BOLETÍN CIBERSEGURIDAD

CSIRT - DATASEC

DataSec

Arsink, spyware que suplanta apps populares, alcanza 143 países

TLP:CLEAR

09.02.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: ⟶ Arsink, spyware que suplanta apps populares, alcanza 143 países

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.

Cisco Unified Communications Products Remote Code Execution Vulnerability

CVE-2026-20045

High (8.2)

Impacto : Ejecución arbitraria de código

Resumen: Una vulnerabilidad crítica relacionada con la validación inadecuada de entradas en solicitudes HTTP afecta a varios productos de Cisco Unified Communications. Esta falla permite que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema operativo subyacente del dispositivo comprometido.

Versiones Afectadas

Algunas de las versiones compatibles afectadas son:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Webex Calling Dedicated Instance

Ver +INFO.

Solución:

Cisco ha publicado parches y versiones corregidas. Actualizar todas las dependencias afectadas a versiones que contienen la corrección.

Ver + INFO.

Fecha de Publicación: 21/ENE/2026 INFO

VMware vCenter RCE Vulnerability Exploited in Attacks

CVE-2024-37079

Critical (9.8)

Impacto : Ejecución arbitraria de código

Resumen: vCenter Server contiene una vulnerabilidad de desbordamiento de memoria (heap overflow) en la implementación del protocolo DCERPC. Un actor malicioso con acceso a la red del vCenter Server podría explotar esta vulnerabilidad mediante el envío de un paquete de red especialmente diseñado, lo que podría derivar en la ejecución remota de código.

Productos Afectados

Algunos productos compatibles afectados con algunas de sus versiones son:

- VMware vCenter Server 8.0 - 7.0
- VMware Cloud Foundation

Ver +INFO.

Solución:

Se recomienda aplicar las últimas actualizaciones de seguridad disponibles para garantizar la remediación de la vulnerabilidad identificada.

Ver +INFO.

Fecha de Publicación: 26/ENE/2026 INFO

Zoom Node Deployments - Command Injection

CVE-2026-22844

Critical (9.9)

Impacto: Ejecución arbitraria de código

Resumen: Una vulnerabilidad que permite que un participante de una reunión con acceso a la red pueda ejecutar código de manera remota (Remote Code Execution – RCE) en el dispositivo afectado, lo que puede resultar en un control total del sistema comprometido.

Productos Afectados

Los productos compatibles afectados son:

- Zoom Node Meetings Hybrid (ZMH) / connector (MC) – módulos MMR / MC: versiones anteriores a 5.2.1716.0

Ver +INFO.

Solución:

Aplicar la actualización de seguridad oficial proporcionada por Zoom para los módulos MMR.

Ver +INFO.

Fecha de Publicación: 20/ENE/2026 INFO

SQLi in administrative interface

CVE-2026-21643

High (9.1)

Impacto: Ejecución de código o comandos no autorizados

Resumen: Una vulnerabilidad de inyección SQL ("SQL Injection") [CWE-89] en FortiClient EMS, causada por la neutralización inadecuada de elementos especiales en comandos SQL, podría permitir a un atacante no autenticado ejecutar código o comandos no autorizados a través de solicitudes HTTP especialmente diseñadas.

Producto Afectado

Producto compatible afectado:

- Fortinet FortiClientEMS 7.4.4

Ver +INFO.

Solución:

Actualizar FortiClientEMS a versiones superiores (7.4.5)

Ver +INFO.

Fecha de Publicación: 06/FEB/2026 INFO

Google Chrome Release
CVE-2026-1504

Google lanzó una actualización del canal estable de Chrome para escritorio que corrige una vulnerabilidad de alta severidad relacionada con una implementación inapropiada de la API Background Fetch, la cual podría ser explotada para comprometer la seguridad del navegador y afectar la ejecución segura de procesos en segundo plano.

Recomendación:
Google recomienda aplicar de manera inmediata las actualizaciones de seguridad del navegador Chrome las cuales se distribuye de forma progresiva

Producto Afectado

Algunos de los productos afectados son:
- Google Chrome para Windows
- Google Chrome para MacOS
- Google Chrome para Linux

Ver +INFO

Fecha de Publicación: 27/ENE/2026 INFO

Tenable Network Monitor Version 6.5.3 Fixes Multiple Vulnerabilities

CVE-2025-6021 - CVE-2025-49794
CVE-2025-49796 - CVE-2025-10911

Tenable lanzó la versión 6.5.3 de Nessus Network Monitor para corregir múltiples vulnerabilidades presentes en componentes de terceros utilizados por el software. libxml2, libxslt, expat, c-ares, curl y sqlite, estas podrían permitir ejecución de código, corrupción de memoria o evasión de seguridad, dependiendo del componente y del contexto de explotación.

Recomendación:
Tenable recomienda actualizar inmediatamente a la versión 6.5.3 de Nessus Network Monitor para mitigar los riesgos asociados a estas vulnerabilidades.

