

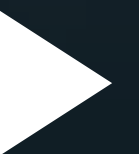


Medusa emplea certificados robados para desactivar antimalware

TLP:CLEAR

01.04.2025

CLICK PARA
EMPEZAR







En esta edición: →

Medusa emplea certificados robados para desactivar antimalware

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.



AIX is vulnerable to arbitrary command execution

CVE-2024-56346



Critical
(10)

Impacto: Ejecutar código o comandos no autorizados.

Resumen: El servicio maestro NIM nimesis de IBM AIX podría permitir a un atacante remoto ejecutar comandos arbitrarios debido a controles de proceso incorrectos.

Versiones Afectadas

- AIX 7.2
- AIX 7.3

Solución: Se recomienda aplicar las actualizaciones de seguridad mas recientes.
[Ver +INFO.](#)



IBM InfoSphere Information Server is vulnerable due to the improper handling of permissions

CVE-2024-51459



High
(8.4)

Impacto: Ejecutar código o comandos no autorizados

Resumen: IBM InfoSphere Information podía permitir a un usuario local ejecutar comandos privilegiados debido a la gestión incorrecta de permisos.

Versiones Afectadas

InfoSphere Information Server
11.7

Solución: Actualice el instalador de IBM InfoSphere Information Server Update a la versión 11.7.1.136 o posterior

[Ver +INFO.](#)



Incorrect handle could lead to sandbox escapes

CVE-2025-2857



**Critical
(10)**

Impacto: Ejecutar código o comandos no autorizados.

Resumen: Esta vulnerabilidad podría permitir a un actor malicioso evadir entornos de pruebas del navegador en sistemas Windows, lo que permitiría la ejecución de un código arbitrario.

Versiones Afectadas

- Mozilla, versiones anteriores a la 136.0.4
- Mozilla para Windows, versiones anteriores a 115.21.1
- Mozilla para Windows, versiones anteriores a 128.8.1.

Solución: Actualizar a la última versión disponible de los productos afectados desde la página web oficial del fabricante, para mitigar el riesgo asociado a esta vulnerabilidad.

Ver [+INFO.](#)



Vulnerabilidad en Google Chrome

CVE-2025-2783



**High
(8.3)**

Impacto: Escalada de privilegios.

Resumen: Esta vulnerabilidad en Google Chrome para Windows podría permitir a algún actor malicioso remoto escapar de la zona protegida mediante un archivo malicioso, comprometiendo la seguridad e integridad de los datos del usuario.

Versiones Afectadas

Versiones anteriores a la 134.0.6998.177/.178 para Windows.

Solución: Actualizar los productos afectados a la última versión más reciente disponible desde la web oficial del fabricante.

Ver [+INFO.](#)



Tenable Nessus Agent Vulnerability

CVE-2025-24915



High
(7.8)

Impacto: Elevación de privilegios local.

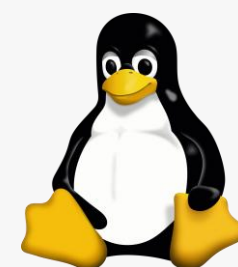
Resumen: Una vulnerabilidad de permisos incorrectos en Nessus Agent, presente en versiones anteriores a la 10.8.3, podría permitir la escalación de privilegios locales en sistemas Windows. Esto sucede cuando el agente se instala en una ubicación no predeterminada sin aplicar permisos seguros a los subdirectorios, lo que podría ser aprovechado por usuarios con acceso al sistema.

Versiones Afectadas

Versiones de Nessus Agent anteriores a la 10.8.3

Solución: Se recomienda realizar actualización a 10.8.3 o superior.

Ver [+INFO](#).



Linux Distros Unpatched Vulnerability

CVE-2025-0927



High
(7.8)

Impacto: Denegación de servicios.

Resumen: Attila Szász descubrió que la implementación del sistema de archivos HFS+ en el kernel de Linux contenía una vulnerabilidad de heap overflow. Un atacante podría usar una imagen del sistema de archivos especialmente diseñada que, al montarse, podría causar una denegación de servicio (fallo del sistema) o incluso ejecutar código arbitrario.

Versiones Afectadas

- 24.10 Oracular
- 24.04 LTS noble
- 22.04 Mermelada LTS
- 20.04 Enfoque LTS
- 18.04 LTS biónico

Ver [+INFO](#).

Solución:

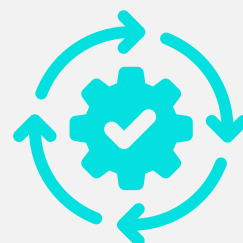
Se recomienda actualizar a las versiones corregidas.

