BOLETÍN CIBERSEGURIDAD

CSIRT - DATASEC

DataSec

Ransomware Interlock explota falla crítica en Firewall Cisco

TLP:CLEAR

30.03.2026

CLICK PARA EMPEZAR

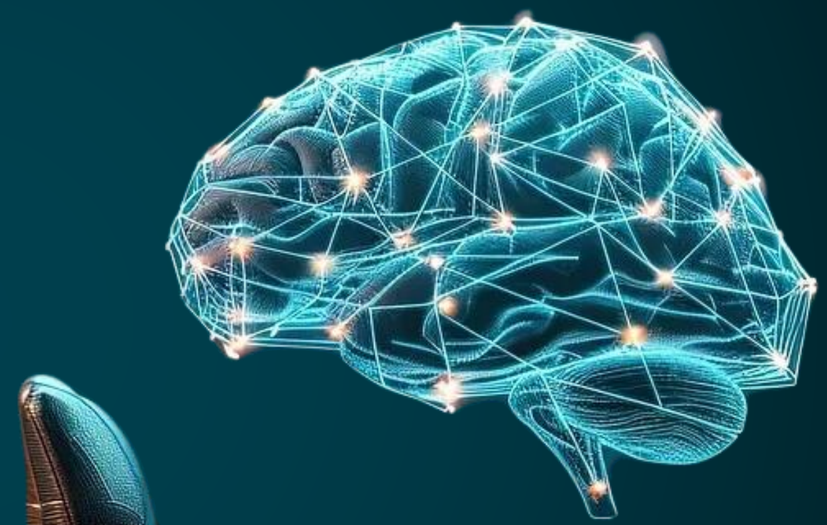
CYBERSOCDTS

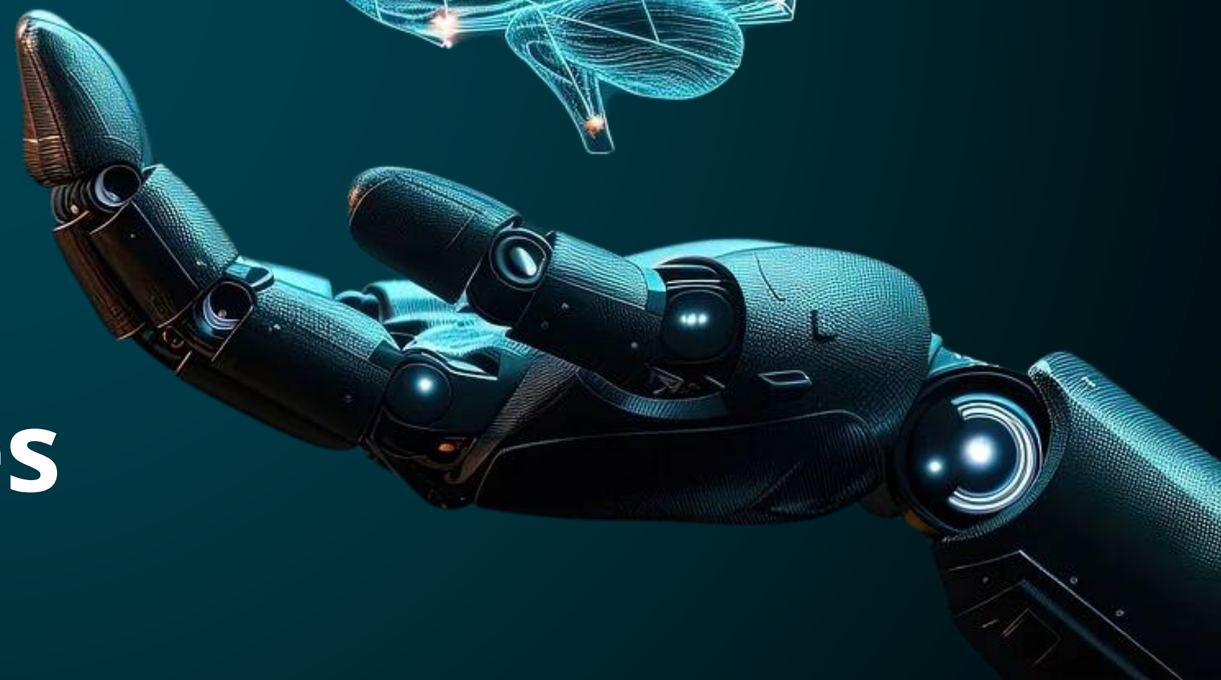
En esta edición: ⟶ Ransomware Interlock explota falla crítica en cortafuegos Cisco

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.

