

BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

El mayor robo cripto de la historia: Binance sufre un ataque multimillonario

TLP:CLEAR
05.11.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: ⟶ Binance: el mayor robo de criptomonedas de la historia.

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.

Oracle E-Business Suite Workflow Notification Mailer Remote Code Execution Vulnerability

CVE-2026-101809



Critical (10.0)

Impacto: Toma de control remoto.

Resumen: Se identificó una vulnerabilidad en el componente Workflow Notification Mailer de Oracle E-Business Suite, que permite a un atacante remoto no autenticado, mediante el envío de solicitudes HTTP especialmente diseñadas, comprometer el flujo de trabajo y tomar el control del sistema. La explotación puede afectar significativamente la confidencialidad, integridad y disponibilidad, así como impactar otros productos relacionados.

Producto Afectado

- Oracle E-Business Suite, versiones 12.2.3 a 12.2.15.
- Oracle E-Business Suite Workflow Notification Mailer.

Ver +INFO.

Solución:

Actualizar Oracle E-Business Suite a una versión corregida

Ver + INFO.

Fecha de Publicación: 20/OCT/2026 INFO

Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

CVE-2026-20127



Critical (10.0)

Impacto: Evasión de autenticación y escalada de privilegios.

Resumen: Se identificó una vulnerabilidad en Cisco Catalyst SD-WAN que permite a un atacante remoto eludir la autenticación y obtener privilegios elevados, posibilitando la manipulación de la configuración de red. Cisco recomienda actualizar el software a las versiones corregidas.

Producto Afectado

- Cisco Catalyst SD-WAN

Ver +INFO.

Solución:

Actualizar Cisco Catalyst SD-WAN a las versiones corregidas y restringir el acceso mediante firewalls y ACL.

Ver +INFO.

Fecha de Publicación: 28/OCT/2026 INFO

Oracle E-Business Suite Core Remote Code Execution Vulnerability

CVE-2026-101767

Critical (9.8)

Impacto: Ejecución remota de código.

Resumen: Se identificó una vulnerabilidad crítica en Oracle Application Object Library de Oracle E-Business Suite que permite a un atacante remoto no autenticado, mediante HTTP, comprometer la aplicación y tomar el control del componente, afectando la confidencialidad, integridad y disponibilidad del sistema.

Producto Afectado

- Oracle E-Business Suite, versiones 12.2.3 a 12.2.15.
- Oracle Application Object Library

Ver +INFO.

Solución:

Actualizar Oracle E-Business Suite mediante la aplicación de los parches de seguridad oficiales.

Ver +INFO.

Fecha de Publicación: 20/OCT/2026 INFO

ipv4: free inet_opt and ireq_opt after an RCU grace period

CVE-2026-98432

Critical (9.8)

Impacto: Denegación de servicio (DoS) y posible escalada de privilegios.

Resumen: Se identificó una vulnerabilidad en el núcleo de Linux que permite el acceso a memoria previamente liberada debido a una condición de concurrencia en el subsistema IPv4/TCP, pudiendo comprometer la estabilidad y seguridad del sistema.

Producto Afectado

- Linux Kernel

Ver +INFO.

Solución:

Actualizar el núcleo de Linux a una versión que incluya la corrección de seguridad correspondiente

Ver + INFO.

Fecha de Publicación: 24/OCT/2026 INFO

Adobe Security Bulletin

CVE-2026-104351 – CVE-2026-104353
CVE-2026-105780 – CVE-2026-105489

Adobe publicó parches de seguridad para corregir ocho vulnerabilidades críticas en Campaign Classic y una en Adobe Connect, que podrían permitir ejecución de código, elusión de seguridad y escalada de privilegios. Se recomienda actualizar a las versiones corregidas.

Recomendación:

- Aplicar oportunamente las actualizaciones de seguridad de Adobe Campaign Classic y Adobe Connect a las versiones corregidas para mitigar las vulnerabilidades identificadas.

