Edición 15

Noviembre 2025

CIBER E-DEA

Boletín de Seguridad

Seguridad louvre: Claves del robo de 100 millones.

Fallas críticas en TEAMS.

Riesgos de utilizar ChatGPT para analizar malware.

Brecha de seguridad en la Aerolínea Iberia.

Ciber Incidentes en Colombia y en el Mundo.

e-dea NETWORKS | CYBER SECURITY

Great Place To Work. Certificada NOV 2024 - NOV 2025 COL

icontec ISO 9001 CO-SC-CER890596

icontec ISO 45001 CO-ST-CER890599

icontec ISO / IEC 27001 CO-SI-2001607

IQNET CERTIFIED MANAGEMENT SYSTEM

Seguridad louvre: Claves del robo de 100 millones.

El reciente robo de joyas en el Museo del Louvre, valoradas en más de 100 millones de dólares, ha destapado una serie de fallas de seguridad que parecen sacadas de una novela de misterio. Una investigación del diario francés Libération reveló que el museo más visitado del mundo operaba con sistemas informáticos obsoletos y contraseñas tan evidentes como "LOUVRE" para acceder a sus servidores críticos.

Las auditorías realizadas por la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) desde 2014 ya habían alertado sobre vulnerabilidades críticas:

- Contraseñas débiles como "LOUVRE" para acceder a la red de videovigilancia.
- Software desactualizado, incluyendo versiones antiguas de Windows (2000, XP y Server 2003), sin soporte desde hace más de una década.
- Riesgo de manipulación de cámaras y accesos físicos.

Advertencias ignoradas

Durante más de diez años, auditorías internas y externas señalaron la necesidad de reforzar protocolos, actualizar sistemas y cambiar contraseñas.

Sin embargo, las recomendaciones fueron ignoradas, dejando al museo vulnerable frente a ataques físicos y cibernéticos.

Más Información

Los errores de Microsoft Teams permiten a los atacantes hacerse pasar por colegas

Tras la divulgación responsable en marzo de 2024, Microsoft abordó algunos de los problemas en agosto de 2024 bajo el identificador CVE CVE-2024-38197, y los parches posteriores se implementaron en septiembre de 2024 y octubre de 2025.

El ataque, que cubre tanto a usuarios invitados externos como a actores maliciosos internos, plantea graves riesgos, ya que socava los límites de seguridad y permite a los posibles objetivos realizar acciones no deseadas, como hacer clic en enlaces maliciosos enviados en los mensajes o compartir datos confidenciales.

Además de eso, las fallas también permitieron cambiar los nombres para mostrar en conversaciones de chat privadas modificando el tema de la conversación, así como modificar arbitrariamente los nombres para mostrar utilizados en las notificaciones de llamadas y durante la llamada, lo que permitió a un atacante falsificar las identidades de las personas que llaman en el proceso.

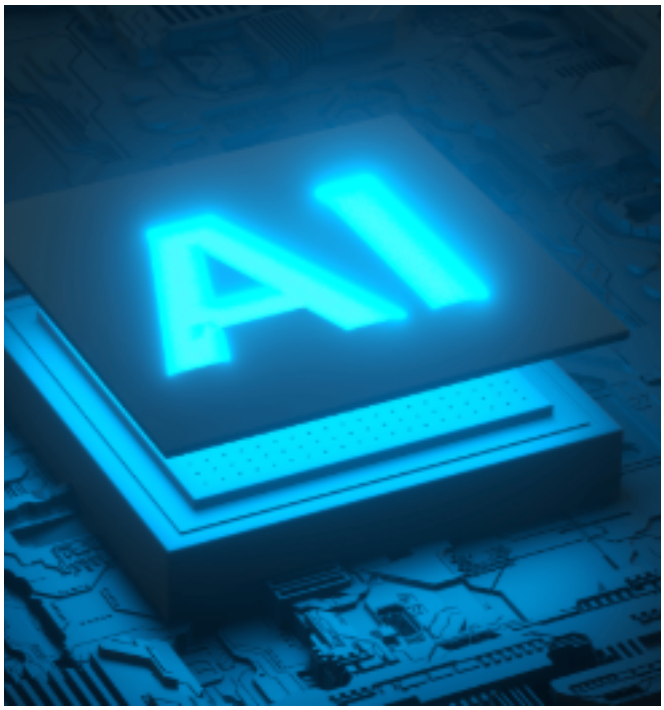
Microsoft ha descrito CVE-2024-38197 (puntuación CVSS: 6.5) como un problema de suplantación de identidad de gravedad media que afecta a Teams para iOS, lo que podría permitir a un atacante alterar el nombre del remitente de un mensaje de Teams y potencialmente engañarlo para que revele información confidencial a través de tácticas de ingeniería social.

Más Información

¿Cuáles son los riesgos de utilizar ChatGPT para analizar malware?

El uso de ChatGPT para analizar malware ofrece ventajas notables, como la capacidad de interpretar código malicioso y explicar su comportamiento en lenguaje natural, facilitando tareas de desofuscación o identificación preliminar de patrones sospechosos.