Deserialization of untrusted data in administrative interface

CVE-2026-20131

Critical (10.0)

Impacto: Ejecución remota de código

Resumen: Una vulnerabilidad de deserialización insegura ("Insecure Deserialization") [CWE-502] en la interfaz de administración web de Cisco Secure Firewall Management Center (FMC), causada por el manejo inseguro de flujos de bytes de Java proporcionados por el usuario, podría permitir a un atacante no autenticado ejecutar código Java arbitrario con privilegios de root mediante el envío de objetos serializados especialmente diseñados a través de solicitudes HTTP.

Producto Afectado

Producto compatible afectado:

- Cisco Secure Firewall Management Center (FMC) (múltiples versiones).

Ver +INFO.

Solución:

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

Ver + INFO.

Fecha de Publicación: 25/MAR/2026 INFO

Azure Cloud Shell Elevation of Privilege Vulnerability

CVE-2026-32169

Critical (10.0)

Impacto: Escalada de privilegios

Resumen: Una vulnerabilidad de Server-Side Request Forgery ("SSRF") [CWE-918] en Azure Cloud Shell, causada por la validación inadecuada de solicitudes realizadas por el servidor, podría permitir a un atacante no autenticado enviar solicitudes HTTP especialmente diseñadas para obtener acceso a recursos internos y elevar privilegios dentro del entorno afectado.

Producto Afectado

Producto compatible afectado:

- Microsoft Azure Cloud Shell

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Microsoft a través del Security Update Guide.

Ver +INFO.

Fecha de Publicación: 19/MAR/2026 INFO

Deserialization of untrusted data in SharePoint

CVE-2026-20963

High (8.8)

Impacto: Ejecución remota de código

Resumen: Una vulnerabilidad de deserialización insegura ("Insecure Deserialization") [CWE-502] en Microsoft Office SharePoint, causada por el manejo inadecuado de datos no confiables durante procesos de deserialización, podría permitir a un atacante autenticado con bajos privilegios ejecutar código arbitrario sobre la red sin interacción del usuario.

Producto Afectado

Producto compatible afectado:

- Microsoft SharePoint Server 2016, 2019 y Subscription Edition (versiones anteriores a 16.0.19127.20442).

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Microsoft que corrigen la vulnerabilidad en versiones posteriores del producto.

Ver +INFO.

Fecha de Publicación: 17/MAR/2026 INFO

Improper input validation in Linux kernel filesystem

CVE-2026-4148

High (8.8)

Impacto: Denegación de servicio

Resumen: Una vulnerabilidad en el kernel de Linux, específicamente en la función block_invalidatepage del subsistema de archivos, causada por la falta de validación adecuada de condiciones internas, podría permitir a un atacante local con privilegios de usuario provocar una condición de denegación de servicio mediante el envío de entradas especialmente manipuladas.

Producto Afectado

Producto compatible afectado:

- Linux Kernel (afecta a ciertas versiones utilizadas en Ubuntu, incluyendo Ubuntu 20.04 LTS).

Ver +INFO.

Solución:

Aplicar actualizaciones del kernel proporcionadas por Ubuntu; las versiones más recientes ya incluyen correcciones para esta vulnerabilidad

Ver +INFO.

Fecha de Publicación: 25/MAR/206 INFO

Google Chrome Release

CVE-2026-3909 – CVE-2026-3910

Google ha publicado una actualización de seguridad para el navegador Chrome con el fin de corregir múltiples vulnerabilidades, incluidas dos fallas zero-day de alta severidad que están siendo explotadas activamente. Las vulnerabilidades incluyen errores de escritura fuera de límites, fallas críticas en componentes como WebML, Web Speech. Estas podrían permitir corrupción de memoria, ejecución de código arbitrario, denegación de servicio.

