BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Piratas informáticos de Crimson Collective apuntan a la nube de AWS para el robo de datos

TLP:CLEAR
15.10.2025

CLICK PARA EMPEZAR

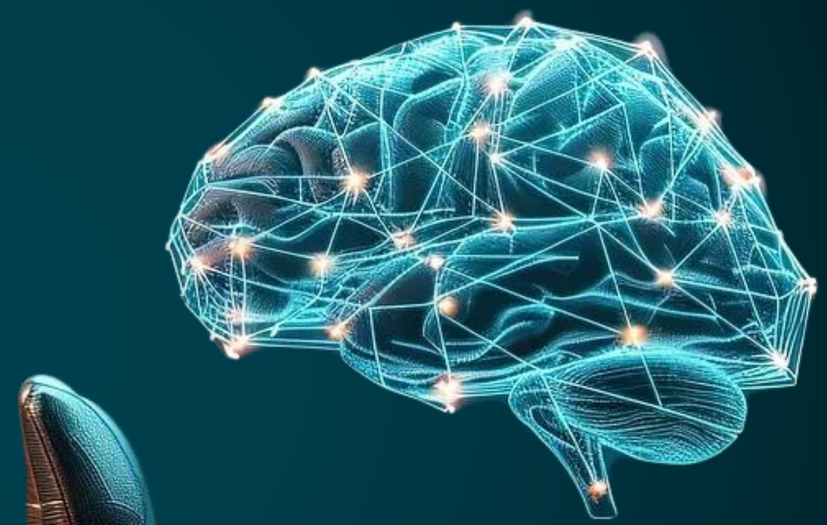
CYBERSOCDTS

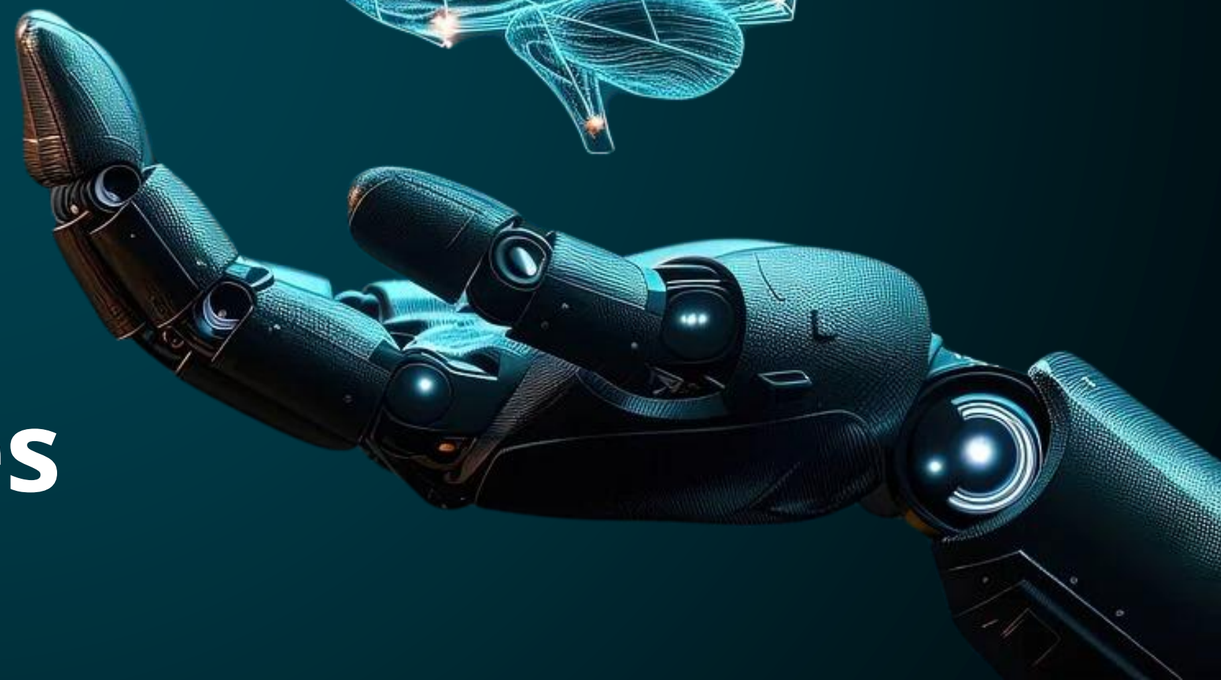
En esta edición: → Piratas informáticos de Crimson Collective apuntan la nube de AWS para el robo de datos

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.

