BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Roban 150 GB de datos al gobierno mexicano con IA generativa

TLP:CLEAR
17.04.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: ⟶

Hackers usan IA para robar datos del gobierno

CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones

NUESTRA ESENCIA

BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

Arbitrary command execution in Cisco Smart Software Manager Center

CVE-2026-20160

Critical (9.8)

Impacto: Ejecución remota de comandos.

Resumen: Una vulnerabilidad de inyección de comandos / ejecución remota de código en Cisco Smart Software Manager On-Prem (SSM On-Prem), causada por la exposición no intencionada de un servicio interno (CWE-668: Exposure of Resource to Wrong Sphere), podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente mediante solicitudes especialmente diseñadas hacia una API expuesta.

Producto Afectado

Producto compatible afectado:

- Cisco Smart Software Manager On-Prem (SSM On-Prem).

Ver +INFO.

Solución:

Actualiza a la versión más reciente disponible que corrija la exposición del servicio interno.

Ver + INFO.

Fecha de Publicación: 01/ABR/2026 INFO

Cisco Integrated Management Controller Authentication Bypass Vulnerability

CVE-2026-20093

Critical (9.8)

Impacto: Acceso no autorizado.

Resumen: Una vulnerabilidad de omisión de autenticación (Authentication Bypass) en dispositivos Cisco Systems, causada por una validación insuficiente de credenciales en la interfaz de administración basada en web (CWE-287: Improper Authentication), podría permitir a un atacante remoto no autenticado obtener acceso a funcionalidades administrativas mediante solicitudes HTTP especialmente manipuladas.

Producto Afectado

Producto compatible afectado:

- Dispositivos Cisco con interfaz de administración web vulnerable.

Ver +INFO.

Solución:

Actualizar a las versiones corregidas proporcionadas por Cisco.

Ver +INFO.

Fecha de Publicación: 01/ABR/2026 INFO

API authentication and authorization bypass

CVE-2026-35616

Critical (9.1)

Impacto: Escalada de privilegios.

Resumen: Una vulnerabilidad de tipo Cross-Site Scripting (XSS) (CWE-79) causada por la neutralización inadecuada de entradas proporcionadas por el usuario en una aplicación web, podría permitir a un atacante inyectar y ejecutar código JavaScript arbitrario en el contexto del navegador de la víctima mediante solicitudes especialmente diseñadas. Esto puede derivar en el robo de cookies de sesión, redirecciones maliciosas o manipulación de la interfaz.

Producto Afectado

Producto compatible afectado:

- Aplicación web vulnerable (según implementación y versión específica)

Ver +INFO.

Solución:

Actualizar a versiones corregidas si el proveedor ha publicado parches.

Ver +INFO.

Fecha de Publicación: 04/ABR/2026 INFO

Unauthenticated Authentication bypass and Privilege escalation in FortiSandbox

CVE-2026-39813

Critical (9.1)

Impacto: Escalada de privilegios.

Resumen: Una vulnerabilidad de path traversal (“../filedir”) [CWE-24] en Fortinet FortiSandbox, causada por una validación insuficiente de rutas de archivos, podría permitir a un atacante remoto no autenticado manipular rutas del sistema y escalar privilegios, lo que potencialmente deriva en la ejecución de acciones no autorizadas dentro del dispositivo afectado.

Producto Afectado

Producto compatible afectado:

- Fortinet FortiSandbox 4.4.0 a 4.4.8 y 5.0.0 a 5.0.5

Ver +INFO.

Solución:

Actualizar a versiones corregidas si el proveedor ha publicado parches de seguridad

Ver +INFO.

Fecha de Publicación: 14/ABR/206 INFO

Tenable Security Center Release

CVE-2026-3909 – CVE-2026-3910

Tenable ha publicado un aviso de seguridad para su producto Security Center con el fin de corregir múltiples vulnerabilidades de alta severidad en componentes de terceros, específicamente en PostgreSQL. Estas vulnerabilidades podrían permitir a un atacante la ejecución remota de código, acceso no autorizado a información sensible y comprometer la integridad y disponibilidad del sistema.

