BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Hackers explotan Microsoft Teams para desplegar malware SNOW

TLP:CLEAR
04.05.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

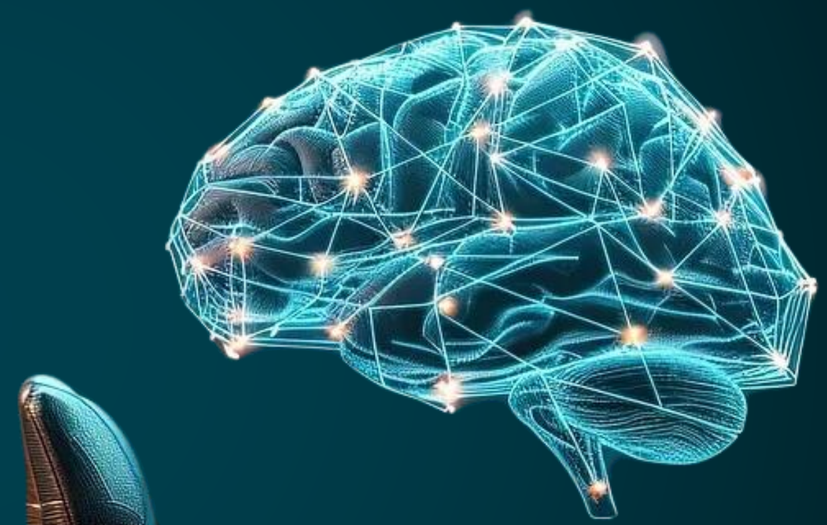
En esta edición:

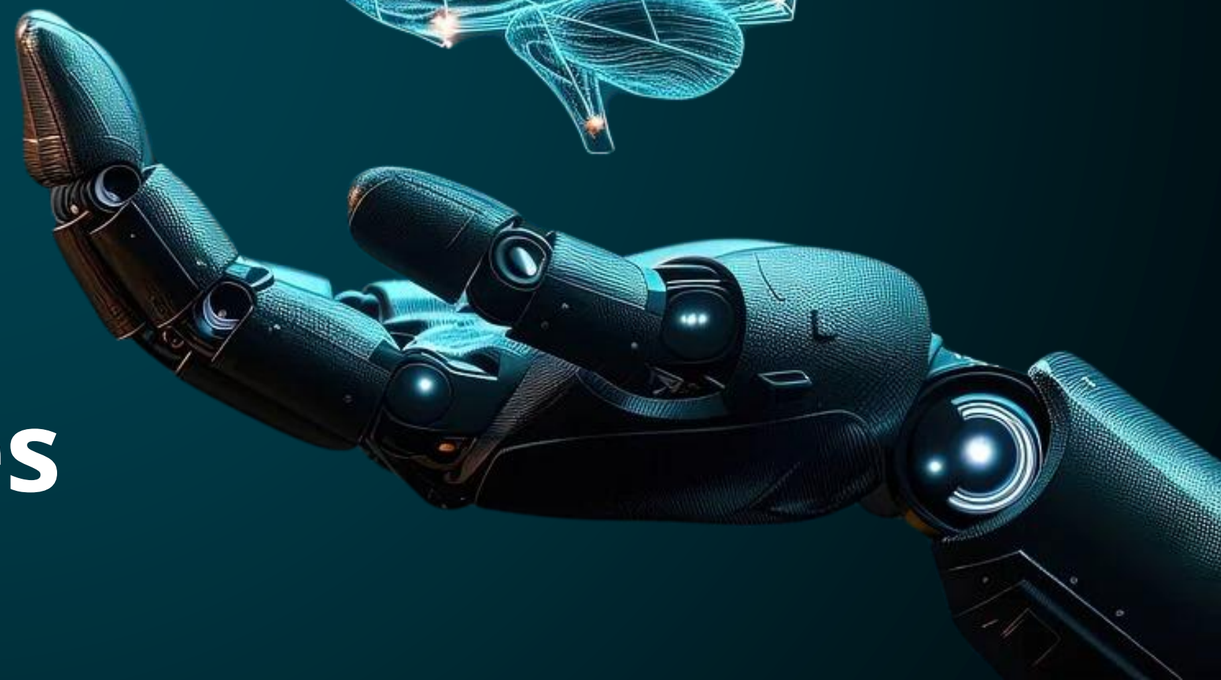
Hackers usan Teams para desplegar malware

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.

