BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

La variante Shai-hulud 2.0 amenaza el ecosistema de la nube

TLP:CLEAR
09.12.2025

CLICK PARA EMPEZAR

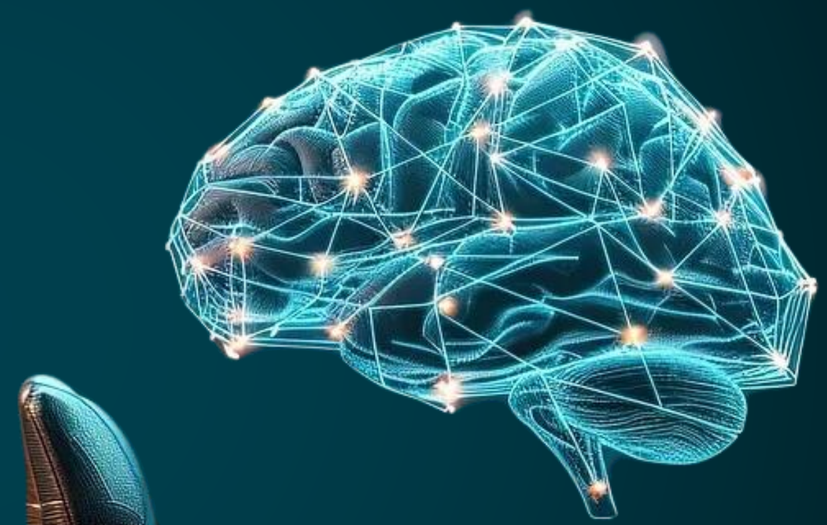
CYBERSOCDTS

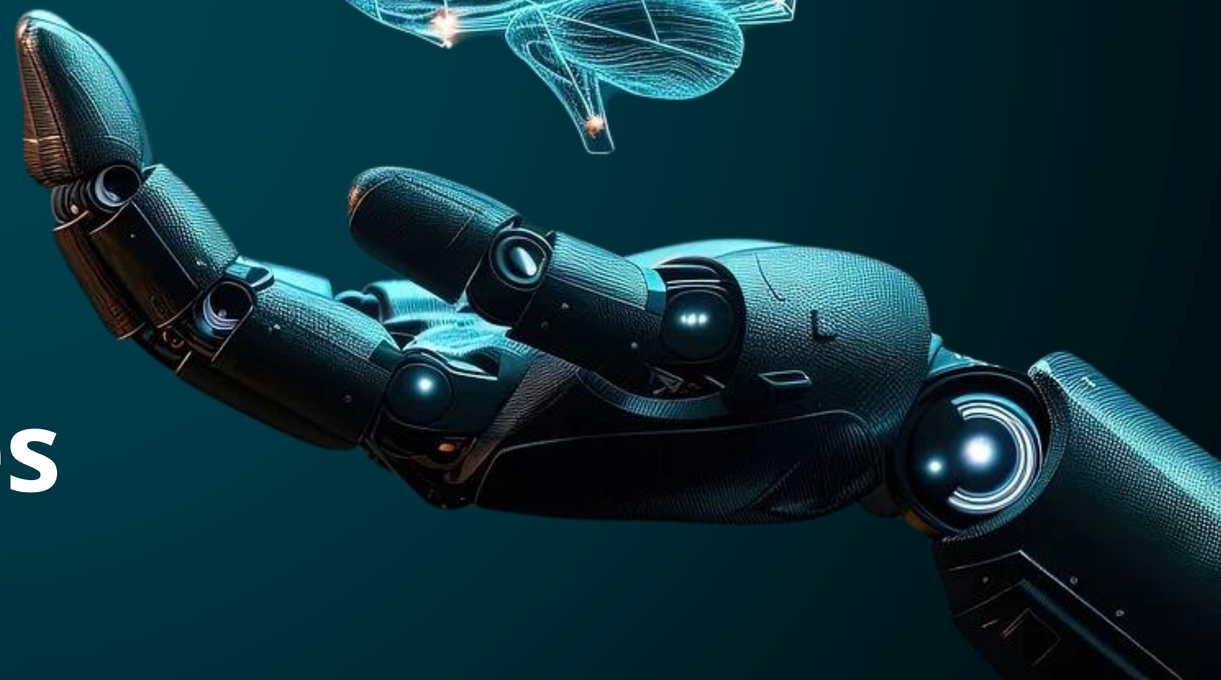
En esta edición: ⟶ La variante Shai-hulud 2.0 amenaza el ecosistema de la nube

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.