Recomendación:

Aplicar inmediatamente el parche Security Center Patch SC202604.1, el cual actualiza PostgreSQL a la versión 16.13 y corrige las vulnerabilidades identificadas.

Productos Afectados

Los productos afectados son:

- Tenable Security Center versiones 6.5.1, 6.6.0, 6.7.2 y 6.8.0 sin el parche SC202604.1 aplicado

Ver +INFO

Fecha de Publicación: 09/ABR/2026 INFO

Google Chrome Release

CVE-2026-3845 – CVE-2026-3847

Google ha publicado una actualización de seguridad para el navegador Chrome con el fin de corregir múltiples vulnerabilidades de alta severidad, incluyendo dos fallas zero-day que están siendo explotadas activamente en el entorno real. Estas fallas podrían permitir a un atacante provocar corrupción de memoria, ejecución de código arbitrario o comprometer la estabilidad del navegador.

Recomendación:

Actualizar el navegador Google Chrome a la versión más reciente disponible de forma inmediata, ya que las vulnerabilidades están siendo explotadas activamente.

Productos Afectados:

Los productos afectados son:

- Google Chrome versiones anteriores a 146.0.7680.75/76 (Windows y macOS) y versiones anteriores a 146.0.7680.75 (Linux).

Ver +INFO

Fecha de Publicación: 10/ABR/2026 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
2/04/2026	CVE-2026-33105	Microsoft	8.7	Permite que un atacante remoto explote una vulnerabilidad en el manejo de validación de entradas en el componente afectado, enviando datos especialmente manipulados que provocan un acceso indebido a memoria, lo que puede derivar en corrupción de memoria y potencial ejecución de código arbitrario en el sistema afectado.
12/04/2026	CVE-2026-34621	Adobe	8.6	Permite que un atacante remoto explote una vulnerabilidad de desbordamiento de búfer en el componente afectado mediante el envío de datos especialmente diseñados, lo que puede provocar corrupción de memoria y potencial ejecución de código arbitrario o una denegación de servicio (DoS) en el sistema comprometido.
7/04/2026	CVE-2026-34990	Tenable	7.8	Permite que un atacante remoto explote una vulnerabilidad de validación insuficiente de entradas en el componente afectado, enviando solicitudes especialmente manipuladas que pueden provocar un consumo excesivo de recursos o comportamientos inesperados, derivando en una posible denegación de servicio (DoS) en las aplicaciones vulnerables.
08/04/02026	CVE-2026-0234	Palo alto	7.2	Permite que un atacante remoto explote una vulnerabilidad en el manejo de datos dentro del componente afectado, enviando entradas especialmente manipuladas que pueden provocar un comportamiento inesperado del sistema, lo que podría derivar en una denegación de servicio (DoS) o, en determinados escenarios, permitir la ejecución de acciones no autorizadas en la aplicación vulnerable.
9/04/2026	CVE-2026-0385	Microsoft	5.0	Permite que un atacante remoto explote una vulnerabilidad en el procesamiento de entradas en el componente afectado, enviando datos especialmente diseñados que pueden causar un manejo incorrecto de memoria o de estados internos, lo que podría derivar en una denegación de servicio (DoS) o en la ejecución de comportamientos no previstos en la aplicación vulnerable.
8/04/2026	CVE-2026-34197	Apache	4.0	Permite que un atacante remoto explote una vulnerabilidad en la validación y manejo de entradas dentro del componente afectado, enviando solicitudes especialmente manipuladas que pueden provocar corrupción del estado interno de la aplicación, lo que podría derivar en una denegación de servicio (DoS) o en la ejecución de comportamientos no autorizados en el sistema vulnerable.

