BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

“Fantasy Hub” usa Telegram para difundir su troyano Android

TLP:CLEAR
18.11.2025

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → Troyano Android 'Fantasy Hub' convierte a Telegram en un centro para piratas informáticos

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.

Cisco Secure FTD and ASA VPN Web Server Remote Code Execution Vulnerability

CVE-2025-20333

Critical (9.9)

Impacto: Ejecución de código arbitrario.

Resumen: Esta vulnerabilidad en el servidor web VPN del software Cisco Secure Firewall Adaptive Security Appliance (ASA) y del software Cisco Secure Firewall Threat Defense (FTD) podría permitir a un atacante remoto autenticado ejecutar código arbitrario en un dispositivo afectado.

Versiones Afectadas

Las versiones compatibles afectadas son:

- Cisco Secure ASA
- Cisco Secure FTD

Ver +INFO.

Solución:

Cisco recomienda que todos los clientes actualicen a las versiones de software fijo.

Ver + INFO.

Fecha de Publicación: 06/NOV/2025 INFO

Cisco Unified Contact Center Express Remote Code Execution Vulnerabilities

CVE-2025-20354 - CVE-2025-20358

Critical (9.8)

Impacto: Escalada de privilégios.

Resumen: Permite que un atacante remoto no autenticado cargue archivos arbitrarios, omita la autenticación, ejecute comandos arbitrarios y eleve los privilegios a root.

Versiones Afectadas

La versión compatible afectada es:

- Cisco Unified CCX

Ver +INFO.

Solución:

Aplicar la actualización de software lanzada por cisco.

Ver +INFO.

Fecha de Publicación: 13/NOV/2025 INFO

Path confusion vulnerability in GUI

CVE-2025-64446

High (9.1)

Impacto: Control de acceso inadecuado.

Resumen: Esta vulnerabilidad de recorrido de ruta relativa [CWE-23] en FortiWeb podría permitir a un atacante no autenticado ejecutar comandos administrativos en el sistema a través de solicitudes HTTP o HTTPS manipuladas.

Versiones Afectadas

- FortiWeb 8.0 – 8.0.0 a 8.0.1
- FortiWeb 7.6 – 7.6.0 a 7.6.4
- FortiWeb 7.4 – 7.4.0 a 7.4.9
- FortiWeb 7.2 – 7.2.0 a 7.2.11
- FortiWeb 7.0 – 7.0.0 a 7.0.11

Ver +INFO.

Solución:

- Actualizar a v8.0.2 o superior
- Actualizar a la v7.6.5 o superior
- Actualizar a la v7.4.10 o superior
- Actualizar a la v7.2.12 o superior
- Actualizar a la v7.0.12 o superior

Ver +INFO.

Fecha de Publicación: 14/NOV/2025 INFO

Zoom Workplace Clients - Inefficient Regular Expression Complexity

CVE-2025-62484

High (8.1)

Impacto: Escalada de privilegios.

Resumen: La complejidad ineficaz de las expresiones regulares en determinados clientes de Zoom puede permitir que un usuario no autenticado lleve a cabo una escalada de privilegios a través del acceso a la red.

Versiones Afectadas

Las versiones compatibles afectadas son:

- Zoom Workplace para iOS antes de la versión 6.5.10 y Android antes de la versión 6.5.10
- SDK de Zoom Meeting para iOS antes de la versión 6.5.10 y Android antes de la versión 6.5.10

Ver +INFO.

Solución:

Aplicar las ultimas actualizaciones disponibles en el sitio oficial.

Ver +INFO.

Fecha de Publicación: 11/NOV/2025 INFO

Actualización de Microsoft

CVE-2025-62215 - CVE-2025-60724
CVE-2025-62220 - CVE-2025-60704

Microsoft lanzo parches para 63 nuevas vulnerabilidades de seguridad, 4 críticas y 59 importantes en gravedad. 29 de escalada de privilegios, 16 ejecuciones remotas de código, 11 de divulgación de información, tres de denegación de servicio (DoS), dos de omisión de funciones de seguridad y dos errores de suplantación de identidad.

Recomendación:
Aplicar los parches de seguridad, disponibles en la pagina de Microsoft

Versiones Afectadas

Las versiones compatibles afectadas son:

- SQL Server
- Agente de Azure Monitor
- Microsoft Office Excel y Word

Ver +INFO

Fecha de Publicación: 11/NOV/2025 INFO

Actualización de Google

CVE-2025-12725 - CVE-202512726
CVE-2025-12727 - CVE-2025-12728
CVE-2025-12729

Google ha lanzado una actualización de seguridad de emergencia para su navegador Chrome, abordando cinco vulnerabilidades que podrían permitir a atacantes ejecutar código malicioso de forma remota. Esta actualización corrige fallas que afectan componentes centrales como WebGPU, el motor JavaScript V8 y la barra de direcciones Omnibox.

