BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

BlindEagle apunta a entidades del gobierno colombiano junto con Caminho y DCRAT

TLP:CLEAR
29.12.2025

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → BlindEagle apunta a entidades del gobierno colombiano junto con Caminho y DCRAT

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.

Remote Code Execution Vulnerability in React and Next.js Frameworks

CVE-2025-55182

Critical (10.0)

Impacto: Ejecución arbitraria de código

Resumen: Permite a un atacante remoto y no autenticado enviar una petición HTTP especialmente diseñada a un servidor que use React Server Components vulnerables, y hacer que el servidor ejecute código malicioso con los privilegios del proceso de la aplicación.

Versiones Afectadas

Algunas de las versiones compatibles afectadas son:

- React-server-dom-webpack: 19.0.0, 19.1.0, 19.1.1, 19.2.0
- react-server-dom-parcel: 19.0.0, 19.1.0, 19.1.1, 19.2.0

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: 17/DIC/2025 INFO

Azure Container Apps Remote Code Execution Vulnerability

CVE-2025-65037

Critical (10.0)

Impacto: Ejecución arbitraria de código

Resumen: Permite que un atacante remoto inyecte y ejecute código malicioso en entornos de Azure Container Apps, con riesgo de control total del servicio, acceso a datos sensibles y pérdida de disponibilidad de aplicaciones.

Productos Afectadas

Los productos compatibles afectados son:

- Microsoft Azure Container Apps

Ver +INFO.

Solución:

Actualizar todos los entornos de Azure Container Apps con los parches más recientes.

Ver +INFO.

Fecha de Publicación: 18/DIC/2025 INFO

Out of bounds memory access in ANGLE

CVE-2025-14174

High (8.8)

Impacto: Ejecución remota de código

Resumen: Permite a un atacante remoto ejecutar código malicioso cuando un usuario visita una página web especialmente diseñada. La vulnerabilidad se debe a un acceso incorrecto a la memoria, que puede causar corrupción, inestabilidad del navegador y toma de control del sistema afectado.

Versiones Afectadas

Algunas de las versiones compatibles afectadas son:

- Chrome en Mac desde 143.0.7499.110 antes del 143.0.7499.110

Ver +INFO.

Solución:

Google Chrome ≥ 143.0.7499.110 o superior. Actualizar cualquier navegador basado en Chromium (Edge, Opera, etc.) a su versión más reciente disponible.

Ver +INFO.

Fecha de Publicación: 10/DIC/2025 INFO

Cisco Secure Email Gateway y Cisco Secure Email and Web Manager

CVE-2025-20393

Critical (10.0)

Impacto: Ejecución remota de código

Resumen: Permite a un atacante ejecutar código malicioso y manipular datos en los sistemas afectados. Esta falla puede ser explotada de forma remota, poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información.

Productos Afectados

Los productos compatibles afectados son:

- Cisco Secure Email Gateway (SEG)
- Cisco Secure Email and Web Manager (SEWM)

Ver +INFO.

Solución:

Seguir las recomendaciones de Cisco Talos y de su centro de respuesta a incidentes (PSIRT) para cubrir entornos afectados

Ver +INFO.

Fecha de Publicación: 17/DIC/2025 INFO

IBM Patches Over 100 Vulnerabilities

CVE-2025-48913 - CVE-2025-53057 - CVE-2025-53066 - CVE-2025-53066

IBM lanzó parches para corregir más de 100 vulnerabilidades en una amplia gama de sus productos de software. La mayoría de estos fallos resueltos incluían vulnerabilidades críticas o de alta severidad, muchas de las cuales estaban relacionadas con dependencias de terceros dentro de los productos.

Recomendación:
IBM publica las actualizaciones en su portal de boletines de seguridad y Fix Central; estas deben ser instaladas en cuanto se evalúe su impacto.

Producto Afectado

El producto afectado es:

- IBM Storage Defender
- IBM Guardium Data Protection
- IBM Maximo Application Suite
- IBM Edge Data Collector

Ver +INFO

Fecha de Publicación: 12/DIC/2025 INFO

Nessus Versions 10.11.1 and 10.9.6 Fix Multiple Vulnerabilities

CVE-2025-49796 - CVE-2025-59375 CVE-2025-49794 - CVE-2024-8176

Tenable ha remediado múltiples vulnerabilidades en el producto Nessus actualizando componentes subyacentes de terceros como expat, libxml2 y libxslt, que presentaban fallos de seguridad como agotamiento de recursos, errores de lógica y otros fallos fueron abordados al actualizar estos componentes a versiones más seguras.

