BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

LockBit 5.0 amplía ataques ransomware a Windows, Linux y ESXi

TLP:CLEAR
23.02.2026

WINDOWS | LINUX | ESXI

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → LockBit 5.0 amplía ataques ransomware a Windows, Linux y ESXi

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.

Firefox Heap Buffer Overflow in libvpx

CVE-2026-2447

High (8.8)

Impacto: Corrupción de memoria.

Resumen: Una vulnerabilidad de heap buffer overflow en la biblioteca libvpx permite que un atacante remoto cause corrupción de memoria significativa al procesar contenido malicioso en aplicaciones que dependen de esta librería, lo que podría resultar en ejecución de código, inestabilidad o exposición de información sensible. Esta falla no requiere privilegios ni autenticación, aunque puede necesitar interacción del usuario para activar el procesamiento de datos maliciosos.

Productos Afectados

Los productos afectados con sus versiones son:

- Firefox - anteriores a 147.0.4
- Firefox ESR - anteriores a 140.7.1 y 115.32.1
- Thunderbird - anteriores a 147.0.2

Ver +INFO.

Solución:

Actualizar los productos afectados a versiones superiores donde se ha corregido esta vulnerabilidad:

- Firefox ≥ 147.0.4
- Firefox ESR ≥ 140.7.1 o 115.32.1
- Thunderbird ≥ 147.0.2

Ver + INFO.

Fecha de Publicación: 16/FEB/2026 INFO

Windows Admin Center Elevation of Privilege Vulnerability

CVE-2026-26119

High (8.8)

Impacto: Elevación de privilegios no autorizado.

Resumen: Una vulnerabilidad de Improper Authentication en Windows Admin Center permite que un atacante autorizado con privilegios bajos eleve sus privilegios sobre la red. Esto puede permitir al atacante acceder a funciones administrativas sensibles, modificar datos o afectar servicios gestionados a través del Windows Admin Center si logra explotar la falla en un entorno de producción.

Producto Afectado

El producto y las versiones afectadas son:

- Windows Admin Center versiones anteriores a 2.6.4

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Microsoft, Windows Admin Center a la versión parcheada más reciente 2.6.4 o posterior.

Ver +INFO.

Fecha de Publicación: 17/FEB/2026 INFO

MongoDB pre-authentication memory exhaustion denial of service

CVE-2026-25611

High (7.5)

Impacto: Denegación de servicios.

Resumen: Una serie de mensajes especialmente diseñados y no autenticados enviados a un servidor MongoDB puede agotar la memoria disponible y provocar que el servidor se bloquee o deje de responder, impidiendo que las aplicaciones que dependen de él funcionen correctamente. El ataque puede realizarse desde la red sin necesidad de autenticación ni interacción del usuario, lo que aumenta su riesgo.

Producto Afectado

El producto y las versiones afectadas son:

- MongoDB Server versiones anteriores 7.0.29 - 8.0.18 - 8.2.4

Ver +INFO.

Solución:

Actualizar MongoDB Server a versiones 7.0.29 o superiores, 8.0.18 o superiores o 8.2.4 o superiores.

Ver +INFO.

Fecha de Publicación: 20/ENE/2026 INFO

Cisco remote Code Execution en interfaz web administrativa

CVE-2026-20045

High (8.2)

Impacto: Ejecución de código arbitrario.

Resumen: Una vulnerabilidad de Code Injection en varios productos de Cisco Unified Communications se debe a la validación incorrecta de entradas proporcionadas por el usuario en solicitudes HTTP enviadas a la interfaz de gestión web. Un atacante remoto no autenticado puede enviar solicitudes HTTP especialmente diseñadas que permiten ejecutar comandos arbitrarios en el sistema operativo subyacente del dispositivo afectado.

Productos Afectados

Algunos de los productos compatibles afectados:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Communications Manager Session Management Edition (Unified CM SME)

Ver +INFO.

Solución:

Actualizar los productos afectados a las versiones parcheadas disponibles proporcionadas por Cisco.

Ver +INFO.