Vulnerabilidad en productos Oracle

CVE-2025-61882

critical (9.8)

Impacto: Acceso no autorizado.

Resumen: Esta vulnerabilidad se puede explotar remotamente sin autenticación; es decir, a través de una red sin necesidad de nombre de usuario ni contraseña. Si se explota con éxito, puede provocar la ejecución remota de código.

Versiones Afectadas

Las versiones compatibles afectadas son:

- 12.2.3
- 12.2.14

Ver +INFO.

Solución:

Oracle recomienda a sus clientes que apliquen las actualizaciones proporcionadas por esta alerta lo antes posible.

Ver +INFO.

Fecha de Publicación: 05/OCT/2025 INFO

AION Business Rules Expert r11.0 for Linux Apache struts library Vulnerability

CVE-2012-0391

Critical (9.8)

Impacto: Ejecutar código o comandos no autorizados.

Resumen: Una vulnerabilidad interpreta los valores de los parámetros como expresiones OGNL durante el manejo de ciertas excepciones para tipos de datos de propiedades no coincidentes, lo que permite a los atacantes remotos ejecutar código Java arbitrario a través de un parámetro diseñado.

Versiones Afectadas

La versión compatible afectada es:

- AION Business Rules Expert para Linux 11.0.

Ver +INFO.

Solución:

Estas vulnerabilidades se han corregido eliminando puntales en la última versión 203.

Ver +INFO.

Fecha de Publicación: 6/OCT/2025 INFO

Weak authentication in WAD/GUI

CVE-2025-49201

High (7.4)

Impacto: Ejecutar código o comandos no autorizados.

Resumen: Una vulnerabilidad de autenticación débil en FortiPAM y FortiSwitch Manager WAD/GUI puede permitir a un atacante eludir el proceso de autenticación a través de un ataque de fuerza bruta.

Versiones Afectadas

- FortiPAM 1.5.0
- FortiPAM 1.4.0 a 1.4.2
- FortiPAM 1.3 todas las versiones
- FortiPAM 1.2 todas las versiones
- FortiPAM 1.1 todas las versiones
- FortiPAM 1.0 todas las versiones
- Administrador de conmutadores Forti de 7.2 a 7.2.4

Ver +INFO.

Solución:

- Actualice a 1.5.1 o superior
- Actualice a 1.4.3 o superior
- Migrar a una versión fija
- Migrar a una versión fija
- Migrar a una versión fija
- Migrar a una versión fija
- Actualice a 7.2.5 o superior

Ver +INFO.

Fecha de Publicación: 14/OCT/2025 +INFO

Restricted CLI command bypass

CVE-2025-58325

High (7.8)

Impacto: Escalada de privilégios.

Resumen: Una vulnerabilidad de provisión incorrecta de funcionalidad especificada [CWE-684] en FortiOS puede permitir que un atacante local autenticado ejecute comandos del sistema a través de comandos CLI diseñados específicamente.

Versiones Afectadas

- FortiOS 7.6.0
- FortiOS de 7.4.0 a 7.4.5
- FortiOS de 7.2.0 a 7.2.10
- FortiOS de 7.0.0 a 7.0.15
- FortiOS 6.4 todas las versiones

Ver +INFO.

Solución:

- Actualizar a 7.6.1 o superior
- Actualizar a 7.4.6 o superior
- Actualizar a 7.2.11 o superior
- Actualizar a 7.0.16 o superior
- Migrar a una versión fija

Ver +INFO.

Fecha de Publicación: 14/OCT/2025 +INFO

Actualización de Google Chrome soluciona varias fallas críticas de seguridad

CVE-2024–45491, CVE-2024–45492,CVE-2025-0838

Google ha publicado una actualización crítica para su navegador Chrome, destinada a corregir tres vulnerabilidades que afectan componentes clave del navegador.

Recomendación:
Actualizar inmediatamente todos los sistemas que utilicen versiones vulnerables de Google Chrome.

