Cientos de millones de dispositivos, en especial smartphones y tabletas con Android, que utilizan conjuntos de chips Qualcomm, son vulnerables a un nuevo conjunto de vulnerabilidades protencialmente graves.

Según un informe de la compañía de seguridad cibernética CheckPoint, los defectos podrían permitir a los atacantes robar datos confidenciales almacenados en un área segura, que de los contrario, se supone que es la parte más protegida del dispositivo móvil.

Las vulnerabilidades residen en el Entorno de Ejecución Segura de Qualcomm (QSEE), una implementación del Entorno de Ejecución Confiable (TEE) basado en la tecnología ARM TrustZone.

También conocido como Qualcomm´s Secure World, QSEE es un área segura aislada por hardware en el procesador principal, que tiene como objetivo proteger la información confidencial y proporciona un entorno seguro (REE) separado para ejecutar aplicaciones de confianza.

Entre la información confidencial, QSEE por lo general contiene claves de cifrado privadas, contraseñas, credenciales de tarjetas de crédito y débito, entre otra información.

Debido a que se basa en el principio del mínimo privilegio, los módulos del sistema Normal World, somo los controladores y aplicaciones, no pueden acceder a las áreas protegidas a menos que sea necesario, aún cuando se tiene permisos de root.

> *«En un proyecto de investigación de 4 meses, logramos revertir el sistema operativo Secure World de Qualcomm y aprovechamos la técnica de fuzzing para exponer el agujero»,* dijeron los investigadores.
>
> *«Implementamos una herramienta de fuzzing hecha a la medida, que probó el código confiable en dispositivos Samsung, LG y Motorola».*

- dxhdcp2 (LVE-SMP-190005)
- sec_store (SVE-2019-13952)
- authnr (SVE-2019-13949)
- esecomm (SVE-2019-13950)
- kmota (CVE-2019-10574)
- tzpr25 (reconocido por Samsung)
- prov (Motorola trabaja en una solución)

Según los investigadores, las vulnerabilidades reportadas en los componentes seguros de Qualcomm podrían permitir que un atacante haga lo siguiente:

- Ejecutar aplicaciones confiables en el mundo normal (Android).
- Cargar aplicaciones confiables parcheadas en Secure World (QSEE).
- No pasar por la cadena de confianza de Qualcomm.
- Adaptar la aplicación de confianza para ejecutarla en un dispositivo de otro fabricante.

> *«Un hecho interesante es que también podemos cargar tristlets desde otro dispositivo. Todo lo que tenemos que hacer es reemplazar la tabla hash, la firma y la cadena de certificados en el archivo .mdt del trustlet con los extraídos del trustlet del fabricante del dispositivo»,* agregaron los investigadores.

En resumen, una vulnerabilidad en el componente TEE deja a los dispositivos vulnerables a una amplia gama de amenazas de seguridad, incluida la fuga de datos protegidos, el enraizamiento de dispositivos, el desbloqueo del cargador de arranque y la ejecución de APT indetectable.

Las vulnerabilidades también afectan a una gran variedad de teléfonos inteligentes y dispositivos IoT que utilizan el componente QSEE para proteger la información confidencial de los usuarios.

Check Point Research divulgó de forma responsable sus hallazgos a todos los proveedores

afectados, de los cuales, Samsung, Qualcomm y LG lanzaron una actualización para las vulnerabilidades QSEE.