Cisco Identity Services Engine Remote Code Execution and Path Traversal Vulnerabilities

CVE-2026-20148

Critical (9.9)

Impacto: Ejecución remota de código.

Resumen: Múltiples vulnerabilidades en Cisco ISE e ISE-PIC permiten a un atacante remoto autenticado ejecutar comandos en el sistema operativo o realizar ataques de path traversal. Estas fallas se deben a una validación insuficiente de entradas. Un atacante podría enviar solicitudes HTTP manipuladas para obtener acceso al sistema e incluso escalar privilegios a nivel root.

Producto Afectado

:

- Cisco Identity Services Engine (ISE)Cisco ISE
- Passive Identity Connector (ISE-PIC)

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Cisco (versiones corregidas posteriores a las vulnerables).

Ver + INFO.

Fecha de Publicación: 15/ABR/2026 INFO

Cisco Catalyst SD-WAN Vulnerabilities

CVE-2026-20128

Critical (9.8)

Impacto: Acceso no autorizado.

Resumen: Varias vulnerabilidades en Cisco Catalyst SD-WAN Manager permiten a un atacante remoto no autenticado evadir la autenticación y acceder al sistema con privilegios elevados. Esto ocurre debido a fallos en la validación de autenticación en la API. Un atacante podría ejecutar comandos con permisos de administrador.

Producto Afectado

Producto compatible afectado:

Cisco Catalyst SD-WAN Manager (versiones anteriores a 20.18)

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Cisco (versiones corregidas posteriores a las vulnerables).

Ver +INFO.

Fecha de Publicación: 22/ABR/2026 INFO

Cisco Integrated Management Controller Command Injection and Remote Code Execution Vulnerabilities

CVE-2026-20094

High (8.8)

Impacto: Ejecución remota de código.

Resumen: Múltiples vulnerabilidades en la interfaz de gestión web de Cisco Integrated Management Controller (IMC) podrían permitir que un atacante remoto autenticado ejecute código o comandos arbitrarios en el sistema operativo subyacente, logrando la escalación de privilegios hasta nivel root.

Producto Afectado

Estas vulnerabilidades afectan a los productos Cisco que ejecuten versiones vulnerables de Cisco IMC, independientemente de la configuración del dispositivo. Para ver los productos afectados ver más info.

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Cisco (versiones corregidas posteriores a las vulnerables).

Ver +INFO.

Fecha de Publicación: 22/ABR/2026

INFO

Vulnerabilidad de desbordamiento de memoria en asyncio de Python en Windows

CVE-2026-3298

Critical (9.1)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad en asyncio de Python en Windows debido a una validación insuficiente en operaciones con sockets. Esto permite escrituras fuera de los límites de memoria mediante la función sock_recvfrom_into(), lo que puede ser explotado para ejecutar código o causar fallos en la aplicación.

Producto Afectado

Producto compatible afectado:

Aplicaciones Python en Windows que usen asyncio (ProactorEventLoop)

Ver +INFO.

Solución:

Se recomienda actualizar Python a la versión más reciente disponible con parches de seguridad, con el fin de mitigar las vulnerabilidades identificadas.

Ver +INFO.

Fecha de Publicación: 21/ABR/206

INFO

Tenable Identity Exposure Version 3.77.17 Fixes Multiple Vulnerabilities CVE-2026-33694

Tenable ha publicado un aviso de seguridad para su producto Tenable Identity Exposure con el fin de corregir múltiples vulnerabilidades en componentes de terceros como .NET Windows Server Hosting, NodeJS, Erlang OTP, SQL Server y Curl. Estas vulnerabilidades podrían comprometer la seguridad del sistema, afectando la confidencialidad, integridad y disponibilidad de la información.

