Alerta de seguridad cibernética	9VSA20-00314-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de noviembre de 2020
Última revisión	02 de noviembre de 2020

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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de WhatsApp respecto a 7 vulnerabilidades que afectan a la aplicación de mensajería instantánea. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-1907
CVE-2020-1906
CVE-2020-1905
CVE-2020-1904
CVE-2020-1903
CVE-2020-1902
CVE-2020-1901

CVE-2020-1907

Impacto
Un error desbordamiento de la pila en la aplicación de mensajería podría haber permitido la ejecución de código arbitrario al gestionar los contenidos de “RTP Extension header”.

Productos Afectados
WhatsApp para Android versiones anteriores a la 2.20.196.16.
WhatsApp Business para Android versiones anteriores a la 2.20.196.12.
WhatsApp para iOS versiones anteriores a la 2.20.90.
WhatsApp Business para iOS versiones anteriores a la 2.20.90.
WhatsApp Portal versiones anteriores 173.0.0.29.505.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1907

CVE-2020-1906

Impacto
Un error de desbordamiento del buffer podría haber permitido una la escritura fuera de los límities en memoria al procesar videos locales malformados con stream de audio “E-AC-3”.

Productos Afectados
WhatsApp para Android versiones anteriores a la 2.20.130.
WhatsApp Business para Android versiones anteriores a la 2.20.46.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1906

CVE-2020-1905

Impacto
Los URI de "Media ContentProvider" utilizados para abrir archivos adjuntos en otras aplicaciones eran generaros secuencialmente, lo que podría haber permitido a una aplicación de terceros maliciosa elegida para que abra el archivo, adivinar los URI de archivos adjuntos abiertos anteriormente hasta que se terminara.

Productos Afectados
WhatsApp para Android versiones anteriores a la 2.20.185.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1905

CVE-2020-1904

Impacto
Un error de validación de ruta en la aplicación podría haber permitido la sobreescritura de archivos en directorio trasversal al enviar archivos docx, xlx y pptx especialmente diseñados como adjuntos en los mensajes.

Productos Afectados
WhatsApp para iOS versiones anteriores a la 2.20.61.
WhatsApp Business para iOS versiones anteriores a la 2.20.61.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1904

CVE-2020-1903

Impacto
Un problema al descomprimir archivos “docx, pptx y xlsx en la aplicación podría haber resultado en una denegación de servicios por falta de memoria. Este problema requería que el emisor del archivo no estuviera en la lista de contactos al descomprimir el archivo.

Productos Afectados
WhatsApp para iOS versiones anteriores a la 2.20.61.
WhatsApp Business para iOS versiones anteriores a la 2.20.61.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1903

CVE-2020-1902

Impacto
Un usuario ejecutando una búsqueda rápida en un mensaje reenviado podría haber sido enviada al servicio de Google en texto plano HTTP.

Productos Afectados
WhatsApp para Android desde la versión 2.20.108 hasta la 2.20.140.
WhatsApp Business para Android desde la versión 2.20.35 hasta la 2.20.49.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1902

CVE-2020-1901

Impacto
Recibir un mensaje de texto grande que contenga URLs podría haber causado que la aplicación se congele mientras procesa el mensaje.

Productos Afectados
WhatsApp para iOS versiones anteriores a la 2.20.91.4.

Mitigación
Actualizar la aplicación a la última versión disponible por el fabricante.

Enlaces
https://www.whatsapp.com/security/advisories/2020/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1901