Recomendación:
Actualiza Tenable Nessus a las versiones 10.9.6 o 10.11.1 para corregir vulnerabilidades en componentes de terceros y proteger tu entorno.

Producto Afectado:

Los productos afectados son:

- Versiones anteriores a 10.9.6 y 10.11.1 son vulnerables debido a bibliotecas de terceros con fallos conocidos.

Ver +INFO

Fecha de Publicación: 22/DIC/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
19/12/2025	CVE-2025-13780	pgAdmin 4	8.8	Permite a un atacante inyectar y ejecutar comandos arbitrarios en servidores que restauran volcamientos PLAIN maliciosos, con una severidad crítica.
23/12/2025	CVE-2025-14847	MongoDB	8.7	Permite a un atacante remoto, sin autenticación, inducir a un servidor MongoDB vulnerable a devolver partes de memoria interna que podrían contener información sensible, simplemente con enviar solicitudes malformadas que abusen del manejo de compresión Zlib.
23/12/2025	CVE-2025-65041	Microsoft	10.0	Permite a un atacante saltarse las restricciones de acceso y obtener permisos superiores en Microsoft Partner Center, potencialmente comprometiendo datos o funciones administrativas de la plataforma.
22/12/2025	CVE-2025-68613	N8N	10.0	Permite a un atacante comprometer totalmente un entorno de workflow automation con n8n, afectando confidencialidad, integridad y disponibilidad de la plataforma y servidores asociados.
9/12/2025	CVE-2025-62562	Microsoft Outlook	7.8	Permite a un atacante ejecutar código arbitrario en una instalación vulnerable de Microsoft Outlook con interacción del usuario, lo que podría comprometer el sistema afectado.
10/12/2025	CVE-2024-40593	Fortinet	5.9	Permite a un atacante con acceso administrativo extraer claves privadas de certificados de dispositivos Fortinet vulnerables, lo que puede comprometer la confidencialidad de comunicaciones y la seguridad de la infraestructura.
15/12/2025	CVE-2025-13945 / CVE-2025-13946	Wireshark	5.5	Permiten a un atacante impactar en la disponibilidad de Wireshark al provocar fallos o bloqueos (denial of service).

BlindEagle apunta a una agencia del gobierno colombiano junto con Caminho y DCRAT

BlindEagle es un grupo de amenazas cibernéticas enfocado en instituciones gubernamentales en Colombia. En una campaña descubierta por Zscaler ThreatLabz, este actor empleó phishing interno para comprometer cuentas de correo y enviar mensajes maliciosos desde direcciones oficiales, evadiendo controles como DMARC, DKIM y SPF.

La campaña evidencia la evolución de sus tácticas, técnicas y procedimientos (TTP), pasando de malware simple a cadenas multietapa con ofuscación, uso de servicios legítimos (como Discord) y múltiples cargas útiles. Investigadores destacan que BlindEagle perfecciona su arsenal con herramientas como Caminho (downloader) y DCRAT (troyano de acceso remoto) para lograr persistencia y control en sistemas comprometidos.

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

El ATAQUE

La operación consistió en una campaña bien diseñada en múltiples fases que comenzó con spear-phishing interno, utilizando una cuenta comprometida para que el correo pareciera legítimo dentro de Microsoft 365. El mensaje incluía un SVG interactivo que, al abrirse, mostraba una página falsa destinada a engañar al usuario y ejecutar JavaScript oculto. Este script activaba un comando de PowerShell directamente en memoria, sin escribir en disco, lo que daba paso a la descarga de un downloader llamado Caminho, encargado de obtener la carga final desde un servidor externo, en este caso mediante un enlace alojado en Discord. La etapa final fue la implantación de DCRAT, un troyano de acceso remoto que permite control del sistema, evasión de detección y persistencia. En conjunto, la campaña evidencia la evolución de BlindEagle hacia ataques más complejos, con cadenas de malware multicapa que combinan esteganografía, ofuscación avanzada y el abuso de servicios legítimos para evadir los controles tradicionales.