Fecha de Publicación: 13/FEB/2026 INFO

Tenable Security Center Release

CVE-2026-2630 - CVE-2025-54090
CVE-2025-13034 - CVE-2025-14017

Tenable ha publicado parches de seguridad para corregir varias vulnerabilidades con impacto alto, internas y también fallas presentes en componentes de terceros usados por el producto. Estas podrían permitir ejecución de código remoto y fallas en componentes integrados.

Recomendación:
Aplicar los parches liberados por Tenable lo antes posible y asegurar el entorno donde se aloja el producto.

Productos Afectados

Los productos afectados son:

- Tenable Security Center 6.5.1
- Tenable Security Center 6.6.0
- Tenable Security Center 6.7.2

Ver +INFO

Fecha de Publicación: 17/FEB/2026 INFO

Google Chrome Release

CVE-2026-2313 - CVE-2026-2314
CVE-2026-2315 - CVE-2026-2316

Google Chrome ha publicado una nueva versión estable (Chrome 145) para Windows, macOS y Linux, con varias correcciones de seguridad importantes. Esta versión corrige 11 vulnerabilidades internas del navegador, varias de ellas de alta severidad que podrían permitir ataques si no se aplica el parche.

Recomendación:
Actualizar Chrome inmediatamente a la versión estable más reciente.

Productos Afectados:

Los productos afectados son:

- Windows (Chrome 145.0.7632.45/46)
- macOS (Chrome 145.0.7632.45/46)
- Linux (Chrome 145.0.7632.45)

Ver +INFO

Fecha de Publicación: 10/FEB/2026 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
11/02/2026	CVE-2026-0229	Palo alto	6.6	Permite a un atacante enviar paquetes maliciosos especialmente diseñados a un firewall para hacer que el dispositivo se reinicie repetidamente o quede fuera de servicio, afectando la disponibilidad de la red protegida con PAN-OS que tenga habilitada la función Advanced DNS Security.
10/02/2026	CVE-2026-20026 CVE-2026-20027	Cisco	5.8	Permite a un atacante remoto y sin autenticación enviar muchas solicitudes DCE/RPC malformadas a un dispositivo que esté ejecutando Snort 3. Si el motor de inspección procesa estas solicitudes, puede: reiniciar inesperadamente el motor Snort, provocar una interrupción del análisis de tráfico de red y Causar un estado de denegación de servicio (DoS) en la función de inspección del firewall o sistema afectado.
12/02/2026	CVE-2025-20359 CVE-2025-20360	Cisco	6.5	Permite a un atacante remoto y sin autenticarse enviar paquetes HTTP manipulados a través de una conexión inspeccionada por Snort 3, provocando posible divulgación de información o reinicio inesperado, lo que puede detener temporalmente la inspección de tráfico.
12/02/2026	CVE-2026-2026	Tenable	6.9	Permite a un atacante con acceso local acceder o modificar archivos y potencialmente provocar una denegación de servicio.
12/02/2026	CVE-2026-1707	PostgreSQL	7.4	Permite a un atacante con acceso a la interfaz web obtener control parcial del servidor durante una restauración de base de datos, permitiéndole ejecutar comandos en ese equipo.
11/02/2026	CVE-2026-21318	Adobe	7.8	Permite escritura fuera de límites en memoria, lo que puede conducir a ejecución de código malicioso si la víctima abre un archivo malicioso.
23/02/2026	CVE-2025-25249	Fortinet	7.4	Permite que un atacante no autenticado envíe paquetes especialmente diseñados (crafted packets) al dispositivo o sistema afectado y, aprovechando el fallo, logre ejecutar código arbitrario de forma remota. Como consecuencia, podría comprometer completamente el dispositivo, obtener acceso a información sensible, modificar configuraciones críticas de seguridad e incluso provocar la interrupción del servicio, dejando el equipo inutilizable.

LockBit 5.0 amplía ataques ransomware a Windows, Linux y ESXi

LockBit es una de las operaciones de ransomware-as-a-service (RaaS) más prolíficas del mundo, en la que desarrolladores mantienen el código y afiliados llevan a cabo ataques. Su versión más reciente, LockBit 5.0, fue lanzada en septiembre de 2025 y está diseñada para ser multiplataforma, con binarios específicos para Windows, Linux y VMware ESXi, permite comprometer infraestructuras heterogéneas desde estaciones de trabajo hasta servidores y entornos virtualizados. Utiliza cifrado moderno para bloquear archivos y combina doble extorsión (cifrado de datos más exfiltración) para presionar a las víctimas a pagar rescates. El ransomware incorpora técnicas avanzadas de evasión, ofuscación, terminación de servicios de seguridad y eliminación de registros para dificultar su detección, análisis forense y respuesta. LockBit 5.0 ha sido observado en campañas activas que afectan empresas en múltiples sectores y regiones, demostrando la resiliencia y evolución.

