BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Nueva campaña de malware instala Remcos RAT en Windows por etapas

TLP:CLEAR
20.01.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → Nueva campaña de malware instala Remcos RAT en Windows por etapas

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.

Firewall Denial of Service (DoS) in GlobalProtect Gateway and Portal

CVE-2026-0227

High (7.7)

Impacto: Denegación de servicios

Resumen: Una vulnerabilidad en el software PAN-OS de Palo Alto Networks permite a un atacante no autenticado provocar una denegación de servicio (DoS) al firewall. Los intentos repetidos de provocar este problema hacen que el firewall entre en modo de mantenimiento.

Versiones Afectadas

Los productos compatibles afectados con algunas de sus versiones son:

- 12.1.0
- 11.2.8
- 11.2.5
- 11.2.0

Ver +INFO.

Solución:

Actualizar a versiones:

- Actualizar a 12.1.4
- Actualizar a 11.2.10
- Actualizar a 11.2.7
- Actualizar a 11.2.4

Ver + INFO.

Fecha de Publicación: 14/ENE/2026 INFO

Heap-based buffer overflow in cw_acd daemon

CVE-2025-25249

High (7.4)

Impacto: Ejecución de código o comandos no autorizados

Resumen: Una vulnerabilidad de desbordamiento de búfer basado en heap (heap-based buffer overflow) [CWE-122] en el daemon cw_acd de FortiOS y FortiSwitchManager podría permitir que un atacante remoto no autenticado ejecute código o comandos arbitrarios mediante solicitudes específicamente diseñadas.

Productos Afectadas

Los productos compatibles afectados con algunas de sus versiones son:

- FortiOS 6.4.0 – 6.4.16
- FortiOS 7.4.0 – 7.4.8
- FortiSwichManager 7.0.0 – 7.0.5

Ver +INFO.

Solución:

Actualizar los productos afectados a las versiones parchadas.

Ver +INFO.

Fecha de Publicación: 13/ENE/2026 INFO

Critical buffer overflow in Net-SNMP's snmptrapd

CVE-2025-68615

Critical (9.8)

Impacto: Ejecución arbitraria de código

Resumen: En versiones anteriores, un paquete especialmente diseñado enviado al daemon snmptrapd de net-snmp puede provocar un desbordamiento de búfer y causar la caída del servicio (crash del daemon).

Versiones Afectadas

Las versiones anteriores a las siguientes se encuentran afectadas:

- Net-SNMP 5.9.5
- Net-SNMP 5.10.pre2

Ver +INFO.

Solución:

Actualizar Net-SNMP a versiones parchadas.

Ver +INFO.

Fecha de Publicación: 07/ENE/2026 INFO

Local privilege escalation in the Nessus Agent Tray application for Windows

CVE-2025-36640

Critical (8.8)

Impacto: Escalada de privilegios

Resumen: Se ha identificado una vulnerabilidad en el proceso de instalación y desinstalación de la Nessus Agent Tray App en hosts Windows, la cual podría permitir una escalada de privilegios.

Productos Afectados

Los productos compatibles afectados son:

- Nessus Agent Tray App en Windows

Ver +INFO.

Solución:

Actualizar a una de las siguientes versiones o superiores:

- Nessus Agent 10.9.3 o superior
- Nessus Agent 11.0.3 o superior

Ver +INFO.

Fecha de Publicación: 15/ENE/2026 INFO

Microsoft Security Updates

CVE-2026-0386 - CVE-2026-20803
CVE-2026-20804 - CVE-2026-20805

Microsoft lanzó parches para corregir más de 100 vulnerabilidades en una amplia gama de sus productos de software, incluyendo Windows, Office y otros componentes, estos fallos resueltos incluían vulnerabilidades críticas, de alta severidad y zero-days.

Recomendación:
Microsoft sugiere aplicar estas actualizaciones cuanto antes para proteger los sistemas contra posibles ataques.

Producto Afectado

Algunos de los productos afectados son:

- Sistemas operativos y servicios de Windows: Windows Kernel
- Aplicaciones y componentes de Microsoft: Microsoft Office

Ver +INFO

Fecha de Publicación: 13/ENE/2026 INFO

Nessus Versions 10.11.1 and 10.9.6 Fix Multiple Vulnerabilities

CVE-2025-49796 - CVE-2025-59375
CVE-2025-49794 - CVE-2024-8176

Tenable ha remediado múltiples vulnerabilidades en el producto Nessus actualizando componentes subyacentes de terceros como expat, libxml2 y libxslt, que presentaban fallos de seguridad como agotamiento de recursos, errores de lógica y otros fallos fueron abordados al actualizar estos componentes a versiones más seguras.

Recomendación:
Actualiza Tenable Nessus a las versiones 10.9.6 o 10.11.1 para corregir vulnerabilidades en componentes de terceros y proteger tu entorno.