Recomendación:
Actualizar Tenable Identity Exposure a la versión 3.77.17 o superior de forma inmediata.

Productos Afectados

Los productos afectados son:

- Versiones anteriores a Tenable Identity Exposure 3.77.17.

Ver +INFO

Fecha de Publicación: 23/ABR/2026

INFO

Firefox 150 - Advisory: MFSA 2026-30

CVE-2026-6746 – CVE-2026-6747

Se publicó una actualización de seguridad (MFSA 2026-30) para Mozilla Firefox que corrige múltiples vulnerabilidades graves. Algunas podían permitir corrupción de memoria, ejecución de código arbitrario o comprometer la estabilidad del navegador.

Recomendación:
Actualizar a la versión más reciente disponible (Firefox 150 o superior) para evitar riesgos de explotación de estas vulnerabilidades.

Productos Afectados:

Los productos afectados son:
Versiones de Mozilla Firefox anteriores a la 150
Firefox ESR
Mozilla Thunderbird

Ver +INFO

Fecha de Publicación: 21/ABR/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
21/04/2026	CVE-2026-35616	Fortinet	9.1	Permite que un atacante remoto no autenticado explote una vulnerabilidad de control de acceso insuficiente en FortiClient EMS. La falla en la validación de autenticación de la API permite enviar solicitudes manipuladas que evaden los controles de seguridad, lo que puede derivar en la ejecución de código o comandos no autorizados y en la escalada de privilegios dentro del sistema comprometido.
16/04/2026	CVE-2026-20184	Cisco	9.8	Permite que un atacante remoto explote una vulnerabilidad en la validación de certificados en servicios Cisco Webex (SSO). Debido a una validación incorrecta de certificados, un atacante podría suplantar identidades o ejecutar acciones con privilegios elevados, lo que podría derivar en ejecución de código arbitrario o acceso no autorizado a los servicios afectados.
24/04/2026	CVE-2023-20185	Cisco	7.4	Permite que un atacante remoto explote una vulnerabilidad en el manejo de cifrado dentro de Cisco ACI CloudSec. Esta falla podría permitir la manipulación de tráfico cifrado o el debilitamiento de los mecanismos de protección, lo que podría derivar en exposición de información sensible o alteración de comunicaciones seguras.
23/04/2026	CVE-2026-33825	Microsoft	7.8	Permite que un atacante local o remoto autenticado explote una vulnerabilidad en el manejo de memoria o validación de entradas en un componente de Microsoft. La explotación mediante datos especialmente manipulados podría provocar corrupción de memoria, lo que permitiría la ejecución de código arbitrario con privilegios elevados en el sistema afectado.

Hackers explotan Microsoft Teams para desplegar malware SNOW

Un grupo de hackers identificado como UNC6692 logró llevar a cabo una campaña de ciberataques dirigida utilizando la plataforma Microsoft Teams como vector principal de intrusión. Según investigadores de ciberseguridad, los atacantes emplearon técnicas avanzadas de ingeniería social para ganarse la confianza de las víctimas y distribuir un malware conocido como Snow malware. Este software malicioso les permitió obtener acceso no autorizado a sistemas corporativos, facilitando el robo de información sensible y el control remoto de los dispositivos comprometidos.

Durante la operación, los atacantes suplantaron personal de soporte técnico para engañar a los usuarios e instalar malware, evidenciando el uso de ingeniería social avanzada. El caso refleja la vulnerabilidad de plataformas como Microsoft Teams y el aumento de ataques que combinan manipulación con malware sofisticado.

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

El ATAQUE

El ataque del grupo UNC6692 se desarrolló en varias fases técnicas. Primero realizaron email bombing para saturar las bandejas de entrada de las víctimas y generar confusión.

Luego contactaron a los usuarios a través de Microsoft Teams haciéndose pasar por personal de soporte técnico, usando cuentas externas para parecer legítimos.

