BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

SynkLoader: el malware que convierte Teams en una puerta de entrada

TLP:CLEAR
07.09.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: ⟶ SynkLoader: Teams y nuevas vías para sus ciberataques

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.

Adobe Campaign Classic (ACC) | Improper Neutralization of Special Elements used in an OS Command

CVE-2026-76197

Critical (10.0)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad crítica de inyección de comandos en Adobe Campaign Classic que puede ser explotada remotamente sin autenticación ni interacción del usuario, permitiendo ejecutar código arbitrario con los privilegios del usuario actual.

Producto Afectado

- Adobe Campaign Classic (ACC) v7 y anterirores.

Ver +INFO.

Solución:

Actualizar a la versión más reciente disponible de Adobe Campaign Classic.

Ver + INFO.

Fecha de Publicación: 29/AGO/2026 INFO

Vulnerabilidad crítica en Oracle Database Portable Clusterware

CVE-2026-71063

Critical (9.6)

Impacto: Compromiso total del clúster.

Resumen: Se identificó una vulnerabilidad crítica en Oracle Database Portable Clusterware que puede ser explotada por atacantes no autenticados con acceso al segmento de red, permitiendo comprometer el clúster y afectar la confidencialidad, integridad y disponibilidad del sistema.

Producto Afectado

- Oracle Database Server – Portable Clusterware (versiones 19c, 21c y 23c)

Ver +INFO.

Solución:

Actualizar Oracle Database Server a la versión más reciente disponible

Ver +INFO.

Fecha de Publicación: 20/AGO/2026 INFO

Cisco BroadWorks: Lectura de archivos mediante XML

CVE-2026-20320

High (7.5)

Impacto: Exposición de información sensible.

Resumen: Se identificó una vulnerabilidad en el analizador XML de Cisco BroadWorks que puede ser explotada por atacantes remotos no autenticados mediante el envío de mensajes XML especialmente diseñados, permitiendo acceder a información sensible y leer archivos del sistema de archivos con los privilegios del usuario Cisco BroadWorks.

Producto Afectado

- Cisco BroadWorks anteriores a RI.2026.07.

Ver +INFO.

Solución:

Actualizar los productos afectados a RI.2026.07 o posterior.

Ver +INFO.

Fecha de Publicación: 20/AGO/2026 INFO

Ipv6: account for fraggap on the paged allocation path

CVE-2026-53362

High (7.8)

Impacto: Corrupción de memoria.

Resumen: Se identificó una vulnerabilidad en el kernel de Linux, específicamente en IPv6, que podía provocar una escritura fuera de los límites de memoria al procesar paquetes UDPv6. Un usuario sin privilegios podía desencadenar la falla, causando corrupción de memoria y afectando la estabilidad y seguridad del sistema.

Producto Afectado

- Kernel de Linux componente IPv6/UDPv6.

Ver +INFO.

Solución:

Actualizar a la versión más reciente disponible de Linux Kernel.

Ver + INFO.

Fecha de Publicación: 28/AGO/2026 INFO

Microsoft security updates

CVE-2026-65816 – CVE-2026-69555

Microsoft corrigió múltiples vulnerabilidades críticas en servicios de Azure y Microsoft Entra ID, incluyendo fallos que podrían permitir a atacantes no autenticados ejecutar código de forma remota y escalar privilegios. Entre las vulnerabilidades destacan una falla de deserialización en Entra ID y vulnerabilidades críticas en Azure Arc, Exchange Online y Azure Managed Instance for Apache Cassandra.

Recomendación:

Aplicar oportunamente las actualizaciones de seguridad de Microsoft correspondientes a agosto de 2026.

Productos Afectados

Algunos de los productos afectados son:

- Microsoft Entra ID
- Azure Arc
- Azure Managed Instance for Apache Cassandra

Ver +INFO

Fecha de Publicación: 21/AGO/2026

INFO

Google chrome releases

CVE-2026-79282 – CVE-2026-79290
CVE-2026-79054 – CVE-2026-79121

Google lanzó Chrome 152, corrigiendo 327 vulnerabilidades, incluidas 10 críticas y 61 de alta gravedad. La mayoría de los fallos fueron descubiertos internamente por Google, con un aumento significativo en la detección mediante IA, aunque investigadores externos también reportaron vulnerabilidades críticas.

Recomendación:

- Actualizar Google Chrome a la versión más reciente disponible.

