QuadRooter, la vulnerabilidad de "900 millones de Android": ¿amenaza real o marketing del miedo?

900 millones de dispositivos Android. Ésa es la estimación que ha hecho Check Point (y que seguramente hayas visto en decenas de titulares) respecto al número de dispositivos que son vulnerables a **QuadRooter**, un bug que afecta a los dispositivos que posean un chip Qualcomm. Pero ¿en qué consiste dicho problema de seguridad? ¿Es tan peligroso como lo pintan?

¿Qué es "QuadRooter"?

Check Point, una empresa de seguridad informática, presentaba este fin de semana en la conferencia DEF CON 24 los resultados de una de sus recientes investigaciones relativa a los **chips LTE de Qualcomm** (que, según ellos mismos indican, están presentes actualmente en un 65% de los smartphones y tablets Android del mercado).

En el informe de su investigación ofrecen algún detalle más sobre QuadRooter. En concreto, explican que son **cuatro las vulnerabilidades que han encontrado** en los drivers de los chips de Qualcomm que vienen preinstalados en cada dispositivo que los utilizan. Los módulos afectados, según detalla la compañía, son IPC router (comunicación entre componentes Qualcomm), Ashmem (sistema de asignación de memoria), kgsl y kgsl_sync (relativos a los drivers gráficos).

Si un atacante aprovecha cualquiera de estos cuatro fallos de seguridad puede lograr **acceso root** y, por tanto, controlar por completo tu dispositivo y todo lo que hay en él. Podrían ver por ejemplo la información almacenada o proceder a la "escucha activa" monitorizando lo que escribes en él o tu posición por GPS.

¿Cómo puedo "infectarme"? ¿Debería preocuparme?

Según Check Point: "Un atacante puede explotar estas vulnerabilidades utilizando una app maliciosa. Estas apps no requieren permisos especiales para aprovecharse de estas vulnerabilidades, reduciendo cualquier sospecha que los usuarios pueden tener al instalarlas". La realidad es un **poco menos espectacular**.

Para que alguien utilice QuadRooter para hacerse con el control de tu dispositivo, tienen que darse varias circunstancias al mismo tiempo:

1. Que tu dispositivo utilice los drivers vulnerables (puedes saltar al siguiente apartado para comprobarlo).
2. Que te descargues una app maliciosa por tu cuenta (hasta el momento no se han detectado apps infectadas en Google Play y, dado que Google fue notificada en abril del problema, posiblemente estarán muy pendientes para que no se cuele ninguna).
3. Que, para descargarte esa app, actives la posibilidad de descargarte aplicaciones desde fuentes desconocidas (desactivada por defecto).
4. Y que, además, tengas desactivada la funcionalidad de "Verificar Aplicaciones" (un "filtro de seguridad" en Android 4.2 o superior al que Google posiblemente haya añadido la posibilidad de detectar estas apps maliciosas).

Si bien Google no ha confirmado que tanto Google Play como su "Verificar Aplicaciones" estén vigilando de cerca que no se cuelen apps que se aprovechen de esa vulnerabilidad (aunque sea lo más lógico dado que fueron avisados hace meses), para que un atacante utilice estos fallos para hacerse con el control de tu dispositivo sería necesario que **tú instalases antes una aplicación infectada**.

A todo esto habría que sumar que, al menos por ahora, **no se han detectado apps infectadas**.

¿Cómo saber si mi dispositivo es vulnerable?

Como decía, el problema (o problemas más bien) está presente en dispositivos con chips LTE de Qualcomm. Check Point han lanzado una aplicación que permite escanear rápidamente tu teléfono o tablet y comprobar si efectivamente utiliza los drivers afectados. La aplicación está en inglés eso sí y no soluciona nada (por mucho que intenten venderte), simplemente sirve para saber si tu dispositivo es vulnerable o no.

Si lo es, que no te extrañe: según Check Point los terminales afectados pertenecen a marcas como **Samsung, HTC, Motorola y LG**. Entre ellos están, por ejemplo, los Nexus (5X, 6 y 6P), el LG 5, el HTC 10, los OnePlus (One, 2 y 3), la BlackBerry Priv y los Samsung Galaxy S7, aunque hay más modelos.

