Correo Malicioso Afecta Aplicación Google Email En Android

Una vulnerabilidad ha sido descubierta en la popular **aplicación de email que se usa en Android**, la cual podría ser explotada por atacantes maliciosos para controlar remotamente su aplicación para teléfonos inteligentes con sólo enviar un correo electrónico especialmente diseñado.

Un investigador de seguridad de España, Héctor Marco, aprovechara la vulnerabilidad en su Samsung Galaxy S4 Mini, el cual usa la versión 4.2.2.0200 de la APP Stock Email para Android. Él dijo que la falla parece afectar a todas las versiones anteriores de Android Stock Email App, aunque los dispositivos que ejecutan 4.2.2.0400 y versiones más recientes no están afectadas.

Según el investigador, cuando la víctima recibe el correo electrónico malicioso y trata de verla, la aplicación bloquea el correo electrónico. Otros intentos para abrir el correo electrónico de nuevo desencadena una caída en el dispositivo, en el cual no se puede lograr mucho para salir de aquel estado.

La falla (**CVE-2015-1574**) se debe a un manejo incorrecto de la cabecera **Content-Disposition**. Los hackers podrían aprovechar esta vulnerabilidad mediante el envío de un correo electrónico con un encabezado Content-Disposition malformado al usuario, con el fin de causar la caída de la aplicación de correo electrónico.

La única manera de **deshacerse de este problema,** es eliminar el correo electrónico malicioso del email Stock Android.

> *«Dado que la aplicación se cuelga inmediatamente, [y la] forma más fácil y directa para eliminar [el mensaje] es mediante el uso de otro cliente de correo electrónico (o vía web) de la bandeja de entrada en el servidor de correo electrónico», explicó Marco en un blog. «Otra forma, es mediante la desactivación de la conexión a Internet (Modo avión) antes de iniciar el lector de correo electrónico, y entonces usted puede eliminar el correo electrónico.»*

Sin embargo, la eliminación de la dirección de correo electrónico malicioso de la bandeja de entrada de la aplicación es sólo una solución temporal porque los atacantes pueden enviar la mayor cantidad de correo electrónico malicioso que ellos deseen.

Para (PoC) demostración de prueba de concepto, Marco publica un código de explotación en Python el martes, y explicó cómo el envío de un correo electrónico especialmente diseñado a un usuario específico puede detener la aplicación de correo electrónico de la víctima.

Hasta el momento, no hay reportes de que Marco del exploit también funciona en iOS u otros usuarios moviles. Pero la vulnerabilidad afecta a la mayoría de los usuarios de smartphones Android como la versión de archivo de correo electrónico de Google, la cual viene pre-instalada en las versiones oficiales de Android.

No está claro si la vulnerabilidad se ha informado a Google. Los usuarios pueden actualizar su aplicación para Android email a la versión 4.2.2.0400 o superior con el fin de protegerse a sí mismos, sino solamente a los usuarios que tienen la opción de actualizar.