Productos Afectados:

Los productos afectados son:

- Google Chrome para Windows
- Google Chrome para MacOS
- Google Chrome para Linux

Ver +INFO

Fecha de Publicación: 25/AGO/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
02/09/2026	CVE-2026-55040	Microsoft	9.1	Se identificó una vulnerabilidad de autenticación débil en Microsoft Office SharePoint que podría permitir a un atacante no autorizado evadir los mecanismos de seguridad a través de la red y realizar acciones no autorizadas en el sistema afectado.
02/09/2026	CVE-2026-63520	Microsoft	8.1	Se identificó una vulnerabilidad relacionada con la validación incorrecta de entradas en Microsoft Office SharePoint, que podría permitir a un atacante no autorizado ejecutar código de forma remota a través de la red y comprometer el sistema afectado.
27/08/2026	CVE-2019-1068	Microsoft	8.8	Se identificó una vulnerabilidad en Microsoft SQL Server que podría permitir la ejecución remota de código debido a un procesamiento incorrecto de funciones internas.
27/08/2026	CVE-2026-81838	AWS	7.1	Se identificó una vulnerabilidad de recorrido de rutas en AWS diagram-as-code (awsdac), que podría permitir a un atacante escribir archivos arbitrarios en el sistema afectado mediante archivos ZIP manipulados.
02/09/2026	CVE-2026-20281	Cisco	7.5	Se identificó una vulnerabilidad en teléfonos Cisco que podría permitir a un atacante remoto no autenticado provocar una denegación de servicio mediante el envío de paquetes HTTP manipulados.

SynkLoader: el malware que convierte Teams en una puerta de entrada

Investigadores de Expel identificaron una nueva familia de malware denominada SynkLoader, distribuida mediante campañas de phishing en Microsoft Teams que se hacen pasar por el soporte informático de las organizaciones. El malware utiliza una combinación de PowerShell, Python, C# y C++ para desplegar módulos destinados al reconocimiento del sistema, persistencia, robo de credenciales, acceso remoto y tunelización de tráfico. Entre sus componentes destaca PhishLocker, que simula una pantalla de bloqueo de Windows para capturar las contraseñas de los usuarios. Por sus capacidades y el reconocimiento de entornos Active Directory, los investigadores consideran que SynkLoader podría estar siendo utilizado como parte de operaciones de ransomware.

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

El ATAQUE

El ataque de SynkLoader comienza con una campaña de phishing a través de Microsoft Teams, donde los atacantes se hacen pasar por el soporte informático de la organización y engañan a la víctima para instalar un archivo MSI malicioso disfrazado de “PowerShell Cleaner”. Al ejecutarlo, se despliegan componentes en PowerShell y Python que recopilan información del sistema y establecen persistencia mediante tareas programadas. Posteriormente, el malware puede activar módulos para robar credenciales mediante una falsa pantalla de bloqueo de Windows, ejecutar comandos de forma remota, controlar el escritorio y crear túneles hacia servicios internos. Estas capacidades permiten a los atacantes mantener el acceso al equipo comprometido y potencialmente utilizarlo como punto de entrada para comprometer la red corporativa.

INFO

CONTEXT	INDICATOR	(MD5)
Dominio	avene-hebergement[.]com	N/A
SHA1	fe4a5c477e968d4ece33f8e8442acf319e33544c	f23e8778c1af081a1a505e310564b3f2
SHA1	fbac058898fc361577cf9ae296de4dcd222084c8	0a47aa3fbb4b852c2d346116c55a6432
SHA1	f2a82779f39a0b36ce61387b2072a7931aa20464	87a339436e4841d0e0f847377137bfd1
SHA256	54ba68040413b23128455952e4a698df112a163d0498ded6f77e863d15113133	45f6d1142b5921f90ddf7939df796774
SHA256	42095fff1452418550440d5adff87a10e6d04a704fedf2b221f83b6a974a0d73	b270253b3fa7838c67ad892f24de799a
SHA256	e37cc7f678aa800b805aefcc57ad86251cb7b89a044c43c72be9a77f36a88e57	232594806588cbdf8dbb79922d33a97f
SHA256	fee8d5964fcc23027685ee1124a19127ce58d4692c9df831bd1b900cdb86faeb	0ecefbf90c207dd0914427846fcad1df

INFO

ÚLTIMAS NOTICIAS

AnonyMousKIT roba códigos de iPhone con IA.

AnonyMousKIT utiliza phishing y agentes de voz con IA para engañar a propietarios de iPhone y robar códigos de acceso y credenciales de Apple, permitiendo desbloquear dispositivos robados, acceder a copias de seguridad de iCloud y obtener información personal y corporativa sensible. La plataforma emplea llamadas, mensajes y páginas falsas que imitan servicios oficiales de Apple para aumentar la credibilidad del engaño y facilitar la extracción de datos. Además, los atacantes aprovechan información real de los dispositivos para personalizar los mensajes y hacerlos más convincentes para las víctimas.