Recomendación:
Aplicar las actualizaciones disponibles.

Producto Afectado:

Los productos afectados son:

- Google Chrome en sus versiones anteriores a la 142.0.7444.134/.135 para Windows, 142.0.7444.135
- Para macOS 142.0.7444.135, para Linux 142.0.7444.134

Ver +INFO

Fecha de Publicación: 05/NOV/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
3/11/2025	CVE-2025-24477	Fortinet	4.0	Permitir que un atacante autenticado ejecute código o comandos arbitrarios a través de solicitudes especialmente diseñadas.
4/11/2025	CVE-2025-58189	Tenable	5.3	Cuando falla el protocolo de enlace de conexión durante la negociación ALPN, el error contiene información controlada por el atacante (los protocolos ALPN enviados por el cliente) que no se escapa.
6/11/2025	CVE-2025-20362	Cisco	6.5	Puede provocar que los dispositivos sin parchear se reinicien inesperadamente, lo que genera una denegación de servicio (DoS).puede provocar que los dispositivos sin parchear se reinicien inesperadamente, lo que genera una denegación de servicio (DoS).
4/11/2025	CVE-2025-23358	Nvidia	8.2	Permite a un atacante local provocar un error en la ruta de búsqueda, podría ejecutarse código y escalar privilegios.
1/11/2025	CVE-2025-11833	WordPress	9.8	Permite el acceso no autorizado de datos debido a la falta de una comprobación de capacidad en la función.
11/11/2025	CVE-2025-59499	Microsoft	7.7	Permite a un atacante autorizado elevar privilegios a través de una red.

“Fantasy Hub” usa Telegram para difundir su troyano Android

Fantasy Hub es un nuevo troyano de acceso remoto (RAT) para Android vendido en canales rusoparlantes de Telegram bajo un modelo de Malware-as-a-Service. Permite a los atacantes tomar control del dispositivo, robar SMS, contactos, credenciales bancarias y hasta activar la cámara y el micrófono en tiempo real. Su plataforma automatizada permite generar apps falsas y versiones troyanizadas de APK legítimos, lo que facilita su uso incluso para atacantes sin experiencia. Este caso se suma al aumento significativo del malware móvil, donde otras amenazas como Anatsa, Void y Xnotice también han proliferado, aprovechando permisos abusivos, superposiciones bancarias y técnicas avanzadas para robar dinero, datos sensibles y códigos de autenticación.

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

El ATAQUE

Infecta dispositivos mediante aplicaciones cuentagotas que se hacen pasar por actualizaciones de Google Play. Una vez instalado, fuerza al usuario a configurarlo como la app de SMS predeterminada, obteniendo permisos amplios para interceptar mensajes, incluidos códigos 2FA. También utiliza superposiciones falsas para robar credenciales bancarias y transmite en tiempo real la cámara y el micrófono usando WebRTC. Su bot de Telegram permite cargar cualquier APK para generar versiones troyanizadas y gestionar suscripciones. El panel C2 muestra dispositivos comprometidos y permite ejecutar comandos para recopilar datos. Esta operación imita a otros RAT modernos y demuestra cómo los atacantes combinan droppers, roles de SMS y técnicas de suplantación para lograr compromisos completos del dispositivo y saquear información financiera.

INFO

CONTEXT	INDICATOR	(MD5)
relis.apk	0cccfcc2a5813d2617213d2c24fe96edd360ff23d25d4f6c5b7c2ad6f3f3e87e	00ba72f40855e703c318cabb441af736
TikTok18.apk	ca33271f15d966b2da95010748d62e5e72c4783c74715953e4f79264cde54cef	00ef76ea4e207d755d41ec7056baaa19
relis.apk	79e0231d25d7588fa17037f64b69d85c08940b5fe3b7672a4366c9e012d353b8	011870e1350719b0e79f6fb95cac8bfc
com.example.MetaMask	9bf6fa1f35a73e5665e0cf8512e576a0f5cb99af31d05ee0640a74de960bb38c	029c7c50b9eeb99cf39388985ce202d3
app-release_protected_strong.apk	0b28875dc8dc8184401e6841364bd866b748a816072aa3008b8f2bde8da306e5	032f2eb7c9dff1ee6a4858451422b9d3
TikTok18.apk	8d96d0d7a8d6b0717e6f75f60a3889e86a4203aa8aab0e9349b70e38ad8ddf8f	0705be119dd534d819f2d58a819ed372
com.p99d1eabc7.tiktok18	d49677515a17747af85c703ae62f36ce5a8bdb80056e6f3b3057f4380866cbea	0d6c53595f3bdd00eae7a48d5dd818fd
com.example.MetaMask	0e1d086d61384d892a97395f22caa569ac16aad4d0dd83fe93cd3043e58de951	0e379c45dabf5bb86c13947442fa02f7
TikTok18.apk	b5542dd5d015d8a5b1405973d9dcf5a94dccdcc970f43b4197e5dbc2dff3028a	0f613ae429f1026badf95e560d836693
tiktok18.apk	7ea73c32040727b17ed265fb4a3f9b2cc314a97665b5d707d43adc0391e80915	0f95387dacb38f90f4e0029ece847d73

