documento PDF, como modificaciones en el texto, las imágenes o los metadatos.

Resumen semanal: Se corrigieron fallas de escalada de privilegios locales de Sudo, los parches de Google explotaron activamente Chrome

A continuación se ofrece un resumen de algunas de las noticias, artículos, entrevistas y vídeos más interesantes de la semana pasada

NOTICIAS DE

NUESTROS PARTNERS

Ocho principales amenazas a la seguridad del SaaS y cómo combatirlas

La seguridad de SaaS requiere nuevos métodos para adaptarse a las amenazas y la infraestructura empresarial en constante evolución. En este blog, descubra las ocho principales amenazas a la seguridad de la identidad y cómo las soluciones basadas en IA pueden ayudar.

Registros y rastros: Por qué el contexto es fundamental para realizar investigaciones fluidas

Se disparan las alertas. Algo falla, la latencia se dispara, hay demasiado ruido y tienes la presión de encontrar la causa raíz rápidamente. Necesitas comprender cómo interactúa tu sistema para resolver el problema lo antes posible.

Deutsche Telekom elige a IBM Concert para acelerar los procesos de TI con automatización impulsada por IA

Deutsche Telekom , uno de los principales proveedores mundiales de servicios de telecomunicaciones y TI, que atiende a millones de clientes residenciales y comerciales, implementará la solución impulsada por IA IBM Concert , que permite la automatización inteligente en la gestión de parches y la orquestación de actividades relacionadas con la seguridad.

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