Productos Afectados

Algunos de los productos afectados son:

- Adobe Campaign Classic
- Adobe Connect Deskto
- Adobe Connect Mobile

Ver +INFO

Fecha de Publicación: 27/OCT/2026

INFO

Android Security Bulletin

CVE-2026-58868 – CVE-2026-58857
CVE-2025-22424 – CVE-2025-22426

Google publicó el boletín de seguridad de Android de noviembre de 2026, que corrige más de 200 vulnerabilidades, incluyendo fallos críticos de ejecución remota de código (RCE) sin interacción del usuario, escalada de privilegios y divulgación de información. No se ha reportado explotación activa. Se recomienda instalar los parches disponibles.

Recomendación:

- Actualizar los dispositivos al nivel de parche de seguridad del 5 de noviembre de 2026 o posterior.

Productos Afectados:

Los productos afectados son:

- Android 14, 15, 16 y 17.
- Componentes de hardware de Qualcomm, MediaTek, Arm, Unisoc e Imagination Technologies.

Ver +INFO

Fecha de Publicación: 02/NOV/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
27/10/2026	CVE-2026-111497	Google	9.2	Se identificó una vulnerabilidad de desbordamiento de búfer en Google Brotli que permite a un atacante remoto no autenticado corromper memoria mediante archivos comprimidos manipulados, pudiendo provocar una denegación de servicio, exposición de información sensible o ejecución de código arbitrario.
27/10/2026	CVE-2026-76473	Cisco	9.8	Se identificaron múltiples vulnerabilidades en productos Cisco relacionadas con la neutralización inadecuada de elementos especiales en las salidas de datos (CWE-74), detectadas durante una revisión interna de seguridad. Estas vulnerabilidades podrían afectar la seguridad de los sistemas y son abordadas mediante versiones de software actualizadas.
19/10/2026	CVE-2026-12148	IBM	7.5	Se identificó una vulnerabilidad en IBM MQ Operator debido a una deserialización insegura de Java en las clases MQ para Java, que podría permitir a un atacante autenticado provocar una denegación de servicio (DoS) o ejecutar código arbitrario.
21/10/2026	CVE-2026-109618	PHP	9.2	Se identificó una vulnerabilidad en PHP relacionada con el manejo de errores por falta de memoria (OOM), que puede dejar la memoria de solicitud en un estado no inicializado. Esta condición podría permitir la ejecución remota de código (RCE) mediante solicitudes especialmente diseñadas.
21/10/2026	CVE-2026-109619	PHP	9.2	Se identificó una vulnerabilidad en PHP relacionada con la gestión de estados globales y la memoria de solicitud, que puede dejar referencias a memoria liberada o en un estado obsoleto. Esta condición podría permitir la ejecución remota de código (RCE) mediante solicitudes especialmente diseñadas.

El mayor robo cripto de la historia: Binance sufre un ataque multimillonario

Binance sufrió un incidente de seguridad que habría ocasionado el robo de aproximadamente 6.430 millones de dólares en criptomonedas, considerado el mayor ataque de este tipo registrado hasta la fecha. La investigación apunta al compromiso del portátil de un ingeniero DevOps, que habría permitido acceder a la infraestructura de la plataforma y ejecutar transacciones no autorizadas.

Firmas de inteligencia blockchain atribuyen el ataque, con distintos niveles de confianza, al grupo norcoreano TraderTraitor. Hasta el momento, se han congelado cerca de 3.000 millones de dólares en activos, mientras Binance refuerza sus sistemas de seguridad, colabora con las autoridades y trabaja en la recuperación de los fondos.

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

El ATAQUE

El ataque contra Binance habría comenzado con el compromiso del portátil de un ingeniero DevOps, lo que permitió a los atacantes acceder a un contenedor de servicio y manipular los sistemas de firma de la plataforma para autorizar transacciones de retirada no autorizadas.

Posteriormente, los atacantes ejecutaron transacciones previamente firmadas para transferir grandes cantidades de criptomonedas a billeteras bajo su control, logrando sustraer aproximadamente 6.430 millones de dólares en activos digitales.