Azure Application Gateway Elevation of Privilege Vulnerability

CVE-2025-64656

Critical (9.4)

Impacto: Elevación de privilegios.

Resumen: Una lectura fuera de límites en Application Gateway permite que un atacante no autorizado eleve privilegios a través de la red.

Versión Afectada

La versión compatible afectada es:

- Azure Aplication Gateway de Microsoft.

Ver +INFO.

Solución:

Aplicar el parche de seguridad que Microsoft ha publicado para corregir esta vulnerabilidad tan pronto como sea posible.

Ver + INFO.

Fecha de Publicación: 20/NOV/2025 INFO

Remote Code Execution Vulnerability in React and Next.js Frameworks

CVE-2025-55182

Critical (10.0)

Impacto: Ejecución arbitraria de código.

Resumen: Esta vulnerabilidad podría permitir que un atacante remoto no autenticado realice una ejecución remota de código en un dispositivo o sistema afectado.

Versiones Afectadas

La versión compatible afectada es:

- React 19: 19.0.0, 19.1.0, 19.1.1 y 19.2.0.
- Frameworks basados en React que usan esos componentes en el servidor (Next.js).

Ver +INFO.

Solución:

Actualizar de inmediato a versiones parcheadas de React Server Components (19.0.1, 19.1.2, 19.2.1 o superiores) y actualizar Next.js o cualquier framework que dependa de estos componentes. *Ver +INFO.*

Fecha de Publicación: 03/DIC/2025 INFO

Azure Monitor Elevation of Privilege Vulnerability

CVE-2025-62207

High (8.6)

Impacto: Elevación de privilegio.

Resumen: Esta vulnerabilidad permite que un atacante externo pueda enviar solicitudes creadas de forma maliciosa que engañen al servicio para que éste realice peticiones hacia recursos internos.

Versiones Afectadas

Las versiones compatibles afectadas están asociadas con:

- Azure Monitor “Control Service”.

Ver +INFO.

Solución:

Se recomienda aplicar los parches o actualizaciones de seguridad que publique Microsoft para Azure Monitor lo antes posible.

Ver +INFO.

Fecha de Publicación: 20/NOV/2025 INFO

Critical vulnerability in Apache Struts

CVE-2025-64775

High (7.5)

Impacto: Denegación de servicio.

Resumen: Esta vulnerabilidad permite a atacantes desencadenar ataques de disk exhaustion mediante una filtración de archivos en el procesamiento de solicitudes multipart, causando denegación de servicio.

Versiones Afectadas

Las versiones compatibles afectadas son:

- Apache Struts 2.0.0 – 2.3.37.
- Apache Struts 2.5.0 – 2.5.33.
- Apache Struts 6.0.0 – 6.7.4.
- Apache Struts 7.0.0 – 7.0.3.

Ver +INFO.

Solución:

Actualizar a Apache Struts versión 6.8.0 o superior dentro de la rama 6.x, o a la versión 7.1.1 o posterior.

Ver +INFO.

Fecha de Publicación: 03/DIC/2025 INFO

Actualización de Google

CVE-2025-13634 - CVE-2025-13640
CVE-2025-13631

Google lanzó la versión 143 de Chrome para Windows, macOS y Linux, una actualización crítica que corrige 13 vulnerabilidades de seguridad, incluidas fallas graves de Type Confusion en el motor V8 y vulnerabilidades de use-after-free en componentes como Skia, las cuales podrían permitir la ejecución de código arbitrario y comprometer la seguridad del navegador.

