“Nueva” vulnerabilidad en Android afectaría al 99 por ciento de los dispositivos.

¿Problemas de seguridad en Android? Lamentablemente, eso no es ninguna novedad. Cada vez que visito la *Google Play Store*, entre las aplicaciones más recomendadas encuentro antivirus y otras soluciones de seguridad, aunque también se ha dicho que no sirven de mucho. Lo último que necesita Android en este momento es otra piedra en el camino, pero la gente de **Bluebox Security** reveló que ***un bug de cuatro años de edad*** podría comprometer toda la estructura de seguridad en el sistema operativo, afectando al *99 por ciento* de los dispositivos. Ahora, la pregunta es: ***¿Qué tan cierto es todo esto?***

En una reciente publicación a través de su sitio oficial, el CTO de **Bluebox Security** Jeff Forristal anunció el descubrimiento de una nueva vulnerabilidad que permitiría a un desarrollador malicioso modificar el código APK de una **aplicación Android** *sin comprometer su firma criptográfica*. Hasta este punto, las consecuencias parecen terribles: Si se puede insertar código malicioso a una aplicación sin afectar su firma, no habría forma de diferenciar en primera instancia a una aplicación infectada de una real. Otro aspecto de la vulnerabilidad es que, de acuerdo a Bluebox, está presente ***desde el lanzamiento de Android 1.6***. Si hacemos un poco de memoria, Android 1.6 Donut hizo su debut en septiembre de 2009, por lo tanto, el bug estaría presente en *cada dispositivo Android* que ha sido lanzado desde esa fecha, más aquellos que recibieron Donut como *update*.

Sólo los dispositivos más recientes tienen una corrección de fábrica

El bug en cuestión, bajo el número 8219321, fue reportado apropiadamente a Google en febrero de este año. Mountain View hizo su trabajo, pero como ya sabemos bien, la situación de **Android** es muy diferente a la de otros sistemas como iOS. Desde cierto punto de vista, ***cada fabricante puede personalizar a su antojo los builds Android*** para sus dispositivos, y muchos de ellos han dejado de recibir actualizaciones apropiadas, forzando a los usuarios a realizar un proceso de *"rooting"* e instalación de un firmware alternativo. Bluebox ha dicho que el **99 por ciento de los dispositivos** está en riesgo. El bug es un hecho, está suelto, y debe ser corregido o contenido… *pero no se trata del 99 por ciento*. La realidad indica que la cantidad de smartphones y tablets es menor, y que ese número sólo se aplica *de modo potencial*. ¿Por qué?

Porque no todos los usuarios corren el riesgo de instalar aplicaciones que no tengan a la Google Play Store como fuente *(y esto también requiere varias acciones adicionales)*. Dicho de otra forma, mientras el usuario se mantenga *en la caja de arena de Google*, no debería ser afectado por esta vulnerabilidad. ***Sentido común y precaución son nuestros mejores aliados***. Bluebox reporta que Samsung ya ha lanzado una corrección para su Galaxy S4, y que Google está haciendo lo mismo con su serie Nexus. *Mountain View ha prohibido* a las aplicaciones que entreguen actualizaciones *"por fuera"* de la tienda, por lo tanto, existe un mecanismo de verificación funcionando. En resumen: ***Usa la tienda, chequea los permisos de cada aplicación, y ante la duda, busca una alternativa.***