Tras el robo, se identificaron movimientos automatizados de fondos entre múltiples direcciones, utilizando intercambios y protocolos DeFi para dificultar su rastreo. Las investigaciones vinculan el incidente con el grupo norcoreano TraderTraitor, aunque la causa raíz del compromiso todavía no ha sido confirmada.

INFO

CONTEXT	INDICATOR	(MD5)
Dominio	Dafnefonseca[.]com	N/A
Dominio	Infodigitalnew[.]com	N/A
SHA256	765a79d22330098884e0f7ce692d61c40dfcf288826342f33d976d8314cfd819	1c7d0ae1c4d2c0b70f75eab856327956
SHA256	867c8b49d29ae1f6e4a7cd31b6fe7e278753a1ba03d4be338ed11fd1efc7dd36	5d43baf1c9e9e3a939e5defd8f8fbd8d
SHA256	89b5e248c222ebf2cb3b525d3650259e01cf7d8fff5e4aa15ccd7512b1e63957	8397ea747d2ab50da4f876a36d673272
SHA256	8acd7c2708eb1119ba64699fd702ebd96c0d59a66cba5059f4e089f4b0914925	9a6307362e3331459d350a201ad66cd9
IPv4	45[.]14[.]227[.]58	N/A



INFO

ÚLTIMAS NOTICIAS



Phishing Skyw4lker en EE. UU.

La campaña de phishing Skyw4lker ataca organizaciones estadounidenses de los sectores de salud, tecnología y manufactura mediante documentos falsos y procesos de autenticación de Microsoft para robar códigos de acceso y comprometer cuentas corporativas. Los atacantes aprovechan servicios legítimos como Google y Microsoft para evitar ser detectados. Para prevenir estos ataques, se recomienda utilizar herramientas Sandbox, inteligencia de amenazas e indicadores de compromiso (IOC) que permitan identificar y bloquear actividades maliciosas a tiempo.

INFO



Estafas de soporte en Teams.

Investigadores de ciberseguridad alertan sobre una campaña de ingeniería social que utiliza chats externos de Microsoft Teams para suplantar al personal de soporte técnico y engañar a los empleados. Los atacantes combinan bombardeos de correos electrónicos, cuentas y dominios falsos para generar confianza y obtener acceso remoto a los equipos mediante herramientas legítimas. Una vez dentro, pueden robar información, moverse por la red corporativa, instalar malware y desplegar ransomware.

INFO



Extensión Claude maliciosa con acceso SSH persistente.

Una versión maliciosa de la extensión Claude Code distribuyó una puerta trasera SSH que permitía a los atacantes acceder remotamente a los equipos de los desarrolladores y mantener el acceso incluso después de reiniciarlos. Además, recopilaba información del sistema y datos sobre posibles credenciales. El incidente pudo afectar hasta 5.000 usuarios de Cursor. Se recomienda eliminar los archivos maliciosos, revisar las claves SSH, cambiar las credenciales y aislar los equipos comprometidos.

INFO

Hackear la confianza es más fácil que hackear un sistema.

En ciberseguridad, los atacantes buscan aprovechar cualquier oportunidad para engañar a los usuarios, utilizando técnicas que parecen inofensivas o legítimas. Muchas veces, mientras el atacante identifica pequeños detalles para encontrar una vulnerabilidad, la víctima confía sin verificar y termina facilitando el acceso a su información.

🎭 La confianza puede ser una vulnerabilidad: no debemos asumir que toda solicitud proviene de una fuente legítima.

📩 Los detalles hacen la diferencia: un correo puede parecer auténtico, pero esconder intenciones maliciosas.

🧠 El conocimiento no siempre es suficiente: saber de ciberseguridad no nos hace inmunes a los engaños.

🔐 Verificar es proteger: antes de hacer clic, responder o compartir información, debemos comprobar la autenticidad de la solicitud.

🚨 El atacante busca el mínimo descuido: una pequeña distracción puede convertirse en una gran brecha de seguridad.

En ciberseguridad, la mayor ventaja del atacante puede ser nuestra confianza y la mejor defensa siempre será nuestra capacidad de cuestionar.



ISO/IEC 27001 • ISO/IEC 20000-1

LL-C (Certification)

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4

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