Hacker usa Claude Code y GPT-4.1 para robar registros del gobierno mexicano

Un hacker logró ejecutar un ciberataque altamente sofisticado contra varias agencias del gobierno de México usando herramientas de inteligencia artificial como Claude Code y GPT-4.1. Según investigadores de ciberseguridad, el atacante consiguió automatizar gran parte del proceso de intrusión, lo que le permitió operar con una eficiencia similar a la de un equipo completo. Durante el ataque, que se habría desarrollado entre finales de 2025 y principios de 2026, se habrían comprometido múltiples instituciones gubernamentales y se habrían filtrado cientos de millones de registros personales de ciudadanos, incluyendo datos fiscales, registros civiles y otra información sensible. En total, se habla de la extracción de alrededor de 150 GB de datos. El caso es considerado uno de los primeros ejemplos claros de “cibercrimen asistido por IA” a gran escala, lo que muestra cómo estas herramientas pueden acelerar y facilitar ataques que antes requerían grandes equipos técnicos.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver *+INFO*.

El ATAQUE

El ataque fue ejecutado por un solo actor que utilizó Claude Code como asistente operativo para generar scripts, automatizar comandos y realizar tareas de intrusión como reconocimiento, explotación de vulnerabilidades y movimiento dentro de sistemas comprometidos. El atacante habría manipulado los modelos de IA para que generaran código malicioso y herramientas de ataque, en algunos casos haciéndose pasar por un investigador de seguridad o “bug bounty” para evadir filtros. Además, utilizó GPT-4.1 para analizar la información robada y producir reportes estructurados, lo que le permitió decidir qué sistemas atacar después y cómo explotar mejor los datos obtenidos. También se reporta que se explotaron múltiples vulnerabilidades (alrededor de 20 CVE), y que se automatizó la exfiltración de datos desde cientos de servidores. Claude ejecutaba gran parte de los comandos remotos, mientras que scripts personalizados procesaban y enviaban la información robada para su análisis.

+ INFO

CONTEXT	INDICATOR	(MD5)
chisel_1.11.3_linux_amd64	b84450974bd3f1fc5dc09ec0edeec50647df81716e305ef391c9115c751aab17	8f4d1321af5a7df4dd6ba88dbe158d52
ysoserial.jar	2c9bddd6a1a4ec66c1078ea97dacb61eb66d1c41aec7b6d21e3c72214ce170f1	5f8b625e5b48ed2691d6314d83d9a7f2
myfile.exe	91eda7b1e7bf2b2642f7060ccc018e5d4399936c53e714adf2ddf6e104b2df01	29b6a338fe47e4d83d4e08e36cba3751
GodPotato-NET4.exe	9a8e9d587b570d4074f1c8317b163aa8d0c566efd88f294d9d85bc7776352a28	1fdb1dd742674d3939f636c3fc4b761f
IPv4	165[.]22[.]184[.]26	N/A
IPv4	159[.]65[.]202[.]204	N/A
IPv4	188[.]166[.]16[.]232	N/A
Dominio	Lightbox-voltage-acute-duncan.trycloudflare[.]com	N/A

INFO

ÚLTIMAS NOTICIAS

Hackeo a Cisco con credenciales robadas

ShinyHunters afirma haber accedido a sistemas internos de Cisco mediante credenciales comprometidas, posiblemente obtenidas en una brecha previa de tipo supply chain. Con ese acceso, lograron entrar a plataformas conectadas como Salesforce, repositorios de GitHub y entornos en la nube (AWS).Una vez dentro, los atacantes exploraron la infraestructura, recopilaron grandes volúmenes de datos (millones de registros) y obtuvieron evidencias del acceso, como capturas de pantallas de sistemas internos. Luego, usaron esta información como prueba para presionar a la empresa.

INFO

GlassWorm usa Solana para distribuir malware

El malware Storm Infostealer se distribuye como un servicio (malware-as-a-service), lo que permite a distintos atacantes usarlo fácilmente para robar información. Una vez infecta un dispositivo, se enfoca en extraer datos sensibles desde navegadores como contraseñas, cookies y billeteras de criptomonedas. Evaden la protección de Chrome enviando datos cifrados a un servidor externo, donde son desencriptados, evitando así los mecanismos de seguridad locales. Esto le permite obtener información que normalmente estaría protegida. Además, puede secuestrar sesiones activas, lo que significa que los atacantes pueden acceder a cuentas sin necesidad de contraseñas o códigos de verificación (MFA).

