



Masterhacks - Según un reporte de la empresa de seguridad informática ESET, la aplicación Swiftkey de los Samsung Galaxy tiene una vulnerabilidad, misma que se relaciona con la manera en que se actualiza. Consulta al servidor de manera periódica, pero este proceso lo realiza de manera que el archivo ejecutable que se descarga no está encriptado.

A partir de lo anterior, cualquier pirata informático puede comprometer al servidor de actualizaciones para enviar un archivo malicioso al dispositivo.

«El archivo podría convertir al dispositivo en un bug, tomando el control de la cámara y micrófonos, instalando otras apps y hasta robando datos», afirmó ESET.

Los dispositivos Samsung que estuvieron en riesgo son los Galaxy S3, S4, S5, S6 y S6 Edge. De igual forma los Galaxy Note 3 y 4.

Por su parte, Swiftkey respondió con lo siguiente: «Hemos visto reportes de un inconveniente de seguridad relacionado al teclado por defecto de Samsung que utiliza el SDK de SwiftKey. Estamos en condiciones de confirmar que la app del Teclado SwiftKey, disponible a través de Google Play o el App Store de Apple, no está afectada por esta vulnerabilidad. Tomamos los reportes de esta índole muy seriamente y por eso estamos investigando en profundidad el asunto».

Ryan Welton, investigador de la empresa de seguridad NowSecure, quien descubrió la vulnerabilidad, afirmó durante una conferencia que Samsung parece haber arreglado el error, pero mostró desconfianza acerca de la distribución entre todos los que fueron afectados.