Alerta

Técnica

Vulnerabilidades Críticas Detectadas

COLCERT AL-20251003-078

TLP:CLEAR

Se han identificado dos (2) vulnerabilidades, **CVE-2025-55177** en **WhatsApp** y **CVE-2025-43300** en **Apple ImageIO**, explotadas en conjunto mediante ataques zero-click que permiten **comprometer dispositivos sin interacción del usuario**. Aunque los fabricantes ya han liberado parches, la probabilidad de que surjan variantes o que se reutilicen estas técnicas en el corto y mediano plazo es alta, dado el interés de actores de amenaza en la explotación de servicios de mensajería ampliamente utilizados.

El impacto potencial se proyecta más allá de casos dirigidos, logrando escalar hacia campañas de espionaje o ataques contra sectores estratégicos, con consecuencias severas para la confidencialidad y disponibilidad de la información. El nivel de incertidumbre en la detección temprana se mantiene moderado a alto, lo que obliga a anticipar medidas de protección, actualización constante y ejercicios de simulación para fortalecer la resiliencia organizacional.

Vulnerabilidades identificadas

CVE	PRODUCTOS AFECTADOS	SCORE CVSS	DESCRIPCIÓN	CISA KEV
CVE-2025-55177	WhatsApp para iOS (versión anterior a 2.25.21.73), WhatsApp Business iOS (antes de 2.25.21.78), WhatsApp para Mac (antes de 2.25.21.78).	**5.4 (medio)**	Autorización incompleta en mensajes de sincronización de dispositivos vinculados (“linked device sync”) en WhatsApp, que podría permitir que un usuario no autorizado provoque el procesamiento de contenido desde una URL arbitraria en el dispositivo objetivo.	**TRUE**
CVE-2025-43300	Sistemas Apple: iOS (versiones anteriores a 18.6.2), iPadOS (anteriores a 17.7.10 / 18.6.2), macOS (Sonoma antes de 14.7.8, Ventura antes de 13.7.8, Sequoia antes de 15.6.1).	**8.8 (alto)**	Escritura fuera de límites (out-of-bounds write) en el framework ImageIO al procesar una imagen maliciosa (por ejemplo, un DNG manipulado), lo que puede corromper memoria y permitir ejecución remota de código.	**TRUE**

NIVEL DE RIESGO

ALTO

¿Cómo se podrían explotar estas vulnerabilidades?

1. **Reconocimiento y enumeración**: el ciberdelincuente recopila información sobre el objetivo como número de teléfono, versiones de WhatsApp y del sistema operativo (iOS/macOS), dispositivos vinculados (linked devices) y comportamientos de descarga automática.

2. **Construcción del artefacto (archivo multimedia DNG)**: se crea un archivo de imagen en formato DNG (un contenedor RAW para imágenes) con estructuras y metadatos manipulados para provocar un fallo en el *parser* de ImageIO.

3. **Vector de entrega**: El DNG se envía por WhatsApp. Vulnerabilidades en la lógica de mensajería o en el proceso de sincronización de "linked devices" permiten que el archivo sea procesado por el cliente sin intervención del usuario (zero-click). El envío puede venir directamente desde un número o a través de sesiones vinculadas.

4. **Procesamiento automático y activación del fallo**: al procesar automáticamente la imagen por la generación de miniatura, indexación o preview, la librería nativa de manejo de imágenes sufre una corrupción de memoria (out-of-bounds, uso posterior de memoria liberada u otro fallo de integridad) que puede derivar en la desviación del flujo normal para ejecutar código controlado por el ciberdelincuente.

5. **Elevación de privilegios y persistencia**: con ejecución inicial, el actor intenta escalar privilegios o moverse a componentes con mayor persistencia para instalar agentes (*launchd* o *daemons* en macOS), añadir perfiles de configuración maliciosos, o abusar de credenciales almacenadas (*keychain*) si están accesibles.

6. **Recolección y exfiltración de datos**: una vez establecido el control, el atacante exfiltra mensajes, contactos, archivos y activa micrófono y cámara, o usa la mensajería para expandir la campaña hacia contactos del objetivo. Puede establecer canales de comando y control cifrados o aprovechar servicios legítimos para encubrir exfiltración.

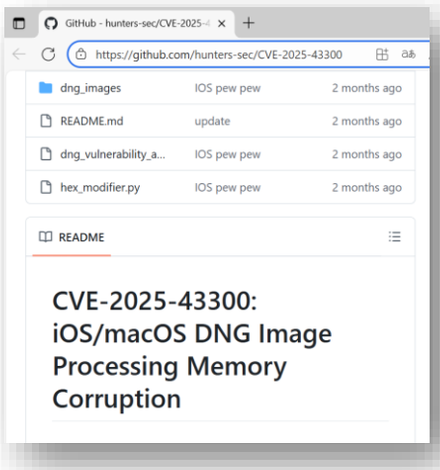
7. **Encubrimiento y mantenimiento**: eliminación o manipulación de logs, establecimiento de mecanismos de reentrada y vigilancia continua del dispositivo comprometido.