Producto Afectado:

Los productos afectados son:
- Nessus Network Monitor en versiones anteriores a 6.5.3

Ver +INFO

Fecha de Publicación: 27/ENE/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
22/01/2026	CVE-2026-0723	GitLab	7.4	Permite a un atacante eludir mecanismos de seguridad, mediante la manipulación de solicitudes o respuestas del sistema, lo que le permitiría obtener acceso no autorizado a cuentas legítimas
21/01/2026	CVE-2026-20080	Cisco	5 .3	Permite a un atacante no autenticado realizar un ataque de denegación de servicio (DoS) contra el servicio SSH de un dispositivo Cisco logrando que este deje de responder y potencialmente interrumpiendo el acceso de administración remota
21/01/2026	CVE-2026-20092	Cisco	6.0	Permite a un atacante autenticado con acceso local y privilegios administrativos elevar sus privilegios a nivel de root en el appliance virtual afectado, o que le daría control total del sistema, incluyendo acceso a información sensible.
26/01/2026	CVE-2026-21509	Microsoft	7.8	Permite a un atacante, mediante el envío de un archivo de Microsoft Office, posibilitar la ejecución de acciones no autorizadas, la exposición o manipulación de información sensible, y el avance de otras cargas maliciosas dentro del sistema afectado.
07/02/2026	CVE-2025-56005	Tenable	9.8	Permite que un atacante ejecute código arbitrario mediante el parámetro picklefile de la función yacc(), el cual deserializa archivos pickle sin validación, permitiendo la ejecución de código malicioso a través del método __reduce__().
20/01/2026	CVE-2025-14533	Wordfernce	9.8	Permite a un atacante no autenticado manipular el proceso de registro de usuarios en el plugin “Advanced Custom Fields: Extended” de WordPress para asignarse el rol de administrador y así obtener acceso administrativo.

Arsink, spyware que suplanta apps populares, alcanza 143 países

Arsink es un spyware para Android identificado como un troyano de acceso remoto (RAT) que permite a los atacantes obtener control total sobre los dispositivos infectados. El malware se distribuye mediante aplicaciones falsas que suplantan a plataformas legítimas y populares como WhatsApp, YouTube, Instagram y TikTok, presentándose como versiones modificadas o premium. Una vez instalado, Arsink solicita múltiples permisos críticos que le permiten acceder a datos sensibles como mensajes, contactos, registros de llamadas, ubicación y almacenamiento, además de activar el micrófono para grabar audio. El spyware opera de forma persistente en segundo plano, puede ocultar su presencia en el dispositivo y comunicarse con servidores de comando y control, lo que lo convierte en una amenaza relevante para la privacidad y la seguridad de los usuarios.

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

El ATAQUE

El ataque de Arsink se basa en técnicas de ingeniería social y distribución de malware fuera de tiendas oficiales. Los atacantes crean aplicaciones maliciosas que imitan servicios legítimos y las difunden a través de plataformas de mensajería, redes sociales y sitios de alojamiento de archivos. El usuario descarga e instala manualmente la aplicación, habilitando la instalación desde fuentes desconocidas. Durante la instalación, la aplicación solicita permisos excesivos que, al ser aceptados, permiten la ejecución del spyware. Una vez activo, Arsink se oculta y establece comunicación con su infraestructura de comando y control, desde donde los atacantes pueden ejecutar acciones remotas, recolectar información, monitorear la actividad del dispositivo y mantener el acceso persistente sin que el usuario lo detecte fácilmente.

+ INFO

CONTEXT	INDICATOR	(MD5)
Nexus Rat [@]marceleven.apk	725fb7b6f3f1d93a5a2d1e2f504062609663dc1ca268d2293274fd538e0fc5a5	0005982a3be4dec1315af2fb85c15c26
app.zip	002a84e55058825d5592954bc662a8ab	002a84e55058825d5592954bc662a8ab
YouTube Black_1.0.apk	3a15c18c53127392d5b08098e5164d533828bb98c83941f23ba07438d3ddec77	0712c514e309617a148a1bb23e1459d8
AIR_1.0.zip	911b4bb73247c23c44337cd3b0a4083efcc3c6d41ada6f2b1d116d3cb60682cc	01a838f467adb982fa0038d7180d22e4
Nako Care Terbaru.apk	2eded0d86955ee7e63ee9bacc436b7f3f6332152f8de9c6c50ff56f1e07a7db5	09aed3f7f99e185805ea25c42ec4da50
Nekopoi care.apk	a9b5a1c223e2335c663c70add3cc54e2da580877f172aa883a6bd7f68bf1abd3	08eb770a808f34e2b0385a01cd38c5f3
Instagram Mod_1.0.apk	5205d9fa877dc04534b3b315e23c71440057e1adda5d219a2f0f38d2c5221167	057518df622ef3026ab6dc2e1a83eb9d
chatgpt.apk	5c5313c2d1753326ee6357127fb8ef1ba6d49e540b9da9de5ab8050d86114bff	09c3c0084356aa78591f8f3cfebd82dc

