



# El Troyano PipeMagic aprovecha vulnerabilidad de día cero de Windows para desplegar Ransomware

**TLP:CLEAR**

**14.04.2025**

CLICK PARA  
EMPEZAR







En esta edición: →

El troyano PipeMagic aprovecha la vulnerabilidad de día cero de Windows para desplegar ransomware

# CONTENIDO



-  **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 Enterprise Chat and Email Denial of Service Vulnerability

CVE-2025-20139



High (7.5)

**Impacto:** Escalada de privilegios.

**Resumen:** Esta vulnerabilidad se debe a una validación incorrecta de la entrada proporcionada por el usuario a los puntos de entrada del chat. Un atacante remoto no autenticado podría explotarla enviando solicitudes maliciosas, lo que provocaría que la aplicación deje de responder y genere una condición de denegación de servicio (DoS), requiriendo posiblemente la intervención manual para restablecer los servicios.

#### Versiones Afectadas

Cisco ECE si la función de chat está habilitada y se ha configurado un punto de entrada.

**Solución:** Cisco ha lanzado actualizaciones de software gratuitas que corrigen la vulnerabilidad descrita en este aviso. [Ver +INFO.](#)



### Cisco Meraki MX and Z Series AnyConnect VPN Denial of Service Vulnerability

CVE-2025-20212



High (7.7)

**Impacto:** Escalada de privilegios.

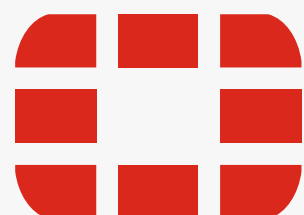
**Resumen:** Una vulnerabilidad en el servidor VPN Cisco AnyConnect de los dispositivos Cisco Meraki MX y Cisco Meraki Z Series podría permitir que un atacante remoto autenticado cause una condición de denegación de servicio (DoS) en el servicio Cisco AnyConnect en un dispositivo afectado.

#### Versiones Afectadas

- MX64
- MX64W
- MX65
- MX65W
- MX67
- Entre Otras

**Solución:** Cisco ha lanzado actualizaciones de software gratuitas que corrigen la vulnerabilidad descrita en este aviso.

[Ver +INFO.](#)



### Unverified password change via set\_password endpoint

CVE-2024-48887



Critical  
(9.3)

**Impacto:** Escalada de privilegios.

**Resumen:** Una vulnerabilidad de cambio de contraseña no verificada [CWE-620] en la GUI de FortiSwitch puede permitir que un atacante remoto no autenticado modifique las contraseñas de administrador a través de una solicitud especialmente diseñada.

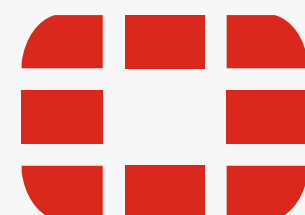
#### Versiones Afectadas

- FortiSwitch 7.6.0
- FortiSwitch 7.4.0 a 7.4.4
- FortiSwitch 7.2.0 a 7.2.8
- FortiSwitch 7.0.0 a 7.0.10
- FortiSwitch 6.4.0 a 6.4.14

#### Solución:

- Actualización a 7.6.1 o superior
- Actualización a 7.4.5 o superior
- Actualización a 7.2.9 o superior
- Actualización a 7.0.11 o superior
- Actualización a la versión 6.4.15 o superior

Ver [+INFO.](#)



### No certificate name verification for fgfm connection

CVE-2024-26013



High  
(7.1)

**Impacto:** Control de acceso inadecuado.

**Resumen:** Una restricción incorrecta del canal de comunicación a la vulnerabilidad de puntos finales previstos [CWE-923] en FortiOS, FortiProxy, FortiManager, FortiAnalyzer, FortiVoice y FortiWeb puede permitir que un atacante no autenticado en una posición de intermediario (MITM) se haga pasar por el dispositivo de administración (FortiCloud o, en ciertos casos, FortiManager), interceptando la solicitud de autenticación FGFM.

