Investigadores de seguridad cibernética descubrieron dos vulnerabilidades graves en la aplicación SHAREit para Android, que permite a los atacantes eludir el mecanismo de autenticación del dispositivo y robar archivos que contienen información confidencial del dispositivo de la víctima.

Con más de 1.5 billones de usuarios en el mundo, SHAREit es una popular app para compartir archivos para Android, iOS, Windows y Mac que fue diseñada para ayudar a las personas a compartir videos, música, archivos y aplicaciones en distintos dispositivos.

Según una publicación de los investigadores de RedForce, la aplicación SHAREit para Android fue vulnerable a una falla de omisión de autenticación de una aplicación de transferencia de archivos y una vulnerabilidad de descarga de archivos arbitraria.

Las vulnerabilidades se descubrieron en un inicio durante diciembre de 2017 y se arreglaron en marzo de 2018, pero los investigadores decidieron no revelar los detalles hasta el lunes, *«dado el impacto de la vulnerabilidad, su gran superficie de ataque y la facilidad de explotación»*.

> *«Queríamos dar a tantas personas como podamos el tiempo para actualizar y parchear sus dispositivos antes de revelar una vulnerabilidad tan crítica»*, dijo Abdulrahman Nour, ingeniero de seguridad de RedForce.

El servidor de SHAREit aloja múltiples servicios por medio de diferentes puertos en un dispositivo, pero los investigadores analizaron dos servicios designados, incluido el Canal de Comando, que se ejecuta en el puerto 55283, y el Canal de Descarga, que se ejecuta en el puerto 2999.

Command Channel es un canal TCP regular donde las aplicaciones intercambian mensajes con otras instancias de SHAREit que se ejecutan en otros dispositivos mediante conexiones de socket sin formato, incluida la identificación del dispositivo, el manejo de solicitudes de transmisión de archivos y la verificación del estado de la conexión.

Download Channel es la implementación del propio servidor HTTP de la aplicación SHAREit que es utilizada principalmente por otros clientes para descargar archivos compartidos.

Según los investigadores, cuando Android utiliza la aplicación SHAREit para enviar un archivo al otro dispositivo, una sesión regular de transferencia de archivos comienza con una identificación regular del dispositivo, luego el remitente envía un mensaje de control al receptor, que indica que se tiene un archivo para compartir.

Una vez que el receptor verifica que el archivo no está duplicado, va al canal de descarga y recupera el archivo enviado utilizando la información del mensaje de control anterior.

Los hackers pueden acceder a tus archivos mediante las vulnerabilidades de SHAREit

Sin embargo, los investigadores descubrieron que cuando un usuario sin sesión válida intenta buscar una página no existente, en lugar de una página 404 normal, la aplicación SHAREit responde con una página vacía de código de estado 200 y agrega al usuario a dispositivos reconocidos, autentificando finalmente un usuario no autorizado.

Según los investigadores, un exploit de prueba de concepto completamente funcional para este defecto sería tan simple como curl http://shareit_sender_ip:2999/DontExist, lo que lo convierte en el bypass de autenticación más extraño y simple.

También encontraron que cuando se inicia una solicitud de descarga, el cliente SHAREit envía una solicitud GET al servidor HTTP del remitente, que se parece a la siguiente URL:

```
http://shareit_sender_ip:2999/download?metadatatype=photo&meta
dataid=1337&filetype=thumbnail&msgid=c60088c13d6
```

Dado que la aplicación SHAREit no puede validar el parámetro «msgid», un identificador

único generado para cada solicitud cuando el remitente inicia una descarga, permite que el cliente malintencionado con una sesión válida descargue cualquier recurso haciendo referencia directamente a su identificador.

Las fallas pueden ser explotadas por un atacante en una red WiFi compartida, y desafortunadamente, las versiones SHAREit vulnerables crean un punto de acceso WiFi abierto fácilmente distinguible que se puede utilizar no solo para interceptar el tráfico entre los dispositivos, sino también para explotar las vulnerabilidades descubiertas y tener acceso ilimitado al almacenamiento de dispositivos vulnerables.

Debido a que la explotación simplemente implica enviar un comando curl que haga referencia a la ruta del archivo de destino, uno debe conocer la ubicación exacta del archivo que se desea recuperar.

Para superar esto, los investigadores comenzaron a buscar archivos con rutas conocidas que ya están disponibles públicamente, como SHAREit History y SHAREit MediaStore Database, que pueden contener información interesante.

> *«Hay otros archivos que contienen información jugosa, como el token de Facebook del usuario, la clave del usuario del servicio web de Amazon, los datos de llenado automático y las cookies de los sitios web visitados con SHAREit webview e incluso el texto plano del punto de acceso original del usuario (la aplicación lo almacena para restablecer el punto de acceso a los valores originales) y mucho más»,* dijeron los investigadores.

Usando su vulnerabilidad de prueba de concepto apodada DUMPit!, los investigadores lograron descargar alrededor de 3000 archivos únicos con 2 GB en menos de 8 minutos de sesión de transferencia de archivos.

El equipo se comunicó con SHAREit varias veces en distintas plataformas a inicios de 2018, pero no obtuvo respuesta hasta principios de febrero, cuando los investigadores advirtieron a

la compañía que publicara los detalles de la vulnerabilidad al público luego de 30 días.

El equipo de SHAREit parchó silenciosamente las vulnerabilidades en marzo de 2018, sin proporcionar a los investigadores versiones parcheadas exactas de la aplicación para Android, identificaciones de CVE de vulnerabilidad o comentarios para la divulgación pública.

> *«La comunicación con el equipo de SHAREit no fue una buena experiencia en absoluto; no solo tardaron mucho en responder a nuestros mensajes, sino que tampoco cooperaron de ninguna forma, y no sentimos que nuestro trabajo o nuestros esfuerzos fueran apreciados en absoluto»,* dijeron los investigadores.

Después de darles a los usuarios el tiempo suficiente para actualizar su aplicación SHAREit, los investigadores publicaron detalles técnicos de las vulnerabilidades, junto con el exploit PoC, DUMBit!, que se puede descargar del sitio web de GitHub.

Las vulnerabilidades afectan a la app SHAREit para Android versión 4.0.38. Si utilizas esta versión de la app, es necesario actualizarla desde la PlayStore cuanto antes.