Recomendación:

Actualizar el navegador Google Chrome a la versión más reciente de forma inmediata

Productos Afectados

Los productos afectados son:

- Google Chrome versiones anteriores a 146.0.7680.75/76 (Windows y macOS), versiones anteriores a 146.0.7680.75 (Linux), para Android versiones anteriores a 146.0.76380.115

Ver +INFO

Fecha de Publicación: 26/MAR/2026

Mozilla Firefox Release

CVE-2026-3845 – CVE-2026-3847

Mozilla ha publicado una actualización de seguridad para Firefox con el fin de corregir múltiples vulnerabilidades de alta severidad que afectan distintos componentes del navegador. Las vulnerabilidades incluyen Desbordamiento de búfer en heap, errores de seguridad de memoria. La explotación de estas vulnerabilidades podría permitir corrupción de memoria, ejecución de código arbitrario, acceso indebido a información o recursos restringidos.

Recomendación:

Actualizar Firefox a la versión más reciente disponible de forma inmediata

Productos Afectados:

Los productos afectados son:

- Mozilla Firefox versiones anteriores a 148.0.2

Ver +INFO

Fecha de Publicación: 24/MAR/2026

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
18/03/2026	CVE-2026-4111	Microsoft	7.5	Permite que un atacante remoto explote una falla en la lógica de descompresión de archivos RAR5 en la librería libarchive, enviando archivos especialmente diseñados que provocan un bucle infinito en el proceso de descompresión, lo que consume continuamente recursos de CPU y puede generar una denegación de servicio (DoS) en aplicaciones que utilizan este componente.
25/03/2026	CVE-2026-3888	Ubuntu	7.8	Permite que un atacante local sin privilegios en Ubuntu Desktop (snapd) aproveche una falla en cómo se limpia y recrea el directorio privado de snap para escalar sus privilegios hasta obtener acceso completo como root en el sistema, reconfigurando el comportamiento de componentes como snap-confine y systemd-tmpfiles para ejecutar código con privilegios elevados.
26/03/2026	CVE-2026-25836	Fortinet	6.7	Permite que un atacante con perfil super-administrador y acceso al CLI aproveche una falla de inyección de comandos del sistema operativo en Fortinet FortiSandbox Cloud para enviar solicitudes HTTP especialmente diseñadas que ejecutan código o comandos no autorizados en el producto, pudiendo comprometer completamente su funcionamiento y la confidencialidad, integridad y disponibilidad de la plataforma.
24/03/2026	CVE-2026-4433	Tenable	5.4	Permite que un atacante remoto sin autenticación explote una falla en FreeRDP para provocar un comportamiento inesperado o impacto en disponibilidad, como interrupción del servicio o ejecución de operaciones no deseadas al enviar datos especialmente diseñados al servicio afectado, afectando la estabilidad y seguridad de la plataforma.
23/03/2026	CVE-2026-4056	Wordpress	5.4	Permite que un atacante autenticado con permisos de nivel Contributor explote una falta de verificación de capacidades en el plugin User Registration & Membership para WordPress. La ausencia de una comprobación adecuada permite al atacante listar, crear, modificar, duplicar o eliminar reglas de restricción de contenido en el sitio, lo que puede exponer contenido restringido o alterar el acceso legítimo, aunque no obtenga privilegios de administrador completos.

Ransomware Interlock explota falla crítica en cortafuegos Cisco

El grupo de ransomware Interlock está explotando una vulnerabilidad crítica en los cortafuegos empresariales de Cisco (CVE-2026-20131) para ejecutar ataques dirigidos. La falla afecta al Cisco Secure Firewall Management Center (FMC) y permite a atacantes remotos ejecutar código Java con privilegios de root sin autenticación.

El equipo de inteligencia de Amazon Web Services (AWS) detectó la actividad maliciosa y localizó la infraestructura usada por Interlock. La campaña utiliza backdoors, scripts de reconocimiento y técnicas de evasión para mantener el control sobre los sistemas comprometidos.

Interlock es un grupo de ransomware financiero conocido por ataques de doble extorsión, cifrando datos y robándolos para presionar a las víctimas a pagar.