INFO

ÚLTIMAS NOTICIAS

Phishing en sector energético

Microsoft ha alertado sobre una campaña de phishing multi-etapa con técnica adversary-in-the-middle que ha comprometido cuentas de Microsoft pertenecientes a múltiples organizaciones del sector energético. Los atacantes usaron cuentas previamente comprometidas para enviar correos con enlaces a SharePoint que redirigían a sitios de credential harvesting, permitiéndoles robar credenciales y tomar control de buzones corporativos. Una vez dentro, configuraron reglas de bandeja de entrada para ocultar la actividad y enviaron más de 600 correos de phishing desde las cuentas comprometidas, incluso respondiendo y eliminando mensajes para parecer legítimos

INFO

VS Code explotado para acceso remoto encubierto

Darktrace identificó una campaña de spear-phishing dirigida a organizaciones en Corea del Sur, atribuida a actores de amenazas vinculados a la RPDC (Corea del Norte). La campaña utiliza documentos señuelo con temáticas gubernamentales que contienen scripts JSE ofuscados, los cuales descargan y ejecutan Visual Studio Code para establecer un túnel remoto mediante VS Code, otorgando acceso persistente al sistema comprometido. Al abusar de herramientas legítimas y servicios confiables de Microsoft (living-off-the-land), los atacantes logran evadir controles de seguridad tradicionales, facilitando el movimiento lateral, la persistencia y la posible exfiltración de información sin desplegar malware convencional.

INFO

Ataque a npm: Shai-Hulud eludido vía Git

Investigadores de Koi Security descubrieron fallas, denominadas PackageGate, que permiten a actores de amenazas eludir los mecanismos de defensa introducidos tras los ataques de la cadena de suministro “Shai-Hulud” al instalar dependencias desde repositorios Git. Estas debilidades afectan a herramientas de gestión de dependencias como npm, pnpm, vlt y Bun, y pueden permitir ejecución de código malicioso incluso con la bandera --ignore-scripts activada, debido a que archivos de configuración maliciosos pueden anular rutas al binario de Git. Se recomienda fortalecer la gestión de dependencias y adoptar prácticas de hardening para reducir riesgos en la cadena de suministro de software.

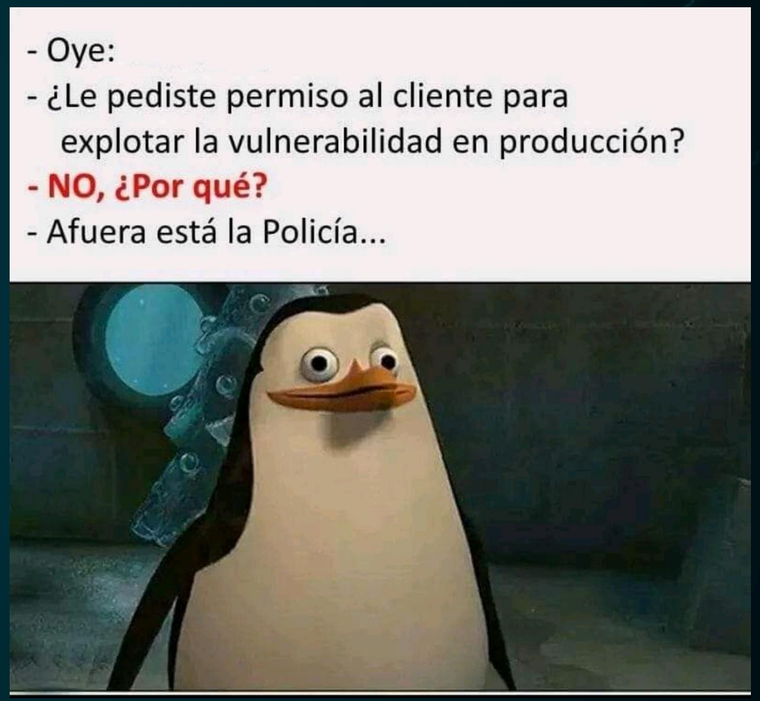
INFO

La seguridad también se prueba con responsabilidad

En el ámbito de la seguridad informática, realizar pruebas en sistemas de producción sin la debida autorización implica riesgos técnicos y legales. Aunque el objetivo sea validar vulnerabilidades, hacerlo sin consentimiento puede generar interrupciones del servicio y responsabilidades legales. Por ello, estas pruebas deben ejecutarse bajo un marco controlado y con la aprobación correspondiente, garantizando la integridad de los sistemas y el cumplimiento normativo. A continuación, algunas recomendaciones:

📶 Solicitar y obtener autorización formal antes de ejecutar cualquier prueba en ambientes productivos.
🔒 Priorizar el uso de entornos de prueba o desarrollo para validar vulnerabilidades.
📡 Establecer y respetar protocolos claros que definan el alcance y límites de las pruebas.
📱 Documentar y comunicar adecuadamente los hallazgos para facilitar su gestión y mitigación.

Actuar con responsabilidad y respeto a los procedimientos no solo protege a la organización, sino que también fortalece la confianza y profesionalismo del equipo de seguridad.



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4