#### Versiones Afectadas

- FortiAnalyzer 7.4.0 a 7.4.2
- FortiAnalyzer 7.2.0 a 7.2.2
- FortiAnalyzer 7.0.0 a 7.0.11
- FortiAnalyzer 6.4.0 a 6.4.14

#### Solución:

- Actualización a 7.4.3 o superior
- Actualización a 7.2.5 o superior
- Actualización a 7.0.12 o superior
- Actualización a la versión 6.4.15 o superior

Ver [+INFO.](#)



### VMware Aria Operations updates address a local privilege escalation vulnerability

**CVE-2025-22231**



**High (7.8)**

**Impacto:** Escalada de privilegios.

**Resumen:** Una vulnerabilidad de escalamiento de privilegios locales en VMware Aria Operations podría permitir que un actor malicioso con privilegios administrativos locales eleve sus privilegios a nivel root en el appliance afectado.

#### Versiones Afectadas

- Operaciones de VMware Aria
- VMware Cloud Foundation
- Plataforma de nube de telecomunicaciones de VMware
- Infraestructura de nube de VMware Telco

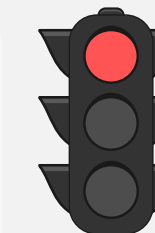
**Solución:** Se recomienda actualizar a las últimas versiones.

[Ver +INFO.](#)



### Remote Code Execution Vulnerability with Query Tool and Cloud Deployment

**CVE-2025-2945**



**Critical (9.9)**

**Impacto:** Ejecución de código arbitrario.

**Resumen:** Vulnerabilidad de seguridad de ejecución remota de código (Remote Code Execution, RCE) en pgAdmin 4, específicamente en los módulos Query Tool y Cloud Deployment. La falla se debe al uso inseguro de parámetros que son enviados a la función eval() de Python, permitiendo la ejecución arbitraria de código. Esta vulnerabilidad afecta a las versiones de pgAdmin 4 anteriores a la 9.2.

#### Versiones Afectadas

Este problema afecta a pgAdmin 4 antes de la versión 9.2.

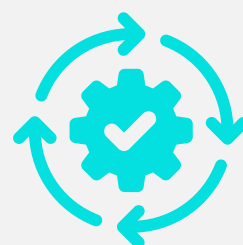
**Solución:** Se recomienda actualizar a una versión superior a la 9.2.

[Ver +INFO.](#)



## Actualización de Seguridad para productos Apple

**CVE-2025-24201, CVE-2025-24085, CVE-2025-24200**



Apple ha lanzado actualizaciones de seguridad para abordar múltiples vulnerabilidades que afectan sus productos. Algunas de estas vulnerabilidades podrían permitir la denegación de servicio, elevación de privilegios, ejecución remota de código, divulgación de información confidencial.

### Recomendación:

Actualizar a las últimas versiones disponibles de los productos afectado desde la página web oficial.

### Productos afectados

- Safari, versiones anteriores a la 18.4.
- Xcode, versiones anteriores a la 16.3.
- iOS, versiones anteriores a: 15.8.4, 16.7.11 y 18.4
- iPadOS, versiones anteriores a: 15.8.4, 16.7.11 y 18.4
- macOS Sequoia, versiones anteriores a 15.4.

Fecha de Publicación: 1/ABR/2025



## Actualización de Seguridad para Google Chrome

**CVE-2025-3067, CVE-2025-3068, CVE-2025-3069, CVE-2025-3070, CVE-2025-3071, CVE-2025-3072, CVE-2025-3073, CVE-2025-3074**



Recientemente, Google ha publicado una actualización de seguridad con el objetivo de corregir múltiples vulnerabilidades identificadas en sus productos. Estas fallas podrían ser aprovechadas por actores maliciosos para comprometer la integridad, confidencialidad o disponibilidad de los sistemas afectados.