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

El ATAQUE

Los ataques de LockBit 5.0 suelen comenzar con acceso inicial a través de vectores comunes como phishing, explotación de servicios expuestos o utilización de credenciales comprometidas. Una vez dentro, el ransomware realiza reconocimiento interno y despliega la variante adecuada según el sistema operativo objetivo, permitiendo cifrar archivos en estaciones Windows, servidores Linux o incluso hipervisores VMware ESXi, lo que puede paralizar múltiples máquinas virtuales desde un solo punto de entrada. El malware ejecuta cifrado rápido y extensivo, añade extensiones de archivo aleatorias, elimina copias de sombra y evasión de copias de seguridad, y deja notas de rescate con enlaces de negociación. En varios casos documentados en la comunidad de seguridad, LockBit 5.0 ha llevado a la publicación de datos robados cuando no se paga rescate, lo que evidencia su doble enfoque de cifrado y exfiltración para maximizar presión sobre las víctimas.

+ INFO

CONTEXT	INDICATOR	(MD5)
LB5Win.exe	180e93a091f8ab584a827da92c560c78f468c45f2539f73ab2deb308fb837b38	5e1f61b9c1c27cad3b7a81c804ac7b86
Dominio	lockbit7z2mmiz3ryxafn5kapbvbbiywsxwovasfkgf5dqqp5kxlajad[.]onion	N/A
bca0u.exe	90b06f07eb75045ea3d4ba6577afc9b58078eafeb2cdd417e2a88d7ccf0c0273	a1539b21e5d6849a3e0cf87a4dc70335
Dominio	Rodericwalter[.]com	N/A
ntdll.dll	1da6525ae1ef83b6f1dc02396ef0933732f9ffdfca0fda9b2478d32a54e3069b	e818a9afd55693d556a47002a7b7ef31
lw44w5aq.exe	98d8c7870c8e99ca6c8c25bb9ef79f71c25912fbb65698a9a6f22709b8ad34b6	9bcff8da7165977f973ace12dd4c0ce0
Dominio	Lockbit7z5hwf6ywfuzipoa42tjlmal3x5suuccngsamsgklww2xgyqd[.]onion	N/A
teszt_exe.exe	7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82	95daa771a28eaed76eb01e1e8f403f7c

INFO

ÚLTIMAS NOTICIAS

RCE activa en SolarWinds Web Help Desk

Microsoft ha detectado la explotación activa de vulnerabilidades en SolarWinds Web Help Desk (WHD), producto de SolarWinds, que permiten Remote Code Execution (RCE) sin autenticación en servidores expuestos a Internet. Los atacantes utilizan estas fallas para ejecutar comandos, desplegar herramientas legítimas de administración remota, establecer persistencia, escalar privilegios, moverse lateralmente y extraer credenciales —incluyendo datos de Active Directory—, lo que convierte la vulnerabilidad en un punto crítico de acceso inicial. Se recomienda aplicar parches de inmediato, revisar actividad sospechosa y asegurar cuentas con privilegios para mitigar el riesgo.

INFO

Carga de archivos afecta 800 k sitios WordPress

Fallo crítico de carga arbitraria de archivos (Unauthenticated Arbitrary File Upload) en el plugin WPvivid Backup & Migration de WordPress, permite que atacantes sin autenticación suban archivos maliciosos y logren RCE en sitios vulnerables, lo que puede llevar a la toma completa del sitio web. La vulnerabilidad afecta versiones hasta 0.9.123 del plugin, instalado en más de 800,000 sitios, y se explota a través del parámetro wpvivid_action=send_to_site cuando la función de recibir backups está habilitada (aunque está desactivada por defecto). Debido a un mal manejo de errores en la desencriptación RSA y la falta de saneamiento de rutas/archivos, los atacantes pueden colocar PHP malicioso en directorios accesibles y ejecutar código.