Recomendación:
Se recomienda a todos los usuarios de Chrome actualizar a la versión más reciente para protegerse contra posibles ataques.

Producto Afectado

El producto afectado es:

- Las versiones anteriores a la 143.0.7499.40 del navegador Google Chrome.

Ver +INFO

Fecha de Publicación: 02/DIC/2025

Actualización de Android

CVE-2025-48633 - CVE-2025-48572
CVE-2025-48631

Se han identificado 107 vulnerabilidades de día cero que afectan tanto a componentes del sistema operativo móvil como a otros sistemas que dependen de su versión de código abierto. Android ha publicado un boletín de seguridad que incluye parches para un subconjunto de estas fallas (51 en total, distribuidas entre el framework y el sistema) mientras que el resto será detallado en una próxima actualización oficial.

Recomendación:
Aplicar las actualizaciones disponibles.

Producto Afectado:

Los productos afectados son:

- Framework Android.
- Sistema operativo móvil.

Ver +INFO

Fecha de Publicación: 01/DIC/2025

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
21/11/2025	CVE-2025-53843	Fortinet	6.9	Permite que un atacante remoto autenticado ejecute código o comando arbitrario como un usuario con pocos privilegios mediante paquetes especialmente diseñados.
18/11/2025	CVE-2025-20289 CVE-2025-20303 CVE-2025-20304	Cisco	5.4	Permite que un atacante remoto autenticado divulgue información confidencial o realice un ataque de secuencias de comandos entre sitios reflejados (XSS).
18/11/2025	CVE-2025-58692	Fortinet	7.7	Permite que un atacante autenticado ejecute código o comandos no autorizados mediante solicitudes HTTP o HTTPS específicamente diseñadas.
18/11/2025	CVE-2025-47761	Fortinet	7.1	Permite que un usuario local autenticado ejecute código no autorizado mediante un controlador fortips. El éxito del ataque requeriría saltarse las protecciones de memoria de Windows como la integridad del montón y HSP.
18/11/2025	CVE-2025-46373	Fortinet	7.1	Permite que un usuario local IPSec autenticado ejecute código o comandos arbitrarios mediante el controlador "fortips_74.sys". El atacante tendría que eludir las protecciones de integridad del montón de Windows.
27/11/2025	CVE-2025-10476	WordPress	4.3	Permite modificaciones no autorizadas en la base de datos del sitio, cambios en configuraciones, en datos de cache, u otras operaciones internas del plugin.
26/11/2025	CVE-2025-12571	GitLab	7.5	Permite a un atacante no autenticado (es decir, sin necesidad de tener usuario o privilegios) enviar peticiones maliciosas que provoquen una condición de Denegación de Servicio (DoS).

La variante Shai-hulud 2.0 amenaza el ecosistema de la nube

Shai-hulud 2.0 es un gusano autorreplicante avanzado que amplía su alcance desde npm hacia GitHub y los principales entornos cloud. Incorpora capacidades de robo de credenciales (AWS, GCP, Azure, GitHub, npm), extracción de secretos mediante los servicios nativos de gestión (Secrets Manager, Secret Manager, Key Vault) y apunta también a Azure Pod Identity. Puede abrir puertas traseras, republicar paquetes maliciosos y emplea un módulo destructivo que borra datos si no puede exfiltrarlos. Su comportamiento autónomo y orientado a datos lo convierte en una amenaza crítica para la cadena de suministro de software.

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

El ATAQUE

El ataque inicia con un correo de phishing suplantando una alerta de seguridad de npm, donde el atacante obtiene las credenciales del desarrollador. Con ellas, compromete su cuenta de npm, envenena paquetes y se autentica en GitHub para contaminar aún más repositorios. A continuación, instala TruffleHog para extraer secretos adicionales, hace públicos los repositorios robados y exfiltra datos a través de solicitudes automatizadas. Luego continúa su propagación infectando proyectos y desarrolladores dependientes mediante la instalación de paquetes contaminados. En fases posteriores, el gusano recopila variables de entorno y credenciales en la nube, utiliza estas para acceder a los gestores de secretos de AWS, GCP y Azure, y continúa robando información sensible. Este flujo de ataque combina phishing, escalamiento mediante envenenamiento de paquetes, exfiltración continua y explotación de credenciales cloud, permitiendo que Shai-hulud 2.0 se expanda a lo largo de toda la cadena de suministro y mantenga su capacidad dañina.