- Oracular 6.11.0-18.18.
- LTS noble 6.8.0-54.56
- Mermelada LTS 5.15.0-133.144
- Enfoque LTS 5.4.0-208.228
- LTS biónico 4.15.0-234.246



Actualización de seguridad en productos CISCO

CVE-2024-20430, CVE-2024-20440, CVE-2024-20439



CISCO ha lanzado actualizaciones de seguridad que abordan múltiples vulnerabilidades de gravedad «alta» y «crítica» encontradas en varios productos.

Recomendación:

Aplicar las mitigaciones disponibles siguiendo las instrucciones de cada vulnerabilidad.

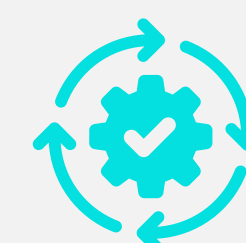
Productos afectados

- Utilidad de licencias inteligentes de Cisco
- Agente de Cisco Meraki Systems Manager (SM) para Windows



Actualización de Seguridad para Google Chrome

CVE-2025-2476



Google ha lanzado una actualización para su navegador Chrome, corrigiendo dos nuevas vulnerabilidades de seguridad, de las cuales dos son clasificadas como de severidad crítica.

Recomendación:

Actualizar los productos afectados en Windows, Mac y Linux a la última versión disponible desde la web oficial del fabricante.

Versiones Afectadas

- Versiones anteriores a 134.0.6998.117/118 para Windows y Mac.
- Versiones anteriores a 134.0.6998.117 para Linux.

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
25/03/2025	CVE-2025-22230	Vmware	7.8	VMware Tools para Windows contiene una vulnerabilidad de omisión de autenticación debido a un control de acceso inadecuado. VMware ha evaluado la gravedad de este problema en el rango de gravedad Importante con una puntuación base CVSSv3 máxima de 7,8.
4/03/2025	CVE-2025-22224	Vmware	9.3	VMware ESXi, y Workstation contienen una vulnerabilidad TOCTOU (Time-of-Check Time-of-Use) que conduce a una escritura fuera de límites. Un actor malicioso con privilegios administrativos locales en una máquina virtual puede explotar este problema para ejecutar código como proceso VMX de la máquina virtual que se ejecuta en el host.
28/03/2025	CVE-2024-20475	CISCO	6.4	Una vulnerabilidad en la interfaz de gestión basada en web de Cisco Catalyst SD-WAN Manager, anteriormente Cisco SD-WAN vManage, podría permitir a un atacante remoto autenticado realizar un ataque de secuencias de comandos en sitios cruzados (XSS) contra un usuario de la interfaz.
11/03/2025	CVE-2024-54018	Fortinet	4.1	Una neutralización inadecuada de elementos especiales utilizados en un comando SQL ('SQL Injection') vulnerabilidad [CWE-89] en FortiSandbox puede permitir a un atacante privilegiado ejecutar código no autorizado o comandos a través de peticiones HTTP específicamente diseñados.
11/03/2025	CVE-2024-52960	Fortinet	4.2	Una vulnerabilidad [CWE-602] en FortiSandbox puede permitir a un atacante autenticado con al menos permiso de sólo lectura ejecutar comandos no autorizados a través de peticiones falsificadas.
11/03/2025	CVE-2024-33501	Fortinet	4.0	La vulnerabilidad [CWE-89] en FortiAnalyzer, FortiManager y FortiAnalyzer-BigData puede permitir a un atacante con privilegios ejecutar código o comandos no autorizados a través de peticiones CLI específicamente diseñadas.
24/03/2025	CVE-2024-44305	Apple	7.8	Una aplicación puede obtener privilegios de root. Este problema se ha solucionado en macOS Sonoma 14.6.
17/03/2025	CVE-2025-2241	Red Hat	8.2	Se detectó una falla en Hive, un componente de Multicluster Engine (MCE) y Advanced Cluster Management (ACM). Esta vulnerabilidad provoca la exposición de las credenciales de VCenter en el objeto ClusterProvision tras aprovisionar un clúster de VSphere. Los usuarios con acceso de lectura a los objetos ClusterProvision pueden extraer credenciales confidenciales incluso sin acceso directo a los secretos de Kubernetes. Este problema puede provocar acceso no autorizado a VCenter, la gestión del clúster y la escalada de privilegios.