+ INFO

CONTEXT	INDICATOR	(MD5)
IPv4	181[.]206[.]158[.]190	N/A
IPv4	74[.]124[.]24[.]240	N/A
Microsoft.Win32.Task Scheduler.dll	c208d8d0493c60f14172acb4549dcb394d2b92d30bcae4880e66df3c3a7100e4	9799484e3942a6692be69aec1093cb6c
Client.exe	e7666af17732e9a3954f6308bc52866b937ac67099faa212518d5592baca5d44	97adb364d695588221d0647676b8e565
AGT27.txt	d139bfe642f3080b461677f55768fac1ae1344e529a57732cc740b23e104bff0	bbb99dfd9bf3a2638e2e9d13693c731c
3OZFA_AUTO ADMISORIO DEMANDA LABORAL RADICADO No FGN 2025 339	8f3dc1649150961e2bac40d8dabe5be160306bcaaa69ebe040d8d6e634987829	d80237d48e1bbc2fdda741cbf006851a
Hostname	startmenuexperiencehost.ydns.eu	N/A

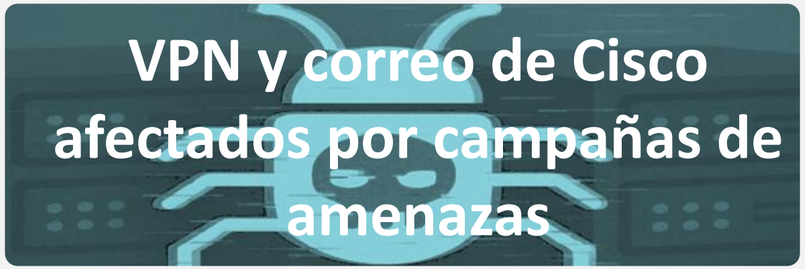
INFO

ÚLTIMAS NOTICIAS

ConsentFix secuestra cuentas de Microsoft vía Azure CLI

ConsentFix, variante de ataque que secuestra cuentas de Microsoft mediante Azure CLI sin requerir contraseñas ni evadir autenticación multifactor (MFA). Identificado por Push Security como evolución de ClickFix, usa ingeniería social para guiar a las víctimas en el flujo OAuth 2.0 de Azure CLI, capturar el código de autorización y obtener un token de acceso con control total. La campaña emplea páginas comprometidas con un falso Cloudflare Turnstile CAPTCHA y redirige a los usuarios a copiar una URL de localhost con el código OAuth en sitios maliciosos. Esta técnica explota una aplicación OAuth de primera parte (Azure CLI), difícil de bloquear, y evade controles tradicionales, representando un riesgo crítico para cuentas empresariales y personales.

INFO



VPN y correo de Cisco afectados por campañas de amenazas

Un grupo APT vinculado a China, explotó una vulnerabilidad zero-day crítica en Cisco Secure Email Gateway y Secure Email and Web Manager con AsyncOS, permitiendo privilegios root y ejecución de comandos arbitrarios, además de desplegar AquaShell, AquaTunnel y AquaPurge. Cisco emitió una advisory con mitigaciones temporales, sin parche disponible aún. Paralelamente, una campaña de fuerza bruta atacó VPNs SSL de Cisco y GlobalProtect de Palo Alto Networks con millones de intentos de autenticación (credential stuffing) contra contraseñas débiles o comprometidas. Investigadores recomiendan auditorías de dispositivos perimetrales, contraseñas reforzadas y autenticación multifactor (MFA).

INFO

Hackers convierten Nezha en troyano encubierto

Atacantes abusan de la herramienta de código abierto Nezha para usarla como Remote Access Trojan (RAT) y tomar control de sistemas comprometidos. Nezha, legítima para monitorización de servidores, pasa desapercibida en productos de seguridad (0/72 detecciones en VirusTotal). Los atacantes instalan su agente y lo reutilizan como RAT, obteniendo acceso SYSTEM/root, ejecución de comandos y gestión de archivos. Su tráfico usa protocolos web estándar, mezclándose con tráfico legítimo y evadiendo detección. Este abuso refleja la tendencia de aprovechar software legítimo para post-exploitation y persistencia, lo que exige detección basada en comportamiento y monitoreo contextual.

INFO

La amenaza invisible entre tú y tu destino

Un ataque Man-In-The-Middle (MITM) ocurre cuando un atacante intercepta y modifica la comunicación entre dos dispositivos sin que lo detecten, robando o manipulando información. A continuación, algunas recomendaciones:

🛡️ La seguridad física también es clave para proteger nuestras redes.

🎯 Asegura físicamente los equipos: mantén cerrados y controlados los gabinetes de red.

📧 Usa cifrado: protege las comunicaciones con protocolos seguros como TLS y VPN.

🔗 Monitorea la red: detecta actividades sospechosas con herramientas IDS.

☝️ Haz revisiones periódicas: evita la entrada de animales o intrusos que dañen el equipo.

La seguridad digital y física van de la mano. Protégete contra ataques MITM y también contra riesgos físicos inesperados como un “ratón en medio”.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4