INFO

CONTEXT	INDICATOR	(MD5)
bun_environment.js	f099c5d9ec417d4445a0328ac0ada9cde79fc37410914103ae9c609cbc0ee068	207b3c83c0460d5ed9091036af2b357a
bun_environment.txt	cbb9bc5a8496243e02f3cc080efbe3e4a1430ba0671f2e43a202bf45b05479cd	2711e7496f9943ad1fac508ef5665867
setup_bun.js	a3894003ad1d293ba96d77881ccd2071446dc3f65f434669b49b3da92421901a	4d6b9efc22ec229be58b90c7991c02dd
bun_environment[.]jj_s.js	62ee164b9b306250c1172583f138c9614139264f889fa99614903c12755468d0	6914d930998108adfc93b7fe1aa3e64e
deobfuscated.txt	f1df4896244500671eb4aa63ebb48ea11cee196fafaa0e9874e17b24ac053c02	caecb47e161c8789ba965e67c27cda55
bundle (4).js	46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09	78e701f42b76ccde3f2678e548886860

INFO

ÚLTIMAS NOTICIAS

17.000 secretos filtrados en GitLab

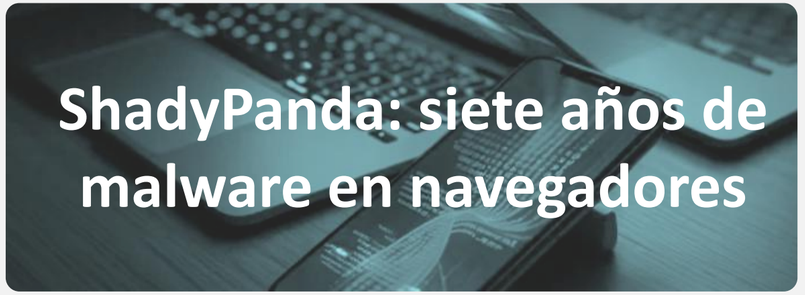
Un ingeniero de seguridad escaneó 5,6 millones de repositorios públicos de GitLab Cloud y descubrió más de 17.000 secretos expuestos, incluyendo credenciales de GCP, MongoDB, Telegram, OpenAI y claves de GitLab. El análisis, realizado con TruffleHog mediante AWS Lambda, reveló una densidad de secretos filtrados mucho mayor que en otras plataformas. Los secretos expuestos (algunos válidos desde 2009) representan un riesgo crítico, ya que podrían permitir accesos no autorizados a infraestructuras cloud y servicios sensibles. Aunque muchas organizaciones revocaron las claves tras ser notificadas, persisten credenciales activas aún accesibles públicamente

INFO

Invitados de Teams expuestos a ataques

Una investigación reveló que los atacantes están abusando del Acceso de Invitados B2B en Microsoft Teams para atraer a empleados a entornos externos sin protecciones, donde Microsoft Defender deja de aplicarse. Con solo aceptar una invitación de Teams —que hoy puede enviarse a cualquier correo— las víctimas quedan expuestas a phishing, enlaces maliciosos y exfiltración de datos sin generar alertas. Los atacantes crean inquilinos de bajo nivel de seguridad o de prueba de Microsoft 365 sin seguridad para usarlos como “zonas libres de protección”, explotando así la colaboración B2B para lanzar ataques efectivos.

INFO



ShadyPanda: siete años de malware en navegadores

El grupo ShadyPanda infectó a 4,3 millones de usuarios de Chrome y Edge mediante extensiones que parecían legítimas desde 2018, pero en 2024 recibieron actualizaciones maliciosas. Estas activaron puertas traseras, registrando actividad web, historiales, clics y huellas del navegador, y enviando datos a servidores en China. Extensiones como Clean Master y WeTab fueron las más afectadas. Microsoft eliminó las extensiones tras el reporte, pero la campaña mostró cómo ShadyPanda explotó la falta de monitoreo continuo en las tiendas de extensiones para operar durante años antes de activar sus cargas maliciosas.