Producto Afectado:

Los productos afectados son:

- Versiones anteriores a 10.9.6 y 10.11.1 son vulnerables debido a bibliotecas de terceros con fallos conocidos.

Ver +INFO

Fecha de Publicación: 22/DIC/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
5/01/2026	CVE-2025-54957	Android	6.7	Esta vulnerabilidad afecta al decodificador de audio Dolby UDC. Su explotación se debe a un cálculo incorrecto de la longitud para ciertas operaciones de escritura, lo que puede provocar una escritura fuera de los límites de memoria. Permite a un atacante ejecutar código arbitrario, ataques zero-click en Android, bloqueos o caídas de procesos y corrupción de memoria y escalada de ataques.
7/01/2026	CVE-2026-20026 CVE-2026-20027	Cisco	5.8	Esta vulnerabilidad afecta al motor de deteccion Snort 3 (usado en varios productos cisco). Esta relacionada con la logica de manejo de memoria al procesar solicitudes DCE/RPC, lo que causa una condicon de Uuso de memoria despues de liberarla. Poermite a un atacante realizar ataques DoS.
7/01/2026	CVE-2022-23439	Fortinet	4.1	Esta vulnerabilidad afecta a mutiles productos de Fortinet . Esta relacionada con un problema de referencia externamente controlada a recursaos en otra esfera. Permite a un atacante envenenar el cache web
13/01/2026	CVE-2025-67685	Fortinet	3.4	Esta vulnerabilidad afecta a Fortinet FortiSandbox, es un fallo de tipo Server-Side Request Forgery. Permite a un atacante realizar solicitudes internas a través del servidor vulnerable.
13/01/2026	CVE-2026-20805	Windows	5.5	Esta vulnerabilidad afecta a Microsoft Windows, específicamente al componente Desktop Windows Manager y es un error de divulgación de información.

Nueva campaña de malware instala Remcos RAT en Windows por etapas

La campaña identificada como SHADOW#REACTOR distribuye el Remcos RAT, un troyano de acceso remoto ampliamente usado para espionaje, robo de información y control total del sistema comprometido. El malware se entrega mediante una cadena de infección por múltiples etapas, diseñada para evadir soluciones de seguridad tradicionales. Inicia con un script VBS altamente ofuscado que ejecuta PowerShell para descargar cargas útiles fragmentadas. Estas piezas se reconstruyen y descifran en memoria utilizando un ensamblado .NET protegido con .NET Reactor, y finalmente se ejecuta el payload usando MSBuild.exe, una herramienta legítima de Windows, lo que dificulta su detección y análisis.

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

El ATAQUE

El ataque comienza cuando la víctima ejecuta un archivo o enlace malicioso, lo que activa un script VBS disfrazado como contenido legítimo. Este script lanza comandos PowerShell que descargan múltiples archivos de texto desde un servidor controlado por el atacante. Posteriormente, los archivos se combinan y decodifican en memoria sin escribir directamente el malware en disco. El uso de binarios confiables de Windows (living-off-the-land) permite que Remcos RAT se ejecute de forma sigilosa, establezca persistencia y se comunique con su servidor de comando y control.
El resultado es un acceso oculto y persistente al sistema víctima mediante Remcos, un paquete comercial de administración remota usado de forma maliciosa. La técnica modular, evasiva y basada en memoria facilita a los atacantes mantener el control sobre la máquina y evadir las defensas tradicionales.

INFO

CONTEXT	INDICATOR	(MD5)
IPv4	193[.]24[.]123[.]232	N/A
IPv4	91[.]202[.]233[.]215	N/A
payload_1.bin	1106b820450d0962abf503c80fda44a890e4245555b97ba7656c7329c0ea2313	6b5c843de269a8c99c390fe8e393375d
iocpbvh.exe	1fd111954e3eefeef07557345918ea6527898b741dfd9242ff4f5c2ddceaa5e9	c9070442a4f9e8b94ec8a2d99ab13b27
teste32.txt	507c97cc711818eb03cfffd3743cebb43820eeafa5c962c03840f379592d2df5	377717ee253f5e70d2a37461392494f2
win64.vbs	90d552da574192494b4280a1ee733f0c8238f5e07e80b31f4b8e028ba88ee7ea	21f1da8b05ab5f52520fc8febe1f7746
f8ygr6v.exe	985513b27391b0f9d6d0e498b5cec35df9028a5af971b943170327478d976559	75bc24315a945d4d88f1514a7a239381

ÚLTIMAS NOTICIAS

Dos extensiones maliciosas exfiltran datos de ChatGPT

Con más de 900,000 instalaciones que roban conversaciones de ChatGPT, así como el historial de navegación de los usuarios, enviando esos datos a servidores controlados por atacantes cada 30 minutos.

Estas extensiones se hacen pasar por herramientas legítimas de IA y piden permisos bajo el pretexto de “analítica anónima”, pero en realidad extraen mensajes de chat y URLs abiertas mediante la lectura del DOM y la envían a dominios remotos.