### Recomendación:

Actualizar Chrome a 135.0.7049.52 en Linux

Actualizar Chrome 135.0.7049.41/42 en Windows y Mac.

### Versiones Afectadas

- Actualizar Google Chrome a la versión más reciente disponible para asegurar la protección contra vulnerabilidades conocidas.
- Habilitar las actualizaciones automáticas en Google Chrome para recibir correcciones de seguridad de manera oportuna.

Fecha de Publicación: 1/ABR/2025



## LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
5/04/2025	<a href="#">CVE-2025-30401</a>	Whatsapp	6.7	Un problema de suplantación de identidad en WhatsApp para Windows anterior a la versión 2.2450.6 mostraba los archivos adjuntos según su tipo MIME, pero seleccionaba el controlador de apertura de archivos en función de la extensión del nombre de archivo del archivo adjunto.
2/04/2025	<a href="#">CVE-2024-53868</a>	Apache server	7.5	Esta vulnerabilidad afecta a ATS y permite a un atacante aprovechar la forma en que maneja los mensajes con codificación de transferencia en fragmentos (chunked encoding). Mediante esta explotación, un atacante puede inyectar solicitudes maliciosas que evaden controles de seguridad, manipulan la caché del servidor o incluso secuestran sesiones de usuarios.
1/04/2025	<a href="#">CVE-2025-30065</a>	Apache	10	El análisis de esquemas en el módulo parquet-avro de Apache Parquet 1.15.0 y versiones anteriores permite a los malos actores ejecutar código arbitrario. Se recomienda a los usuarios que actualicen a la versión 1.15.1, que soluciona el problema.
8/04/2025	<a href="#">CVE-2024-52962</a>	Fortinet	5.0	Una vulnerabilidad de neutralización de salida incorrecta para registros [CWE-117] en FortiManager y FortiAnalyzer puede permitir que un atacante remoto no autenticado contamine los registros a través de solicitudes de inicio de sesión diseñadas.
1/04/2025	<a href="#">CVE-2025-3066</a>	Chrome	8.8	El uso gratuito en el aislamiento del sitio en Google Chrome antes de 135.0.7049.84 permitía a un atacante remoto explotar potencialmente la corrupción del montón a través de una página HTML diseñada. (Gravedad de seguridad de Chromium: Alta)
3/04/2025	<a href="#">CVE-2025-22004</a>	Linux	7.8	En el kernel de Linux, se ha resuelto la siguiente vulnerabilidad: net: atm: arreglar el uso después de libre en lec_send() La operación ->send() libera skb, así que guarde la longitud antes de llamar a ->send() para evitar un uso después de libre.
3/04/2025	<a href="#">CVE-2025-25000</a>	Microsoft Edge	8.8	El acceso al recurso mediante un tipo incompatible ('confusión de tipos') en Microsoft Edge (basado en Chromium) permite a un atacante no autorizado ejecutar código a través de una red.
3/04/2025	<a href="#">CVE-2024-4877</a>	OpenVPN	8.8	OpenVPN versión 2.4.0 a 2.6.10 en Windows permite que un proceso externo con menos privilegios cree una tubería con nombre a la que se conectaría el componente GUI de OpenVPN, lo que le permitiría escalar sus privilegios.



## El Troyano PipeMagic aprovecha vulnerabilidad de 0-day de Windows para desplegar Ransomware

Microsoft ha revelado que una falla de seguridad ahora parcheada que afecta al Sistema de Archivos de Registro Común de Windows (CLFS) fue explotada como un día cero en ataques de ransomware dirigidos a un pequeño número de objetivos.

"Los objetivos incluyen organizaciones en los sectores de tecnología de la información (TI) y bienes raíces de los Estados Unidos, el sector financiero en Venezuela, una empresa española de software y el sector minorista en Arabia Saudita", dijo el gigante tecnológico.