Medusa desactiva antimalware con un controlador malicioso y certificados robados

El ransomware Medusa ha sido detectado utilizando el controlador malicioso ABYSSWORKER en ataques del tipo BYOVD para desactivar herramientas de seguridad. Elastic Security Labs identificó que el cifrador fue entregado mediante un cargador empaquetado con HeartCrypt, acompañado de un controlador firmado con un certificado revocado de un proveedor chino. ABYSSWORKER, identificado en VirusTotal desde agosto de 2024, imita un controlador legítimo de CrowdStrike Falcon y está firmado con certificados robados. Su capacidad para evadir sistemas de seguridad y desactivar soluciones EDR ha sido documentada previamente. Al ejecutarse, añade procesos a una lista protegida y procesa solicitudes de control de I/O, permitiendo manipulación de archivos, terminación de procesos y desactivación de sistemas de defensa.

EL ATAQUE

Los atacantes pueden explotar el código de control de I/O 0x222400 para desactivar productos de seguridad eliminando devoluciones de llamada de notificación, una técnica utilizada en herramientas como EDRSandBlast y RealBlindingEDR. Venak Security reportó el abuso de un controlador vulnerable de ZoneAlarm en ataques BYOVD para obtener privilegios elevados y desactivar medidas de seguridad en Windows. Además, se detectó que RansomHub emplea el backdoor Betruger, con funciones avanzadas como keylogging, captura de pantalla, escalamiento de privilegios y exfiltración de datos, lo que indica una evolución en las tácticas de ransomware. A continuación, compartimos los IoC para ser agregados a las herramientas de seguridad perimetral.

CONTEXT	INDICATOR	(MD5)
PEXE - PE32+ executable	6a2a0f9c56ee9bf7b62e1d4e1929d13046cd78a93d8c607fe4728cc5b1e8d050	988d7cdc386b2731acc86bbc883e5f31
PEXE - PE32+ executable	b7703a59c39a0d2f7ef6422945aaeaaf061431af0533557246397551b8eed505	9e82ee5bde6b5d29281a3c280e6d1f2e
PEXE - PE32+ executable	baa980ae253101066ae7e551a354116454e8697ff2154a907c9885770cdae4ae	80d852cd199ac923205b61658a9ec5bc
PEXE - PE32+ executable	9d5616672189557f171cae0f122853f3498bc9160ee92f3844404d46ec45210a	040262368513b862a2bf6fe49c55b075
PEXE - PE32+ executable	276024580b5bc903656a1c12a7ec02daccb10e6e6bdf6872765c9a67f1cd6da5	0f707f120bcb5a73c1c78b443db78230
PEXE - PE32+ executable	6106d1ce671b92d522144fcd3bc01276a975fe5d5b0fde09ca1cca16d09b7143	8f86e05716f5b2bae87704ec7e75bfc3
PEXE - PE32+ executable	8dff18f10c857dd3eeb5511f5724da0ab1d9e411044aea27f6de23ee33f798c8	b73234f07c36e68092239408a956acda
PEXE - PE32+ executable	3770c122f3f289cea730a5d1d16978e7f354686d3d2d4f667cfd9e37d5e9d368	1182110ac0e80608fe0c660ba009e2dd
PEXE - PE32+ executable	6a2a0f9c56ee9bf7b62e1d4e1929d13046cd78a93d8c607fe4728cc5b1e8d050	988d7cdc386b2731acc86bbc883e5f31



+ INFO



Riesgos de Seguridad al Convertir Fotos en Dibujos Animados

Convertir fotos en dibujos animados puede parecer divertido, pero puede comprometer tu seguridad digital. Antes de usar estas aplicaciones, considera los siguientes riesgos:

- ◆ **Exposición a hackeos:** Muchas apps almacenan tus fotos en servidores que podrían ser vulnerables a ataques.
 - ◆ **Falta de eliminación permanente:** Aunque borres una imagen, no hay garantía de que desaparezca por completo de sus sistemas.
 - ◆ **Venta de datos personales:** Algunas plataformas pueden compartir o vender tu información a terceros sin tu consentimiento.
 - ◆ **Riesgo de fraude e identidad falsa:** Los ciberdelincuentes pueden usar tus imágenes para crear perfiles falsos y cometer fraudes en línea.
- ✓ Antes de usar estas aplicaciones, revisa sus políticas de privacidad y seguridad. Protege tu información y evita riesgos innecesarios.





 csirt_datasec@datasec.com.co

 +57 310 285 8969