INFO

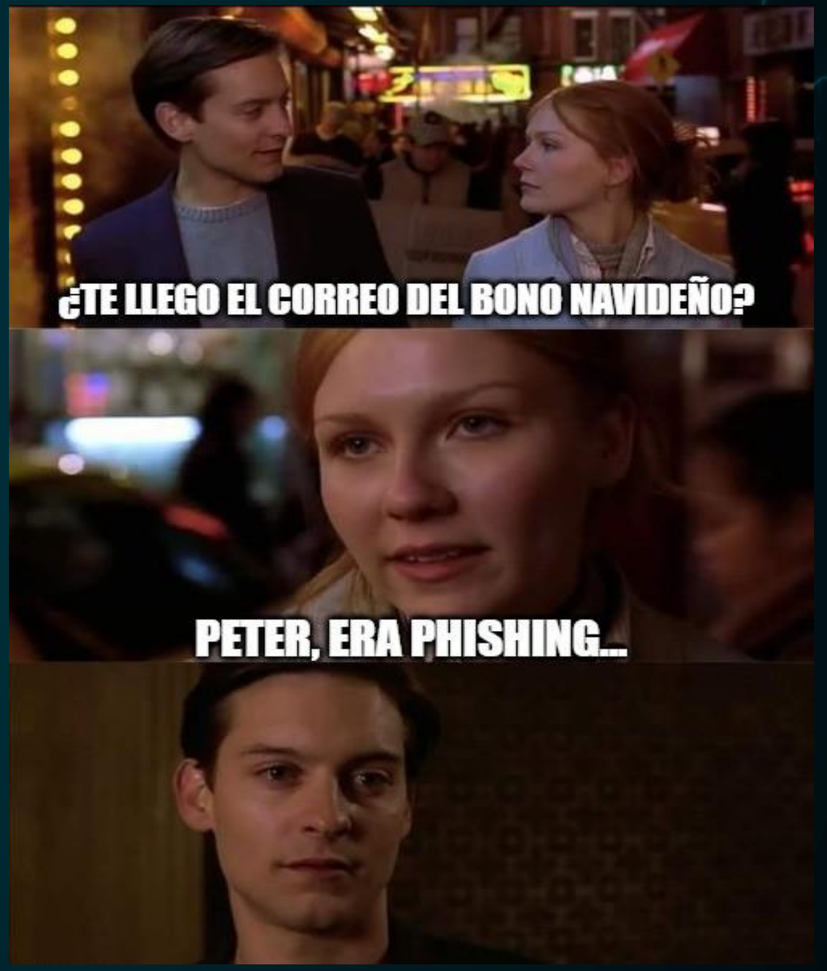
La ciberseguridad empieza por ti: pequeños hábitos, gran impacto

Durante las temporadas festivas, se incrementan los intentos de fraude mediante correos electrónicos que simulan ser comunicaciones legítimas. El objetivo principal es que el usuario haga clic en enlaces maliciosos, entregue credenciales o descargue archivos infectados.

🛡️ Recomendaciones para evitar caer en correos fraudulentos

🎯 Desconfía de mensajes con urgencia o presión emocional.
📧 Revisa el remitente y el dominio real, no solo el nombre visible.
🔗 Antes de hacer clic, verifica la URL pasando el cursor por encima.
📎 No abras archivos adjuntos inesperados, aunque parezcan documentos legítimos.
📞 Confirma por un canal oficial (Talento Humano, Intranet, Mesa de Ayuda).
🔐 Activa y usa 2FA para proteger tus cuentas.
🚨 Reporta inmediatamente cualquier correo sospechoso.

🎁 En épocas festivas aumentan los intentos de fraude disfrazados de “bonos” o “beneficios”. Si un correo parece demasiado bueno para ser verdad, probablemente no lo sea.



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4