Microsoft está rastreando la actividad y la explotación posterior al compromiso de CVE-2025-29824 bajo el apodo Storm-2460, y los actores de amenazas también aprovechan un malware llamado PipeMagic para entregar el exploit, así como las cargas útiles de ransomware.

A continuación, compartimos los IoC para ser agregados a las herramientas de seguridad perimetral. [Ver +INFO.](#)

### EL ATAQUE

El ataque comienza con la explotación de la vulnerabilidad CVE-2025-29824 en CLFS, lo que permite a los atacantes obtener privilegios elevados en el sistema. Una vez dentro, utilizan el troyano PipeMagic, que se despliega a través de un archivo MSBuild malicioso que contiene una carga útil cifrada. Al ejecutarse, PipeMagic establece una puerta trasera en el sistema, permitiendo el acceso remoto completo y la extracción de datos sensibles. Además, PipeMagic facilita la instalación de complementos adicionales y el lanzamiento de ataques adicionales en la red corporativa. Este malware emplea técnicas como la creación de pipes con nombres aleatorios para recibir cargas útiles codificadas y señales de control, operando en conjunto con servidores de comando y control alojados en plataformas como Microsoft Azure.



CONTEXT	INDICATOR	(MD5)
kernel32_dll_xor_exe_key_90	18663fccb742c594f30706078c5c1c27351c44df0c7481486aaa9869d7fa95f8	0c158a5076aa8580e1d9c3ad29494e7e
HackTool:Win64/Mikatz!dha	ef7cc405b55f8a86469e6ae32aa59f693e1d243f1207a07912cce299b66ade38	2d9cb4e97ecb8029c71c26da729f0b27
SLFPER:KPAT:Cobalt.shell	a4eebe193e726bb8cc2ffbdf345ffde09ab61d69a131aff6dc857b0d01dd3213	c9fd2694522b846ccb74beac66c1366f
URL	http://makeonlineform[.]com/f/c3ad6a62-6a0e-4582-ba5e-9ea973c85540	N/A
domain	Makeonlineform[.]com	N/A
SLFPER:KPAT:Cobalt.shell	a4eebe193e726bb8cc2ffbdf345ffde09ab61d69a131aff6dc857b0d01dd3213	c9fd2694522b846ccb74beac66c1366f
kernel32_dll_xor_exe_key_90	18663fccb742c594f30706078c5c1c27351c44df0c7481486aaa9869d7fa95f8	0c158a5076aa8580e1d9c3ad29494e7e
VirTool:MSIL/Covenant.C	ee34c2fccc7e605487ff8bee2a404bc9fc17b66d4349ea3f93273ef9c5d20d94	daf2068b535b89c076d2799f06ef4bba
HackTool:Win64/Mikatz!dha	ef7cc405b55f8a86469e6ae32aa59f693e1d243f1207a07912cce299b66ade38	2d9cb4e97ecb8029c71c26da729f0b27







**+ INFO**



## ¡Evita el caos! Prueba antes de aplicar cambios

Realizar cambios de configuración directamente en producción puede traer consecuencias serias: caídas del sistema, errores inesperados o afectación a los usuarios. Por eso, es clave probar siempre en un ambiente de pruebas antes de implementar.

Recomendaciones clave:

-  Usa ambientes de prueba: Simulan el entorno real sin afectar a los usuarios. Ideal para detectar errores antes de que lleguen a producción.
-  Haz cambios en horarios de baja demanda: Si no hay ambiente de pruebas, al menos hazlo cuando el impacto sea mínimo.
-  Prepara un plan de rollback: Siempre ten una forma rápida de revertir cambios si algo sale mal.
-  Cuida la seguridad: Verifica que las nuevas configuraciones no generen brechas ni debiliten el sistema.

Una prueba a tiempo puede prevenir muchos problemas. ¡La estabilidad del sistema empieza con buenas prácticas!





 [csirt\\_datasec@datasec.com.co](mailto:csirt_datasec@datasec.com.co)

 +57 310 285 8969