Sin embargo, también implica riesgos técnicos significativos. Entre ellos destacan la posible fuga de datos al subir muestras a la plataforma, las interpretaciones erróneas derivadas de su análisis puramente textual (ya que no ejecuta código ni realiza observaciones dinámicas), y las manipulaciones mediante técnicas de prompt injection, donde el propio malware puede incluir instrucciones ocultas o metadatos diseñados para engañar al modelo.



En definitiva, ChatGPT debe considerarse un complemento y no un sustituto de las soluciones tradicionales de ciberseguridad. El análisis de malware sigue requiriendo ejecución controlada, depuración avanzada, correlación de eventos y criterio experto.

La integración de IA en este campo debe hacerse bajo un enfoque híbrido que combine la eficiencia del modelo con el juicio humano y las defensas técnicas consolidadas.

Más Información

Brecha de seguridad en la Aerolínea Iberia.

Recientemente, la aerolínea Iberia ha informado sobre un incidente de seguridad que resultó en la exposición de datos de sus clientes. Según la compañía, la información comprometida no se ha utilizado de forma fraudulenta, pero el evento subraya la necesidad de mantener una postura de seguridad proactiva.

Este tipo de incidentes nos recuerda que, incluso en ausencia de uso fraudulento inmediato, los datos expuestos pueden ser utilizados en futuros ataques de phishing, ingeniería social o para intentos de acceso a otras cuentas (mediante la técnica de credential stuffing).

Medidas inmediatas recomendadas

- Cambie inmediatamente la contraseña de su cuenta.
- Elija una contraseña fuerte y única que combine letras mayúsculas y minúsculas, números y símbolos.
- Si utilizó la misma contraseña de Iberia para otros servicios o cuentas, cámbielas también. La reutilización de contraseñas es una de las mayores vulnerabilidades.

Más Información

Vulnerabilidades destacadas

Permite a un atacante remoto, sin necesidad de autenticarse, ejecutar código arbitrario mediante un archivo especialmente manipulado que explota GDI+.

CVE-2025-60724

Microsoft

CVE-2025-62215

Microsoft

Es una vulnerabilidad de elevación de privilegios en el kernel de Windows, que ha sido identificada como ya explotada.

Alta
9.8

Ciber incidentes en Colombia y en el mundo

Ransomware y Vulnerabilidades Zero-Trust Amenazan Infraestructura en Colombia

El COLCERT (Equipo de Respuesta a Incidentes de Seguridad Informática de Colombia) informa que la actividad cibernética en el país mantiene una alta intensidad, dirigida principalmente a entidades del sector salud y organismos gubernamentales. Los incidentes detectados en la semana reflejan una tendencia peligrosa que combina la manipulación de la infraestructura web con ataques de alto impacto.

Incidentes Locales Destacados

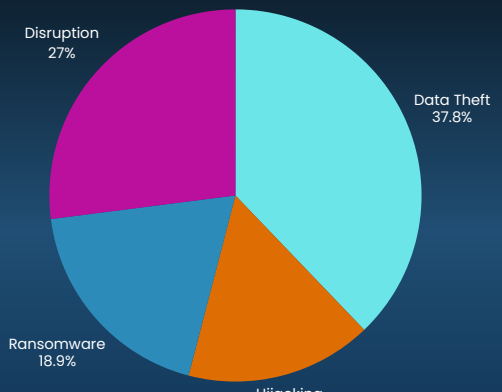
Una entidad gubernamental sufrió un ataque de ransomware que incluyó la exfiltración de datos sensibles. El grupo KillSec ha sido vinculado a operaciones de ransomware y exfiltración contra instituciones de salud

Más información

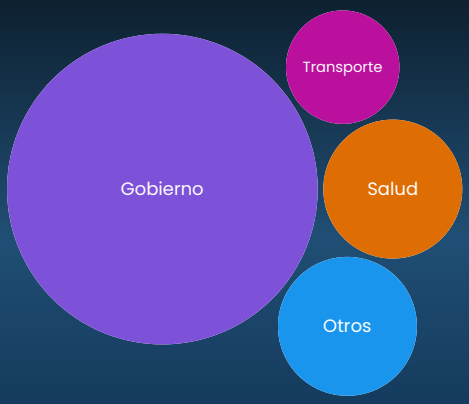
El mundo

46
Ciber incidentes

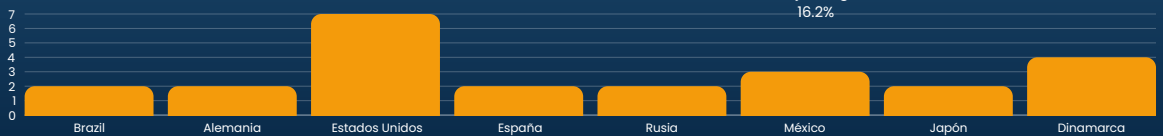
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co