¿Qué puedo hacer para solucionarlo?

Para solucionarlo, poco. Sólo Google y el fabricante de tu teléfono pueden arreglarlo con **un parche que solucione los cuatro bugs**. Desde Qualcomm aseguran que ya han arreglado el problema y distribuido la solución. Tres de los fallos de seguridad incluso ya se han parcheado con la actualización mensual de seguridad de Google, mientras que el cuarto llegará con la actualización de septiembre a los dispositivos Nexus.

Los parches de los fabricantes para otros modelos ya son otro asunto distinto y podrían tardar meses. De hecho, es algo que critica en su informe Check Point:

Cadena Suministros

> ¿POR QUÉ SIGUE PASANDO ESTO? La cadena de suministros
>
> Los proveedores, al igual que los fabricantes de chipsets, proporcionan los módulos de hardware y de software que se necesitan para para fabricar teléfonos y tablets. Los fabricantes (OEMs) combinan estos módulos de software, las builds de Android de Google y sus propias personalizaciones para crear un Android único creado para un dispositivo particular. Los distribuidores revenden los dispositivos, a menudo incluyendo sus propias personalizaciones y aplicaciones, y creando otra versión única más de Android. Cuando se necesita un parche, estos deben moverse a través de esta cadena de suministros hasta el dispositivo final del usuario. Este proceso lleva semanas o incluso meses.

¿Y para evitar que alguien pueda aprovecharlo en mi dispositivo?

Evita descargarte aplicaciones de desarrolladores desconocidos y con pocas descargas en Google Play pero, sobre todo, **evita descargarte aplicaciones de otras fuentes** por tu cuenta.

Entonces ¿es para tanto?

QuadRooter existe y sí, si alguien quisiera, en determinadas circunstancias podrían aprovecharse de él, eso nadie lo pone en duda. Ahora bien, **¿es motivo para que se cree una alarma social?** Para Check Point estos fallos de seguridad son muy graves, pero es lo esperable dado que es su investigación y se dedican al negocio de la seguridad. Otros no lo ven así y cito, por ejemplo, a Andreas Proschofsky, editor del medio especializado en Open Source der Standard:

> ¿Por qué todo el mundo grita tan fuerte sobre QuadRooter cuando preguntas? Sencillo: Check Point hizo un gran trabajo de marketing. Han creado una app, han elegido de forma inteligente un titular para su blog y contaron con que nadie miraría de cerca. También se aseguraron de que su informe se publicara antes de que los bugs se arreglaran, para que todos y cad uno de los dispositivos mostraran un "vulnerable" cuando los usuarios utilizaran su app para maximizar el factor miedo. Y no puedes realmente culparles por ello (bueno, sí, quizá por la última parte porque es poco profesional), ya que al final es como funcionan estas compañías: encuentran bugs e intentan anunciarlos lo mejor posible para que la gente compre por miedo sus productos. El problema real aquí es que todo el mundo está cayendo en ello porque da un gran y alarmante titular.

En teoría, 900 millones de dispositivos son vulnerables, pero la clave está en el **"en teoría"**. Si no te descargas aplicaciones extrañas procedentes de fuera de Google Play, por ahora estás a salvo.

El "verdadero" problema: las actualizaciones de seguridad en Android

Dejando a un lado el asunto concreto de estas vulnerabilidades, lo que QuadRooter sí pone de manifiesto es todo el trabajo que tanto Google como los fabricantes tienen por delante en lo relativo a las **actualizaciones de seguridad de Android**. Qualcomm fue notificado del problema en abril de 2016, que confirmó los fallos y distribuyó un parche a los fabricantes, pero todavía en agosto no está solucionado.

La solución parcial para los terminales Nexus ha llegado en la actualización de seguridad de Android de este mes, y se completará en septiembre. Pero ¿y el resto de móviles que utiliza chips Qualcomm? Estos todavía no han recibido solución a este problema y podría incluso **no llegar en semanas o hasta meses**. Y ésa, tanto en este caso como en muchos otros de problemas de seguridad anteriores, sí es una vulnerabilidad real.