Versiones Afectadas

- Google Chrome en versiones anteriores a 141.0.7390.65/.66 para Windows y macOS.
- Google Chrome en versiones anteriores a 141.0.7390.65 para Linux.

Ver +INFO

Fecha de Publicación: 09/OCT/2025 INFO

Actualizaciones de Microsoft corrigen 6 vulnerabilidades de Zero-Day y 172 fallos

CVE-2025-59205, CVE-2025-59203, CVE-2025-59190

Microsoft ha publicado actualizaciones de seguridad para 172 fallas, incluidas seis de vulnerabilidades de día cero, aborda ocho vulnerabilidades "críticas", cinco de las cuales son vulnerabilidades de ejecución remota de código y tres son vulnerabilidades de elevación de privilegios.

Recomendación:
Actualizar a la última versión disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

- Windows 11 versión 25H2, 24H2, 23H2, 22H2
- Windows 10 versión 1607, 22H2, 1607
- Windows server 2016, 2025, 2008

Ver +INFO

Fecha de Publicación: 14/OCT/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
8/10/2025	CVE-2025-36636	Tenable	4.3	Vulnerabilidad de control de acceso inadecuado en la que un usuario autenticado podría acceder a áreas fuera de su alcance autorizado.
1/10/2025	CVE-2025-20356	Cisco	5.4	Vulnerabilidades en la interfaz de administración basada en web de Cisco Cyber Vision Center podrían permitir que un atacante remoto autenticado lleve a cabo ataques de cross-site scripting (XSS) contra un usuario de dicha interfaz.
1/10/2025	CVE-2025-59230	Windows	7.8	Vulnerabilidad de elevación de privilegios del Administrador de conexiones de acceso remoto de Windows permite a un atacante autorizado elevar los privilegios localmente.
14/10/2025	CVE-2025-24990	Windows	7.8	Vulnerabilidad de elevacion de privilegios del controlador de modem de Windows Agere.
2/10/2025	CVE-2024-26008	Fortinet	5.0	Vulnerabilidad de verificación o manejo inadecuado de condiciones excepcionales en el demonio fgfm de FortiOS, FortiProxy, FortiPAM y FortiSwitchManager puede permitir que un atacante no autenticado restablezca repetidamente la conexión fgfm a través de solicitudes TCP cifradas con SSL diseñadas.
14/10/2025	CVE-2025-57740	Fortinet	6.7	Vulnerabilidad de desbordamiento de búfer basada en la conexión de marcadores RDP de FortiOS, FortiPAM y FortiProxy puede permitir que un usuario autenticado ejecute código no autorizado a través de solicitudes diseñadas.
14/10/2025	CVE-2024-50571	Fortinet	6.5	Vulnerabilidad de desbordamiento de búfer basada en el daemon fgfmd de FortiOS, FortiManager, FortiAnalyzer, FortiManager Cloud, FortiAnalyzer Cloud y FortiProxy puede permitir que un atacante autenticado ejecute código o comandos arbitrarios a través de solicitudes específicamente diseñadas.
14/10/2025	CVE-2025-22258	Fortinet	5.7	Vulnerabilidad de desbordamiento de búfer basada en el daemon nodejs FortiOS, FortiProxy, FortiPAM, FortiSRA y FortiSwitchManager puede permitir que un atacante autenticado ejecute código o comandos arbitrarios a través de solicitudes específicamente diseñadas.
14/10/2025	CVE-2025-54822	Fortinet	4.2	Vulnerabilidad de autorización indebida en FortiOS y FortiProxy puede permitir que un atacante autenticado acceda a archivos estáticos de otros VDOM a través de solicitudes HTTP o HTTPS diseñadas.

Piratas informáticos de Crimson Collective apuntan la nube de AWS para el robo de datos

El grupo de amenazas 'Crimson Collective' ha estado apuntando a los entornos de nube de AWS durante las últimas semanas, para robar datos y extorsionar a las empresas.

Un análisis de los investigadores de Rapid7 proporciona más información sobre la actividad de Crimson Collective, que implica comprometer las claves de acceso de AWS a largo plazo y las cuentas de administración de identidad y acceso (IAM) para la escalada de privilegios. Los atacantes utilizan la herramienta de código abierto TruffleHog para descubrir credenciales de AWS expuestas y así obtener acceso.

