Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

WHATSAPP CORRIGE EXPLOIT DE TIPO ZERO-CLICK QUE AFECTABA A IOS Y MACOS

01/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

La seguridad de las aplicaciones de mensajería vuelve a estar en el centro de atención tras la reciente corrección de una vulnerabilidad crítica en WhatsApp para iOS y macOS, la cual permitía ataques de tipo zero-click, es decir, sin necesidad de que el usuario realice ninguna acción. La falla, descubierta por el equipo interno de seguridad de WhatsApp, fue catalogada con una puntuación de alto riesgo y se cree que pudo haber sido utilizada en ataques dirigidos altamente sofisticados.

Este incidente refuerza las advertencias sobre el uso de plataformas de mensajería en entornos corporativos, donde la exposición a fallos de día cero puede traducirse en riesgos significativos para la información sensible. El caso demuestra cómo atacantes con acceso a vulnerabilidades encadenadas pueden comprometer dispositivos de ejecutivos, periodistas y defensores de derechos humanos, lo que convierte a la actualización constante de software y la vigilancia proactiva en medidas fundamentales para la ciberseguridad empresarial.

GUNRA RANSOMWARE: NUEVA VARIANTE PARA LINUX REFUERZA CAPACIDADES DE CIFRADO MASIVO Y PERSONALIZACIÓN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_01_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	01/09/2025
Es día cero (0 day):	Sí

RESUMEN

WhatsApp anunció la corrección de una vulnerabilidad crítica en sus aplicaciones para iOS y macOS, la cual podría haber sido explotada en combinación con un fallo recientemente divulgado por Apple. El ataque permitía comprometer dispositivos sin necesidad de interacción por parte del usuario (zero-click).

La falla, identificada como CVE-2025-55177 (con una puntuación CVSS de 8.0 según CISA-ADP), estaba relacionada con una autorización insuficiente en los mensajes de sincronización de dispositivos vinculados. De haberse explotado, un atacante podía forzar el procesamiento de contenido desde una URL arbitraria en el dispositivo objetivo.

Versiones afectadas y parches

- WhatsApp para iOS: versiones anteriores a 2.25.21.73 (parcheado el 28 de julio de 2025).
- WhatsApp Business para iOS: versión 2.25.21.78 (parcheado el 4 de agosto de 2025).
- WhatsApp para macOS: versión 2.25.21.78 (parcheado el 4 de agosto de 2025).

WhatsApp señaló que este fallo pudo haberse encadenado con CVE-2025-43300, una vulnerabilidad en el framework ImageIO de Apple que provoca corrupción de memoria al procesar imágenes maliciosas. Apple confirmó que esta debilidad fue utilizada en ataques altamente sofisticados dirigidos a individuos específicos.

Posible uso en campañas de espionaje

De acuerdo con investigadores, algunos usuarios fueron notificados por WhatsApp sobre intentos de explotación en los últimos 90 días, posiblemente vinculados a campañas avanzadas de spyware contra periodistas y defensores de derechos humanos. Como medida preventiva, WhatsApp recomendó realizar un restablecimiento de fábrica en los dispositivos afectados y mantener tanto el sistema operativo como la aplicación actualizados.

Riesgo empresarial

Este tipo de vulnerabilidades subraya la creciente amenaza que representan los ataques zero-click para las organizaciones. A diferencia de otras técnicas, no requieren que el usuario abra enlaces o archivos, lo que reduce significativamente las oportunidades de detección. Por ello, resulta esencial:

- Mantener aplicaciones y sistemas operativos en sus últimas versiones.
- Implementar monitoreo avanzado de seguridad móvil.
- Capacitar a empleados y directivos sobre riesgos asociados al uso de aplicaciones de mensajería en entornos corporativos.

Los ataques de espionaje digital, impulsados por proveedores de software espía, continúan siendo una amenaza activa para el sector empresarial y gubernamental en todo el mundo.

NOTICIA COMPLETA

https://devel.group/blog/whatsapp-corrige-exploit-de-tipo-zero-click-que-afectaba-a-ios-y-macos/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/