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

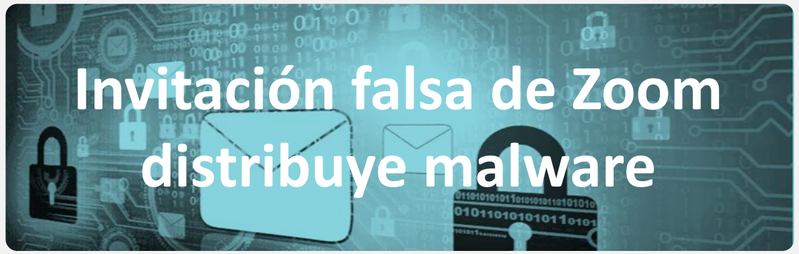
El ATAQUE

El ataque permite ejecutar código Java arbitrario con privilegios de root sin autenticación previa, simplemente enviando un objeto Java manipulado al panel web del FMC. Logrando comprometer sistemas antes de que muchas organizaciones pudieran aplicar la corrección. Una vez que Interlock obtiene acceso inicial, utiliza una cadena de herramientas sofisticadas: scripts de reconocimiento del sistema, troyanos de acceso remoto (backdoors), métodos de evasión para evitar detección y técnicas de persistencia que mantienen el control del dispositivo comprometido. La detección del ataque fue posible gracias a los sistemas de honeypots de Amazon, que revelaron la infraestructura operativa completa de Interlock. Esto permitió observar cómo el grupo prepara, ejecuta y mantiene sus ataques aprovechando la vulnerabilidad no parcheada antes de la divulgación pública.

+ INFO

CONTEXT	INDICATOR	(MD5)
IPv4	144[.]172[.]94[.]59	N/A
Certify.exe	d1caa376cb45b6a1eb3a45c5633c5ef75f7466b8601ed72c8022a8b3f6c1f3be	abe1d920b98240580563f750c1c1e4db
yd1tbc.exe	6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f	12d399e6966db58f6d189d606ac34cc8
IPv4	144[.]172[.]110[.]106	N/A
URL	http://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion/chat[.]php	N/A
Dominio	browser-updater[.]com	N/A
IPv4	206[.]251[.]239[.]164	N/A
dominio	ms-sql-auth[.]com	N/A
dominio	os-update-server[.]org	N/A
IPv4	199[.]217[.]98[.]153	N/A
dominio	browser-updater[.]live	N/A
Dominio	first-update-server[.]com	N/A

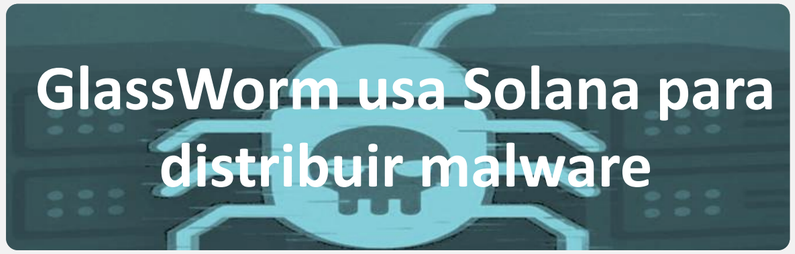
ÚLTIMAS NOTICIAS



Invitación falsa de Zoom distribuye malware

Investigadores detectaron una campaña de phishing que usa invitaciones falsas de Zoom para propagar malware en usuarios de Windows. El ataque comienza con un correo que parece una invitación legítima, llevando al usuario a pruebas de seguridad y a una sala de espera simulada con interfaz de Zoom y participantes ficticios. Durante este proceso, se induce al usuario a descargar un “update” que en realidad instala una herramienta de administración remota usada maliciosamente para tomar control del sistema.
Los correos fraudulentos provienen de cuentas de Gmail y los enlaces no pertenecen a Zoom.

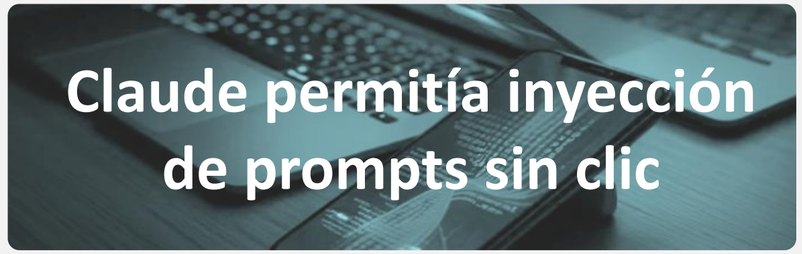
INFO



GlassWorm usa Solana para distribuir malware

Investigadores han identificado una nueva variante del malware GlassWorm que utiliza la blockchain de Solana para obtener instrucciones de comando y control (C2) y descargar cargas maliciosas. La campaña distribuye un RAT que instala una extensión de Chrome capaz de robar datos del navegador y criptomonedas, además de incluir herramientas para phishing y exfiltración de credenciales. Se propaga mediante múltiples vectores, como paquetes en repositorios públicos, representando una amenaza avanzada para desarrolladores y usuarios.