Después los dirigían a páginas de phishing donde robaban credenciales de acceso. Con esa información ejecutaban un loader (basado en scripts como AutoHotkey) que descargaba e instalaba el malware Snow malware.

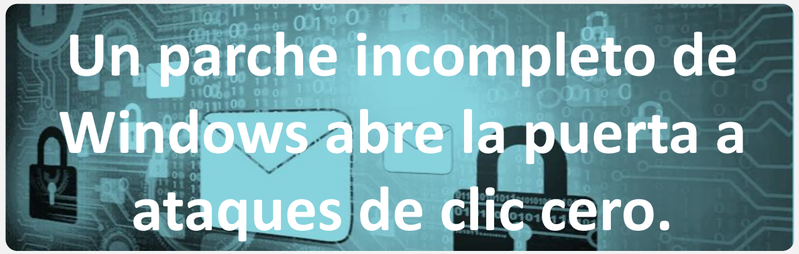
Este malware funcionaba como un framework modular con capacidades de persistencia, acceso remoto y comunicación con servidores de comando y control, permitiendo a los atacantes moverse dentro de la red y extraer información sensible.

+ INFO

CONTEXT	INDICATOR	(MD5)
SHA256	c8940de8cb917abe158a826a1d08f1083af517351d01642e6c7f324d0bba1eb8	ea3590ecf7f83f8cd5e2773f11ac1131
SHA256	ca390b86793922555c84abc3b34406da2899382c617f9dcf83a74ac09dd18190	N/A
Dominio	service-page-25144-30466-outlook.s3.us-west-2.amazonaws[.]com	N/A
Dominio	cloudfront-021.s3.us-west-2.amazonaws[.]com	N/A
Dominio	wss://sad4w7h913-b4a57f9c36eb.herokuapp[.]com/ws	N/A
Dominio	service-page-11369-28315-outlook[.]s3[.]us-west-2[.]amazonaws[.]com	N/A
Dominio	service-page-18968-2419-outlook[.]s3[.]us-west-2[.]amazonaws[.]com	N/A
Dominio	service-page-25144-30466-outlook[.]s3[.]us-west-2[.]amazonaws[.]com/update[.]html?email=<redacted>[.]com	N/A

INFO

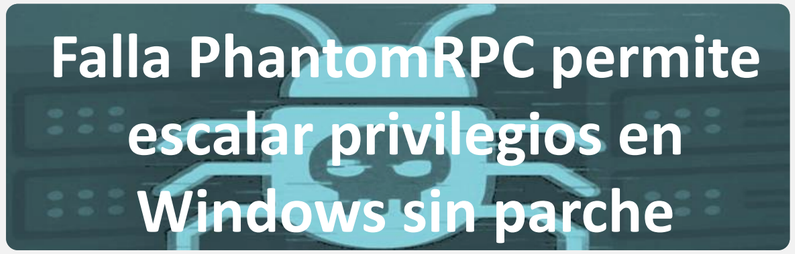
ÚLTIMAS NOTICIAS



Un parche incompleto de Windows abre la puerta a ataques de clic cero.

Investigadores de Akamai descubrieron que un parche incompleto en Windows permitió crear una nueva vulnerabilidad (CVE-2026-32202) que posibilita ataques sin clic para robar credenciales. El grupo APT28 explotó fallos previos (CVE-2026-21510 y CVE-2026-21513) mediante archivos LNK maliciosos para evadir protecciones como SmartScreen, ejecutar código remoto y forzar autenticación automática del sistema, filtrando hashes NTLM sin interacción del usuario. Microsoft ya corrigió este nuevo fallo en abril de 2026, pero fue explotado en ataques dirigidos contra Ucrania y países de la UE.

