Varias aplicaciones de Android de alto perfil siguen utilizando una versión sin parches de la biblioteca de actualizaciones de aplicaciones ampliamente utilizada de Google, lo que potencialmente pone los datos personales de cientos de millones de usuarios de smartphones en riesgo de hackeo.

Muchas aplicaciones populares, incluidas Grindr, Bumble, OkCupid, Cisco Teams, Moovit, Yango Pro, Microsoft Edge, Xrecorder y PowerDirector, siguen siendo vulnerables y pueden ser secuestradas para robar datos confidenciales, como contraseñas, detalles financieros y correos electrónicos.

La vulnerabilidad, rastreada como CVE-2020-8913, tiene una calificación de 8.8 sobre 10 en cuanto a gravedad, impacta en las versiones de la biblioteca Play Core de Android anteriores a la 1.7.2.

Aunque Google abordó la vulnerabilidad en marzo, los nuevos hallazgos de Check Point Research muestran que muchos desarrolladores de aplicaciones de terceros aún tienen que integrar la nueva biblioteca Play Core en sus aplicaciones para mitigar la amenaza completamente.

> *«A diferencia de las vulnerabilidades del lado del servidor, donde la vulnerabilidad se repara por completo una vez que el parche se aplica al servidor, para las vulnerabilidades del lado del cliente, cada desarrollador debe tomar la última versión de la biblioteca e insertarla en la aplicación»,* dijo la compañía de seguridad.

Play Core Library es una biblioteca popular de Android que permite a los desarrolladores administrar la entrega de nuevos módulos de funciones de forma efectiva, activar actualizaciones en la aplicación en tiempo de ejecución y descargar paquetes de idiomas adicionales.

Informado por primera vez a fines de agosto por investigadores de Oversecured, el problema permite que un actor de amenazas inyecte ejecutables maliciosos en cualquier aplicación

que dependa de la biblioteca, lo que le otorga al atacante acceso completo a todos los recursos como el de la aplicación comprometida.

La falla se debe a una vulnerabilidad de recorrido de ruta en la biblioteca que podría explotarse para cargar y ejecutar código malicioso (por ejemplo, un archivo APK) en una aplicación de destino para robar los detalles de inicio de sesión de los usuarios, contraseñas, detalles financieros y otra información confidencial almacenada.

Las consecuencias de la explotación exitosa de la vulnerabilidad son muy grandes. Se puede utilizar para *«inyectar código en aplicaciones bancarias para obtener credenciales, y al mismo tiempo, tener permisos de SMS para robar los códigos de autenticación de dos factores (2FA)»*, capturar mensajes de aplicaciones de chat, espiar las ubicaciones de los usuarios e incluso, obtener acceso a los recursos corporativos manipulando las aplicaciones empresariales.

Según Check Point Research, del 13% de las aplicaciones de Google Play analizadas en el mes de septiembre de 2020, el 8% de esas aplicaciones tenían una versión vulnerable.

Después de que la firma de seguridad cibernética divulgara responsablemente sus hallazgos, Viber, Meetup y Booking actualizaron sus aplicaciones a la versión parcheada de la biblioteca.

Los investigadores también demostraron una prueba de concepto que utilizó una versión vulnerable de la aplicación Google Chrome para desviar los marcadores almacenados en el navegador a través de una carga útil dedicada.

> *«Estimamos que cientos de millones de usuarios de Android están en riesgo de seguridad. Aunque Google implementó el parche, muchas aplicaciones todavía usan bibliotecas Play Core obsoletas. La vulnerabilidad CVE-2020-8913 es altamente peligrosa, y las posibilidades de ataque aquí solo están limitadas por la imaginación*

> *de un actor de amenazas»,* dijo Aviran Hazum, gerente de investigación móvil de Check Point.

Actualización

El 3 de diciembre de 2020, Grindr y Moovit actualizaron sus aplicaciones y ya no son vulnerables. De igual forma, los equipos de Cisco se actualizaron y su aplicación tampoco es vulnerable, según informa Check Point Research.