INFO

Extensiones IA falsas atacan 260.000 usuarios Chrome

Una campaña llamada AiFrame, en la que más de 30 extensiones maliciosas de Google Chrome, “asistentes de IA” y “herramientas de productividad”, fueron instaladas por más de 260,000 usuarios. Estas solicitan permisos amplios y luego inyectan iframes remotos desde servidores controlados por los atacantes, lo que les permite modificar dinámicamente su comportamiento sin cambiar el código publicado en la Chrome Web Store, evadiendo mecanismos de revisión. Pudiendo realizar data exfiltración, robar credenciales, acceder a sesiones activas, interceptar contenido de correo electrónico y monitorear actividad en sitios sensibles, convirtiendo la extensión en un vector persistente de ataque.

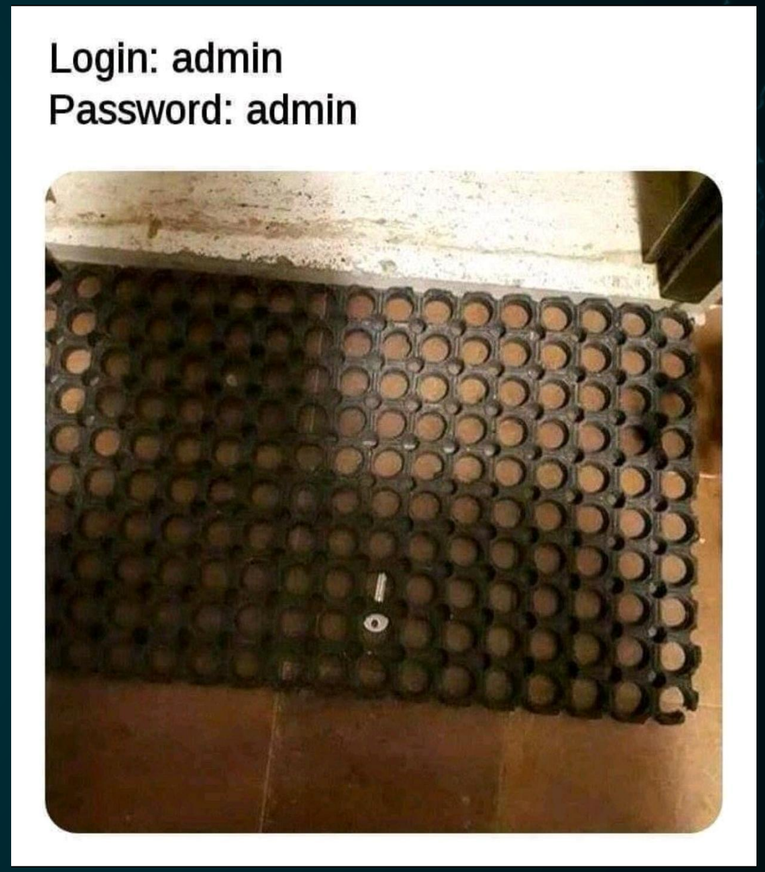
INFO

La seguridad empieza al cambiar la contraseña por defecto

Uno de los errores más comunes en ciberseguridad: mantener las credenciales por defecto en dispositivos, sistemas, routers, cámaras, aplicaciones o plataformas internas. Muchos equipos vienen configurados con usuarios y contraseñas predeterminadas. Si no se cambian, cualquier persona con acceso mínimo o conocimientos básicos puede ingresar fácilmente al sistema. Los atacantes siempre prueban primero credenciales por defecto. Es lo más básico... y sigue funcionando.

🔁 Cambiar inmediatamente las contraseñas por defecto al instalar cualquier equipo o software.
🔐 Usar contraseñas robustas (mínimo 12 caracteres, combinando letras, números y símbolos).
👤 Evitar usuarios genéricos como “admin” si el sistema lo permite.
🛑 Deshabilitar cuentas que no se utilicen.
🔎 Realizar auditorías periódicas para detectar credenciales débiles.
🔑 Implementar autenticación multifactor (MFA) cuando sea posible.

Si la contraseña es fácil de recordar... probablemente también sea fácil de adivinar.



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4