INFO

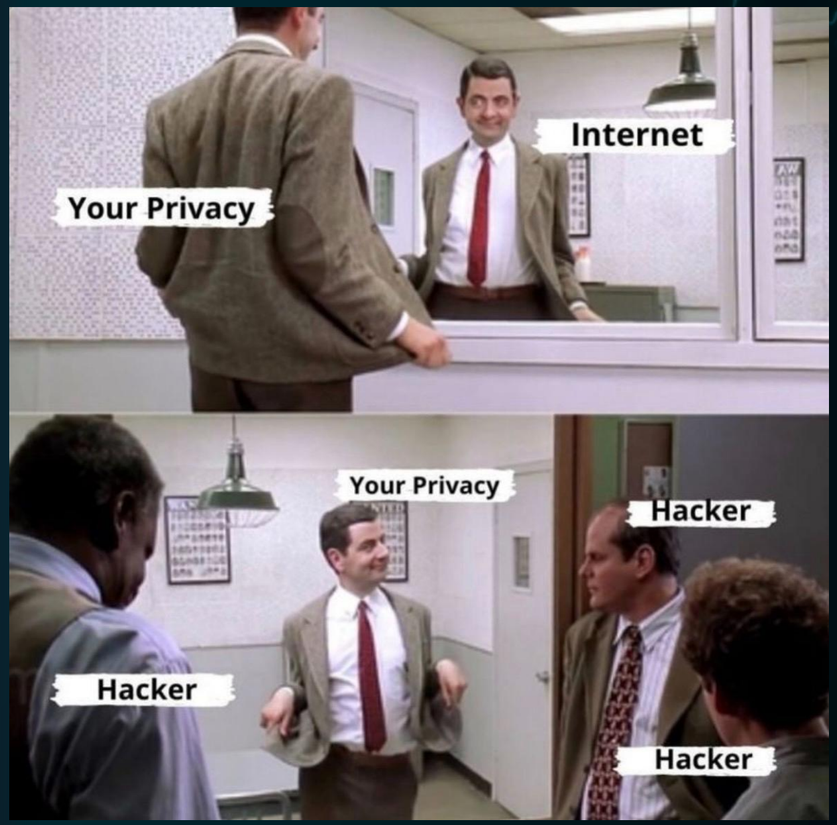
Claude Code permite inyección SQL

Vulnerabilidad en Claude Code, puede ser explotada mediante un archivo llamado CLAUDE.md. Este archivo, aparentemente inofensivo, puede incluir instrucciones maliciosas que la IA interpreta y ejecuta, permitiendo a los atacantes manipular su comportamiento. A través de esta técnica, es posible inducir a la herramienta a realizar ataques de inyección SQL, accediendo a bases de datos y extrayendo información sensible como credenciales o datos internos. El problema radica en que la IA confía en el contenido del archivo sin validar completamente su seguridad. Este tipo de ataque demuestra cómo los sistemas basados en IA pueden ser engañados para ejecutar acciones peligrosas si procesan entradas manipuladas.

INFO

Tu privacidad en internet: más observadores de los que crees

En el entorno digital, la privacidad no es un estado automático, sino una condición que depende de múltiples factores: configuraciones de seguridad, servicios utilizados, hábitos de navegación y actores externos. Con frecuencia, la información personal puede estar más expuesta de lo que el usuario percibe, ya sea por configuraciones poco restrictivas, intercambio de datos con plataformas o posibles intentos de acceso no autorizado. Por ello, entender cómo circula y se protege la información es clave para reducir riesgos.



🔍 Revisa y ajusta periódicamente la configuración de privacidad en tus cuentas y aplicaciones.
🔐 Utiliza contraseñas únicas y complejas para cada servicio.
👥 Activa la autenticación multifactor (MFA) siempre que esté disponible.
🪪 Limita la cantidad de información personal que compartes en línea.
🔁 Mantén sistemas operativos, aplicaciones y navegadores actualizados.
📶 Evita conectarte a redes WiFi públicas sin protección adicional (como VPN).
🔗 Desconfía de enlaces, archivos o mensajes inesperados, incluso si parecen legítimos.

En internet, la privacidad no desaparece… pero sí puede estar observando más de lo que imaginas.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4