INFO



Falla PhantomRPC permite escalar privilegios en Windows sin parche

Un investigador de Kaspersky descubrió una vulnerabilidad sin parchear en Windows llamada PhantomRPC, que permite la escalada de privilegios explotando un fallo en la arquitectura del sistema RPC. Un atacante con acceso limitado puede crear un servidor malicioso que suplante servicios legítimos y engañe a procesos con altos privilegios para obtener control total del sistema. Aunque se identificaron múltiples vías de explotación, Microsoft clasificó el problema como moderado y no ha publicado un parche, por lo que las organizaciones deben aplicar medidas de mitigación como monitoreo de RPC y restricción de privilegios.

INFO

Aumentan ataques de inyección de prompts en IA

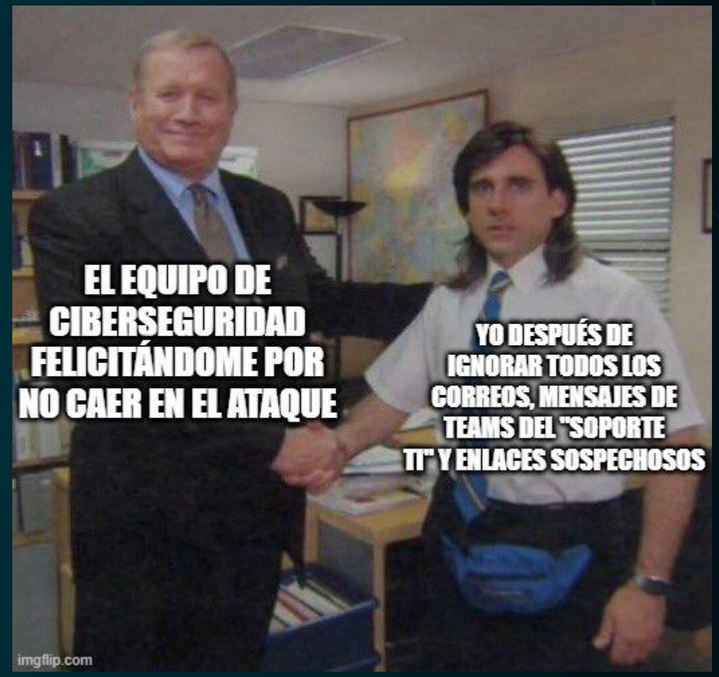
Google reporta un aumento del 32% en ataques de inyección indirecta de prompts en IA, donde se insertan instrucciones maliciosas en sitios web para manipular herramientas como asistentes inteligentes. Aunque la mayoría de estos intentos son poco sofisticados o incluso inofensivos, algunos buscan robar datos (exfiltración) o ejecutar acciones destructivas.

Los investigadores advierten que, aunque actualmente el nivel técnico es bajo, la amenaza está creciendo y se espera que estos ataques evolucionen en complejidad y alcance en el corto plazo.

INFO

En ciberseguridad: no todo lo que ignoras te protege

En el entorno digital, evitar un incidente de seguridad no siempre es resultado de una estrategia consciente, sino muchas veces de decisiones aleatorias o comportamientos poco analizados. Ignorar correos, mensajes o solicitudes puede, en algunos casos, reducir la exposición a amenazas como el phishing; sin embargo, esta práctica también puede generar riesgos operativos, pérdida de información relevante o falta de respuesta ante incidentes reales. La ciberseguridad no se basa en evitar todo, sino en saber qué identificar, qué validar y cómo actuar frente a cada situación.



🔍 Verifica siempre el origen de correos y mensajes antes de interactuar con ellos.
📩 No ignores comunicaciones importantes: analiza su legitimidad.
🔐 Aplica autenticación multifactor (MFA) para proteger accesos críticos.
⚠️ Identifica señales comunes de phishing (urgencia, errores, enlaces sospechosos).
🧠 Capacítate continuamente en buenas prácticas de seguridad digital.
🛡️ Reporta mensajes sospechosos al equipo de seguridad o TI.
🔗 Accede a servicios solo desde enlaces oficiales o previamente verificados.

En ciberseguridad, no se trata de ignorar todo... sino de entender en qué confiar.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4