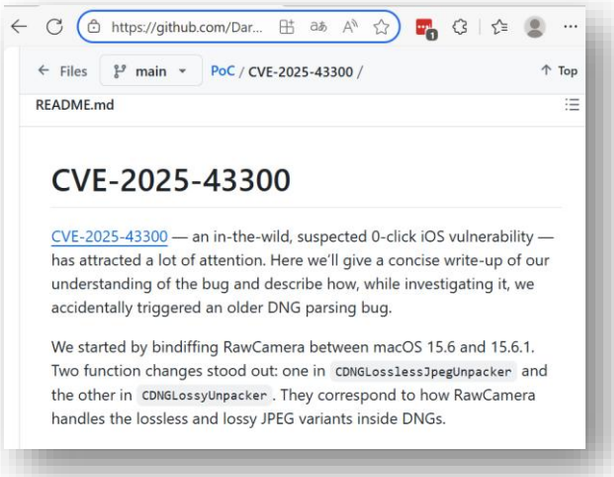
Pruebas de concepto identificadas

Una prueba de concepto (PoC) es una demostración técnica que valida la explotación de una vulnerabilidad. Se encontraron dos PoC para CVE-2025-43300 en:

- https://github.com/hunters-sec/CVE-2025-43300
- https://github.com/DarkNavySecurity/PoC/tree/main/CVE-2025-43300

No se encontraron PoC públicas para CVE-2025-55177.





Impacto para Colombia y la región

- **Sectores afectados**: Todos
- **Riesgo alto**: la combinación de una vulnerabilidad en un cliente de mensajería masivo (WhatsApp) y una falla en un subsistema nativo de procesamiento de imágenes eleva el riesgo porque permite ataques zero-click que no requieren interacción del usuario, facilitando compromisos silenciosos de dispositivos personales y corporativos. Dado el uso ubicuo de WhatsApp en Colombia y la dependencia de dispositivos Apple en perfiles decisores y operativos críticos, la exposición es amplia. Además, exploits de este tipo suelen ser reutilizados o adaptados por actores con motivaciones de espionaje, fraude o extorsión, lo que incrementa la probabilidad de impacto real en organizaciones sensibles.

- **Posibles consecuencias**:
  - Exfiltración de información confidencial (mensajería, contactos, documentos).
  - Compromiso de credenciales y acceso a cuentas corporativas y bancarias.
  - Espionaje contra funcionarios públicos, periodistas y líderes empresariales.
  - Interrupción de servicios críticos si dispositivos clave son usados para pivotar hacia redes operativas.
  - Pérdida de reputación y confianza en entidades afectadas, con impacto comercial y legal.
  - Incremento de incidentes de fraude y suplantación (phishing dirigido desde cuentas legítimas).

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Boot or Logon Autostart Execution	T1547	Uso de mecanismos de arranque o inicio de sesión para establecer persistencia y ejecutar código automáticamente tras reinicio o sesión.
Credentials from Password Stores — Keychain	T1555.001	Extracción de credenciales y secretos almacenados en el Keychain de macOS/iOS para escalar acceso y movimiento lateral.
Audio Capture	T1123	Abuso de capacidades de captura de audio del dispositivo (micrófono) para vigilancia y recolección de información tras el compromiso.
Exploitation for Client Execution	T1203	Explotación de vulnerabilidades en aplicaciones cliente para lograr ejecución de código arbitrario en el contexto del proceso afectado (cliente de mensajería / parser de imágenes).

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Update Software	M1051	Parchear clientes de mensajería y subsistemas (ImageIO/OS) reduce la ventana de exposición a *exploits* que aprovechan fallos en *parsers* y clientes.
Execution Prevention (aplicación/Control de ejecución)	M1038	Control de qué binarios o scripts pueden ejecutarse evita que componentes no autorizados se configuren como persistencia tras un exploit.
Password Policies	M1027	Fortalecer contraseñas y políticas del keychain aumenta la fricción para que un actor obtenga credenciales almacenadas tras comprometer un proceso.
User Guidance	M1011	Concienciación sobre permisos y revisión de apps/privilegios ayuda a reducir la probabilidad de que aplicaciones o payloads abusivos consigan acceso a micrófono.

Soluciones y mitigaciones disponibles

- Actualizar los clientes de WhatsApp a versión **2.25.21.73** o superior para iOS y versión **2.25.21.78** o superior para Mac / WhatsApp Business en iOS, así como actualizar los sistemas de Apple a **iOS/iPadOS 18.6.2**, macOS Sonoma **14.7.8**, macOS Ventura 13.7.8, macOS Sequoia 15.6.1.
- Configurar las aplicaciones de mensajería para desactivar la descarga y previsualización automática de archivos multimedia, reduciendo la superficie de ataque por archivos DNG maliciosos.
- Monitorear activamente los registros de sistema y telemetría de endpoints para identificar crashes recurrentes en procesos relacionados con el procesamiento de imágenes o mensajería.
- Fortalecer las políticas de gestión de credenciales y autenticación multifactor en cuentas corporativas, dificultando la explotación secundaria tras el compromiso inicial.
- Concientizar a los usuarios de alto sobre los riesgos de ataques zero-click, reforzando la cultura de ciberseguridad frente a este tipo de amenazas.

Fuentes

WhatsApp, "WhatsApp Security Advisories 2025", agosto 2025, categoría: anuncio oficial.
https://www.whatsapp.com/security/advisories/2025/
CyberPress, "0-Click WhatsApp Vulnerability", 29 septiembre 2025, categoría: medio especializado.
https://cyberpress.org/0-click-whatsapp-vulnerability/
NVD, "CVE-2025-43300 Detail", 20 agosto 2025, categoría: base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-43300
NVD, "CVE-2025-55177 Detail", 29 agosto 2025, categoría: base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-55177
TheHackerNews, "Apple Backports Fix for CVE-2025-43300 Exploited in Sophisticated Spyware Attack", 16 septiembre 2025, categoría: medio de noticias.
https://thehackernews.com/2025/09/apple-backports-fix-for-cve-2025-43300.html

COLCERT