BOLETÍN DE ALERTA

Boletín Nro.: 2015-09
Fecha de publicación: 30/07/2015
Tema: Vulnerabilidad Stagefright en Android

Sistemas afectados:

- Android desde Froyo 2.2 hasta Android Lollipop 5.1.1

Descripción:

Stagefright, el motor de reproducción de medios de Android contiene siete vulnerabilidades diferentes, incluyendo varios desbordamientos de buffer, lo que permite a un atacante remoto acceder a archivos y posiblemente ejecutar código en el dispositivo. Esta vulnerabilidad parece afectar a todas las versiones de Android desde 2.2 (Froyo) y al menos 5.1.1_r5 Android (Lollipop). La característica que hace que la vulnerabilidad sea aún más grave es que, para reducir el tiempo de retraso en la visualización de vídeo Stagefright procesa automáticamente el vídeo antes de realizar ninguna comprobación.

Un atacante con el número de teléfono celular de la víctima puede enviar mensajes multimedia (MMS) maliciosos que serán procesados incorrectamente mediante Stagefright.
Un video malicioso que es enviado mediante un mensaje multimedia (MMS) a cualquier aplicación de mensajería que pueda procesar un formato de vídeo específico – como una aplicación de mensajería nativa de un dispositivo Android o Google Hangout, puede ser un posible vector de ataque. Por defecto, las aplicaciones de mensajería de MMS cargan los vídeos automáticamente.

De acuerdo con los parches, las vulnerabilidades parecen ser múltiples desbordamientos de enteros y cheques incorrectos de desbordamiento de entero. Como los desbordamientos de enteros son un tipo

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

de error de memoria, la técnica de Address Space Layout Randomization (ASLR) parece mitigar parcialmente el problema; ASLR se introdujo en Android 4.0 y se implementó plenamente en Android 4.1.

Según investigadores, la explotación exitosa proporcionan, por lo menos, acceso directo al audio de un teléfono, la cámara web y al almacenamiento externo. Muchos teléfonos antiguos otorgan privilegios elevados a Stagefright, lo cual podría permitir a los atacantes acceso a muchos más recursos del dispositivo.

Impacto

Un atacante remoto podría ejecutar código en el dispositivo Android, logrando acceso total al mismo.

Solución y Mitigación

- Actualización

  El proyecto de código abierto Android (AOSP) ha lanzado varios parches para solucionar las vulnerabilidades. Algunos de estos parches se han fusionado en Android desde la versión 5.1.1_r5. Actualmente no está claro si todos los parches se han fusionado en última Android. Tenga en cuenta que no todos los teléfonos con Android 5.1.1 (Lollipop) han aplicado estos parches.

  Las actualizaciones y sus procesos dependen del fabricante y la compañía de teléfono, por lo que la actualización puede o no estar disponibles para su teléfono.

- Bloquear todos los mensajes de texto de remitentes desconocidos

  El bloqueo de todos los mensajes de texto de remitentes desconocidos en su defecto la aplicación de manejo de mensajes de texto puede mitigar este problema.

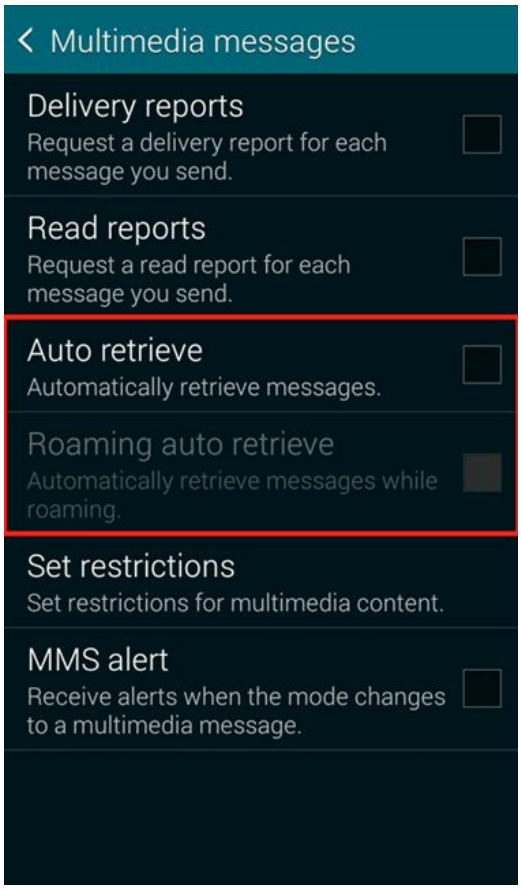
- Desactivar la descarga automática de los mensajes multimedia

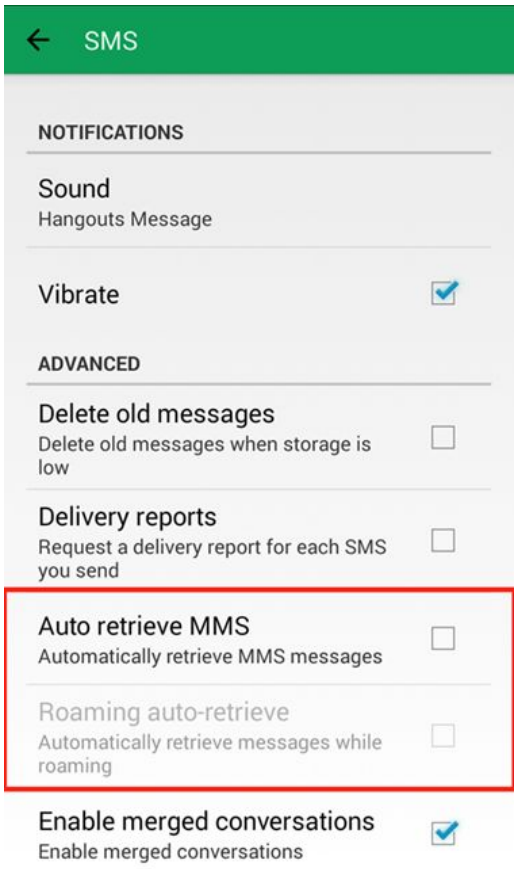
  Si su aplicación de mensajería de texto por defecto no permite el bloqueo de remitentes, también puede desactivar la función de recuperación automática de los mensajes multimedia. Esto puede evitar la carga automática de contenidos MMS en Stagefright.

  En el siguiente enlace encontrará una guía para desactivarla:

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

https://www.avast.com/es-es/faq.php?article=AVKB230





Información adicional:

http://www.kb.cert.org/vuls/id/924951#sthash.4KFerfEf.dpuf

http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

https://www.avast.com/es-es/faq.php?article=AVKB230

http://www.cnet.com/au/news/researcher-finds-mother-of-all-android-vulnerabilities/

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py