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

El ATAQUE

Después de obtener acceso, crean nuevos usuarios de IAM y perfiles de inicio de sesión a través de llamadas API y generan nuevas claves de acceso. Luego viene la escalada de privilegios al adjuntar la política 'AdministratorAccess' a los usuarios recién creados, lo que otorga a Crimson Collective el control total de AWS. Los actores de amenazas aprovechan este nivel de acceso para enumerar usuarios, instancias, depósitos, ubicaciones, clústeres de bases de datos y aplicaciones, para planificar la fase de recopilación y exfiltración de datos.
Modifican las contraseñas maestras de Relational Database Service para obtener acceso a la base de datos, crear instantáneas y, a continuación, exportarlas a Simple Storage Service para su exfiltración a través de llamadas API. Después de completar este paso, Crimson Collective envía a las víctimas una nota de extorsión a través de AWS Simple Email Service dentro del entorno de nube vulnerado, así como a cuentas de correo electrónico externas.

INFO

CONTEXT	INDICATOR	(MD5)
IP	195.201.175.210	N/A
IP	45.148.10.141	N/A
IP	5.9.108.250	N/A
IP	45.61.151.33	N/A
IP	144.172.103.208	N/A
IP	144.172.98.81	N/A
IP	145.223.69.212	N/A
URL	http://144[.]172[.]103.208[:]1194/	N/A
URL	http://144[.]172[.]98[.]81[:]49/	N/A
URL	http://145[.]223[.]69[.]212[:]2012/	N/A
URL	http://172[.]86[.]96[.]67[:]32132/	N/A
URL	http://174[.]138[.]184[.]252[:]61243/	N/A
URL	http://174[.]138[.]184[.]252[:]9109/	N/A
URL	http://45[.]61[.]151[.]33[:]32132/	N/A
URL	http://83[.]147[.]19[.]208[:]32132/	N/A

INFO

ÚLTIMAS NOTICIAS

Suplantando a Davivienda

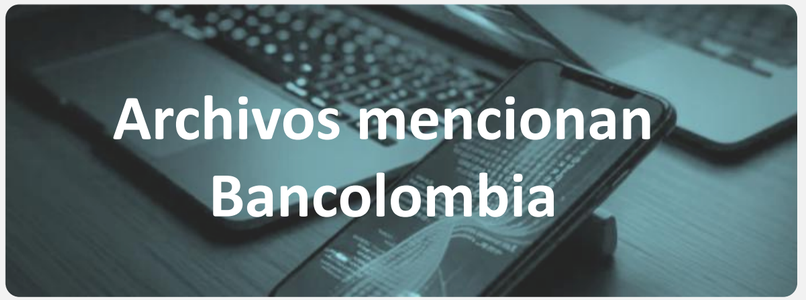
Se ha detectado un mensaje de texto falso que suplanta al banco Davivienda, ofreciendo el canje de puntos que supuestamente vencen el mismo día. El mensaje incluye un enlace a un sitio web fraudulento que busca robar datos personales y bancarios de los usuarios. Recibes un mensaje de texto que parece ser de Davivienda sobre puntos que vencen el mismo día, al hacer clic en el enlace, te piden ingresar datos personales y bancarios, los estafadores capturan esta información para realizar transacciones fraudulentas.

INFO

Filtración de Red Hat

Ciber extorsionadores aseguran haber obtenido los planos, configuraciones y secretos técnicos que sostienen los sistemas informáticos de algunas de las instituciones más vitales de Colombia. Si esos documentos son auténticos, el país enfrenta una exposición de alto riesgo: los atacantes no solo podrían interrumpir servicios, sino también manipularlos desde adentro, habilita ataques dirigidos: explotación de vulnerabilidades, movimientos laterales, interrupción de servicios y exfiltración (Robo) masivo de datos.