INFO



Claude permitía inyección de prompts sin clic

Investigadores revelan una vulnerabilidad crítica en la extensión de Google Chrome de Claude que permitía a cualquier sitio web inyectar prompts maliciosos sin interacción del usuario (zero-click) aprovechando una XSS y una lista de orígenes demasiado permisiva. La falla, conocida como ShadowPrompt, podía hacer que el asistente ejecutara comandos como si fueran legítimos, posibilitando robo de datos sensibles, acceso a conversaciones y acciones en nombre del usuario. Tras divulgación responsable, se lanzó un parche que restringe estrictamente los orígenes permitidos y se mitigó la XSS subyacente.

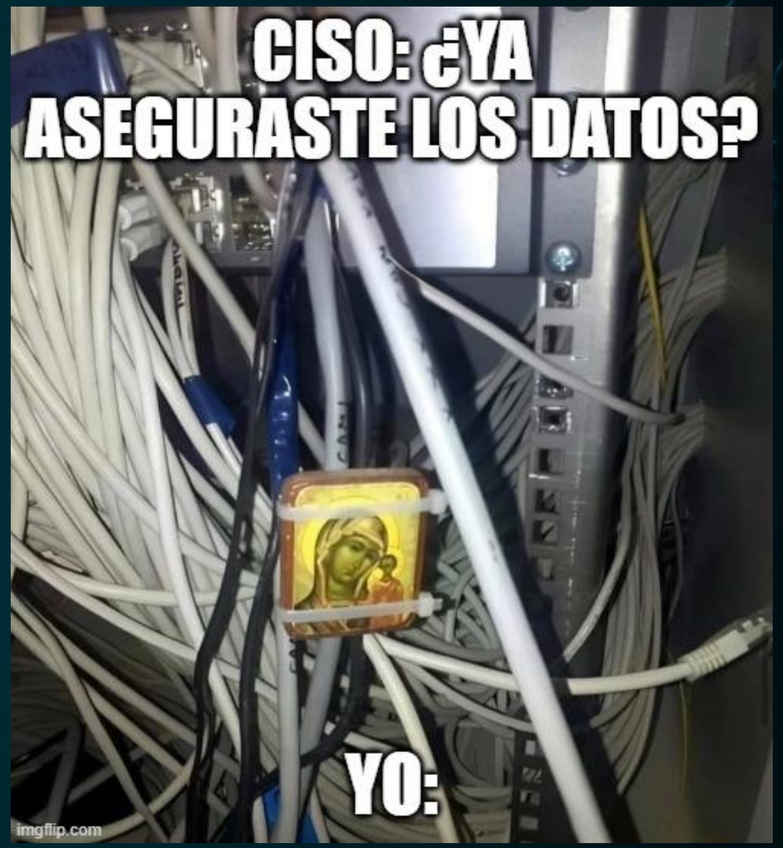
INFO

Ciberseguridad Hoy: Riesgos Reales, Acciones Urgentes

En entornos tecnológicos, esta idea se traduce en prácticas como usar contraseñas débiles, no actualizar sistemas, o asumir que “nunca pasa nada”. La seguridad de la información depende de controles, procesos y buenas prácticas bien implementadas.
La realidad es que los riesgos existen constantemente: accesos no autorizados, pérdida de información, ransomware, entre otros. Por eso, es clave pasar a una seguridad real, basada en prevención, monitoreo y respuesta.

🔐**Usa contraseñas seguras y únicas:** Evita repetirlas y apóyate en un gestor de contraseñas.
👥**Activa la autenticación multifactor (MFA)** siempre que sea posible.
🔁**Mantén sistemas y aplicaciones actualizados** para reducir vulnerabilidades.
📋**Realiza respaldos periódicos** y verifica que puedan restaurarse correctamente.
🔑**Controla el acceso físico y lógico** a equipos y redes.
🧩**Evita conexiones improvisadas o desordenadas** que dificulten la gestión y aumenten riesgos.
👩‍🏫**Capacítate continuamente:** la seguridad también depende de las personas.

La suerte no es una estrategia de seguridad.



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4

© 2025 DataSec SAS. Todos los Derechos Reservados
CYBERSOCDTS by DataSec