ÚLTIMAS NOTICIAS

ChatGPT: fallos de seguridad

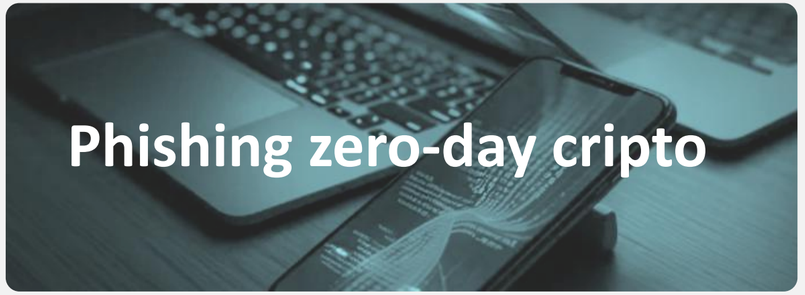
Investigadores de Tenable descubrieron siete vulnerabilidades críticas en ChatGPT y SearchGPT que permiten inyección indirecta de instrucciones, ataques de clic cero y elusión de filtros, además de filtrar datos del historial y la memoria del usuario. Las fallas provienen de cómo los modelos procesan instrucciones externas al abrir páginas o enlaces maliciosos. Algunas aún afectan a ChatGPT-5, y combinadas permiten cadenas de ataque que van desde la inyección hasta la exfiltración y la persistencia, mostrando la urgencia de reforzar la seguridad en la integración de LLM.

INFO

Cisco UCCX permite acceso root

Dos vulnerabilidades críticas que permiten a atacantes no autenticados ejecutar comandos arbitrarios con privilegios de root y eludir la autenticación para crear y ejecutar scripts con permisos de administrador. La falla principal se origina en mecanismos de autenticación inadecuados en el proceso Java RMI, lo que posibilita la ejecución remota de código (RCE). Cisco también abordó una vulnerabilidad de alta severidad en Identity Services Engine (ISE) que puede causar denegación de servicio (DoS), junto con otras cuatro fallas en productos Contact Center que permiten escalada de privilegios, ejecución de comandos y acceso a información sensible.

INFO



Phishing zero-day cripto

Investigadores de Bolster AI detectaron una campaña de phishing dirigida a usuarios de Swapzone.io, usando correos electrónicos falsos que prometen supuestos exploits de zero-day o ganancias instantáneas. Las víctimas son dirigidas a un Google Docs con una línea javascript: que, al ejecutarse, activa un script malicioso que toma control de la sesión del navegador, manipula visualmente los rendimientos mostrados y redirige pagos a billeteras controladas por los atacantes. La operación combina ingeniería social, urgencia y manipulación visual, y está organizada para múltiples criptomonedas, evidenciando un ataque bien estructurado contra usuarios cripto.

INFO

La ciberseguridad empieza por ti: pequeños hábitos, gran impacto

La falta de cultura de ciberseguridad es un riesgo crítico porque, aunque existan buenas herramientas, un solo usuario desinformado puede habilitar ataques como phishing o malware. La seguridad no depende solo de la tecnología, sino de que las personas sepan identificar amenazas. El factor humano sigue siendo la primera línea de defensa.

👥 Capacitación continua: Entrenar a los usuarios para reconocer correos falsos, enlaces maliciosos y prácticas inseguras.

🛡️ Políticas claras: Definir reglas simples y fáciles de seguir para manejar información y actuar ante situaciones sospechosas.

✅ Fomentar el reporte inmediato: Motivar a los empleados a informar cualquier actividad inusual sin miedo a equivocarse.

👉 Buenas prácticas diarias: Usar contraseñas seguras, activar MFA y mantener dispositivos actualizados.

📌 Recordatorios periódicos: Enviar mensajes cortos o infografías para mantener presentes las buenas prácticas.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4