INFO



Archivos mencionan Bancolombia

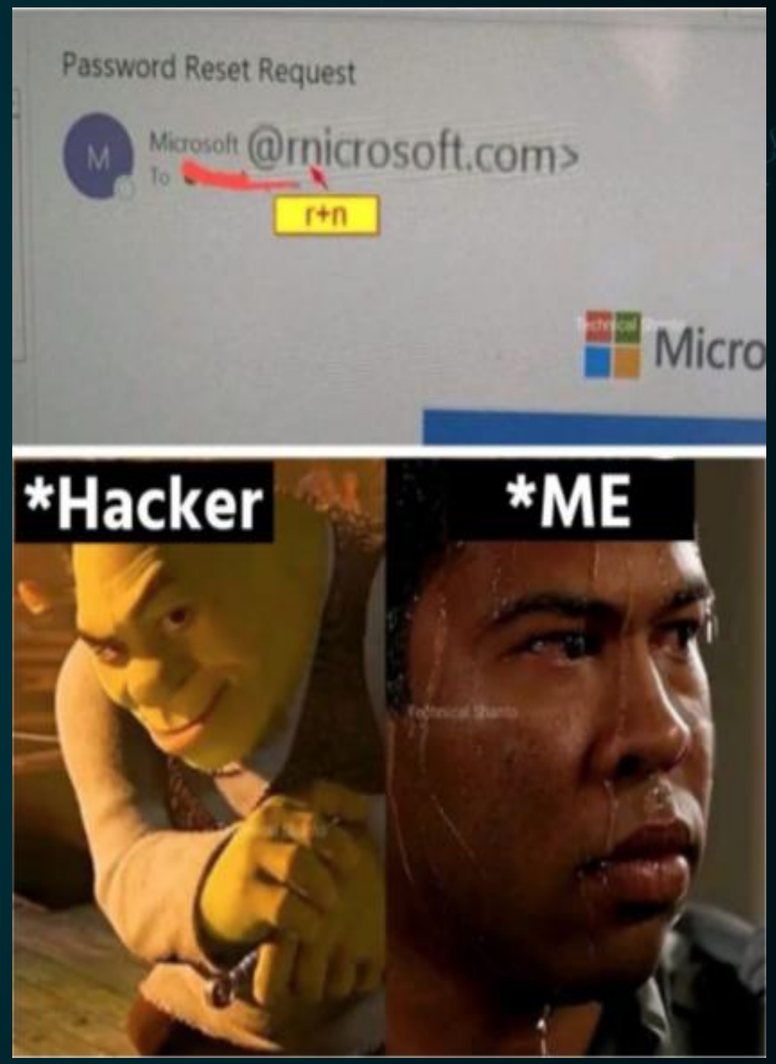
El grupo de extorsión Crimson Collective ha afirmado haber vulnerado una instancia de GitLab de Red Hat Consulting, resultando en la supuesta sustracción de 570 GB de datos internos, lo que ha generado una alerta de ciberseguridad que impacta a nivel global.
Los atacantes mostraron como parte de sus evidencias la estructura jerárquica de carpetas y archivos que habrían robado. Entre ellas aparecen las carpetas bancolombia-rdne y banco-fie (Banco FIE) es la prueba visual que afirma que la información sensible de proyectos relacionados con estas entidades colombianas y bolivianas fue robada.

INFO

No confíes en todo lo que llega a tu bandeja de entrada

No basta con tener filtros de correo o antivirus instalados. La verdadera protección comienza con la conciencia del usuario y la verificación detallada de cada mensaje recibido. El phishing evoluciona constantemente y puede engañar hasta a los ojos más entrenados. La clave está en identificar señales sospechosas antes de caer en la trampa.

🔍 Verifica el remitente: presta atención a detalles sutiles como letras cambiadas (rnicrosoft.com en lugar de microsoft.com). Los atacantes imitan direcciones legítimas para ganar tu confianza.
🚫 No respondas ni hagas clic inmediatamente: si el mensaje pide acciones urgentes o te presiona emocionalmente, es una bandera roja 🚩.
✉️ Revisa la redacción del correo: errores ortográficos, frases genéricas o lenguaje inusual pueden indicar que no proviene de una fuente confiable.
📞 Confirma por canales oficiales: si tienes dudas, contacta directamente a la empresa o área de soporte, nunca respondas desde el mismo correo sospechoso.
🛡️ Reporta el intento: notificar al área de seguridad ayuda a prevenir que otros usuarios caigan en el mismo engaño.
📌 Con estas prácticas, se fortalece la primera línea de defensa: el usuario. El phishing no solo busca robar contraseñas, también puede ser la puerta de entrada a ataques más complejos como el ransomware, robo de identidad o compromiso de cuentas (account takeover).



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4