INFO

ToxicPanda bloquea Google Play mediante VPN.

ToxicPanda 2.0 ha incorporado nuevas capacidades para bloquear Google Play mediante permisos VPN, robar credenciales financieras y mantener la persistencia en dispositivos Android. El malware amplía su alcance a 349 aplicaciones y 167 comandos remotos, además de abusar de ADB inalámbrico para obtener acceso privilegiado y evadir las protecciones del sistema. También emplea superposiciones de phishing, pantallas falsas de bloqueo y actualización, y mecanismos específicos para evitar las restricciones de batería de distintos fabricantes.

INFO

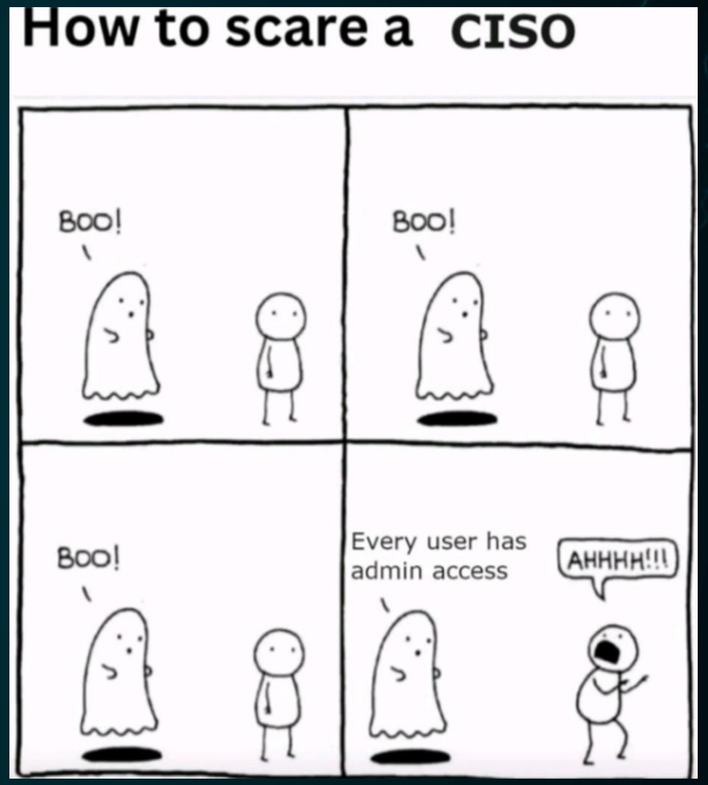
ZeroTokens ejecuta ataques de phishing en tiempo real.

ZeroTokens es una plataforma de phishing que permite a los atacantes monitorear las sesiones de las víctimas en tiempo real y adaptar los engaños según sus respuestas. La campaña afectó a más de 24.000 destinatarios de 700 organizaciones y recopiló credenciales, datos financieros y códigos de verificación, permitiendo a los operadores mantener activas las sesiones hasta completar el robo de información. La plataforma imitaba instituciones financieras legítimas y utilizaba múltiples etapas de verificación para aumentar la efectividad del ataque y evadir las defensas de seguridad.

INFO

El exceso de privilegios también es un riesgo

En ciberseguridad, no todos los riesgos vienen de fuera. A veces, el mayor riesgo comienza con un permiso que nunca debió otorgarse. Cuando los usuarios tienen privilegios administrativos que no necesitan, un simple error, una cuenta comprometida o un malware puede convertirse en una puerta de entrada a sistemas y datos críticos.



🔐 Aplica el principio de mínimo privilegio y asigna únicamente los permisos necesarios para cada función.
👤 Evita el uso generalizado de cuentas con privilegios administrativos para las actividades diarias.
🔎 Revisa periódicamente los accesos y elimina permisos que ya no sean necesarios.
🛡️ Separa las cuentas administrativas de las cuentas de uso cotidiano para reducir la exposición ante incidentes.
🚨 Limita el alcance de una cuenta comprometida para evitar que un incidente pueda propagarse y afectar otros sistemas o información crítica.
📋 Establece políticas de acceso claras y asegúrate de que los privilegios estén alineados con las responsabilidades de cada usuario.

La seguridad también está en saber decir: este acceso no es necesario. Menos privilegios, menor impacto cuando algo sale mal.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4