Los datos extraídos pueden usarse para espionaje corporativo, robo de identidad o campañas de phishing, se recomienda eliminar inmediatamente estas extensiones y tener cuidado incluso con aquellas que aparecen como “destacadas” en la tienda.

INFO

Falla en jsPDF permite robar datos vía PDFs

Se ha descubierto una vulnerabilidad crítica en la biblioteca jsPDF, muy popular en aplicaciones JavaScript para generar archivos PDF, que permite a un atacante leer y exfiltrar archivos sensibles del sistema local al incluirlos en los documentos PDF generados. La falla, identificada como CVE-2025-68428, es un problema de inclusión de archivos y recorrido de directorios en la función loadFile, y afecta principalmente a las versiones de jsPDF anteriores a la 4.0.0 usadas en entornos Node.js. Debido a que esta biblioteca tiene millones de descargas semanales, la falla tiene un impacto amplio y severo, y los desarrolladores deben actualizar a la versión parcheada para mitigar el riesgo de exposición de datos confidenciales como configuraciones, claves o credenciales.

INFO

Falla en Telegram permite rastrear IPs con un clic

Enlaces proxy ocultos en Telegram, que pueden parecer nombres de usuario o vínculos inofensivos, pueden revelar tu dirección IP real con un solo clic debido a cómo la app maneja la configuración de proxies. Cuando un usuario pulsa uno de estos enlaces, Telegram intenta automáticamente conectarse y validar el proxy, lo que provoca que se envíe una solicitud directa desde el dispositivo al servidor del atacante y exponga la IP del usuario incluso antes de que el proxy se active. Esto representa un riesgo de desanonimización, rastreo de ubicación aproximada y ataques dirigidos si los enlaces maliciosos se distribuyen en chats o canales. Telegram ha dicho que añadirá advertencias antes de abrir enlaces proxy para ayudar a prevenir estos engaños.

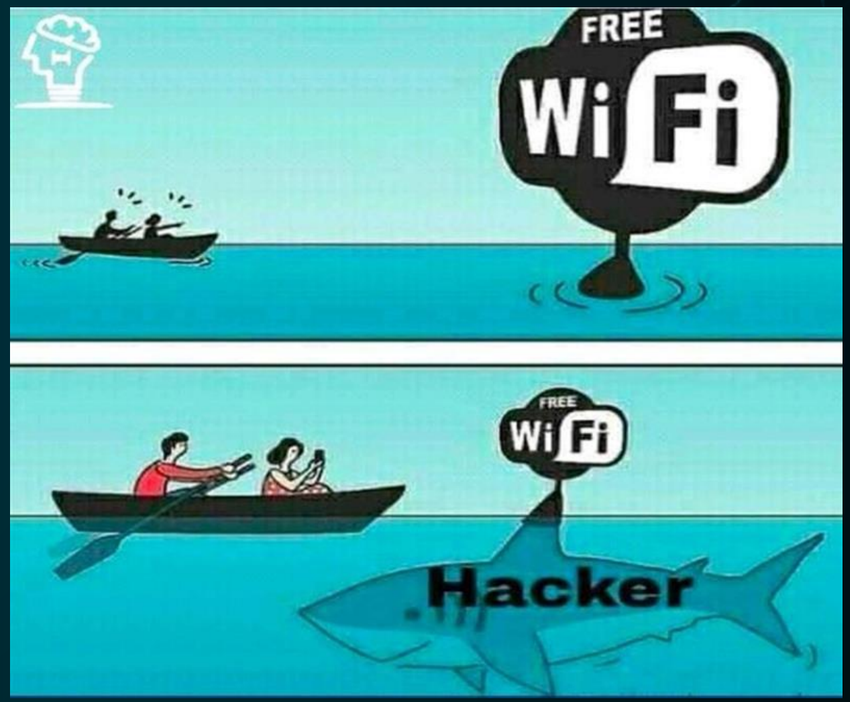
INFO

Lo gratuito no siempre es seguro

El uso de redes Wi-Fi públicas o gratuitas puede representar un riesgo para la seguridad de la información, ya que suelen ser utilizadas por atacantes para espiar el tráfico, capturar credenciales o distribuir contenido malicioso sin que el usuario lo note. A continuación, algunas recomendaciones:

📶 Desconfía del “Free Wi-Fi”: las redes abiertas pueden ser trampas diseñadas para atraer usuarios.
🔒 Evita ingresar información sensible: no accedas a correos corporativos, banca en línea o sistemas internos desde Wi-Fi público.
📡 Desactiva la conexión automática a redes Wi-Fi: evita conectarte sin darte cuenta a redes no seguras.
📱 Mantén tus dispositivos actualizados: las actualizaciones corrigen vulnerabilidades explotables en redes abiertas.

La conectividad gratuita puede parecer conveniente, pero la seguridad siempre debe ser la prioridad. Antes de conectarte a un “Free Wi-Fi”, recuerda que el tiburón 🦈 puede estar esperando.



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4