

Alerta de seguridad informática	9VSA-00060-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2019
Última revisión	03 de octubre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de diferentes fuentes, referente a una vulnerabilidad que afecta a Whatsapp y cómo mitigarla.

Vulnerabilidad

- CVE-2019-11932

Impacto

Un atacante podría explotar esta vulnerabilidad enviando un archivo malicioso de tipo documento (.doc o .docx) especialmente diseñado para que, cuando el usuario, al abrir la galería de imágenes a través de la aplicación, y realice una pre-visualización del contenido multimedia almacenado, se compile el payload, el cual ejecutará el malware en la Shell de Whatsapp, obteniendo todos los privilegios de ésta, y con ello, acceso a todas sus funcionalidades (micrófono, cámara, mensajes, contactos, etc.).

Productos Afectados

Las versiones de Whatsapp vulnerables son la 2.19.230 y anteriores, siempre y cuando estén instaladas sobre las versiones 8.1 y 9.0 de Android.

Mitigación

Actualizar a la última versión a través de Google Play Store. Recomendamos siempre mantener todas las aplicaciones y el sistema operativo Android actualizados en su última versión.

Enlaces

- <https://awakened1712.github.io/hacking/hacking-whatsapp-gif-rce>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11932>