Un grupo de investigadores de la Universidad de Tel Aviv reveló los detalles de vulnerabilidades de diseño «*graves*» ahora parcheadas, que afectan a unos 100 millones de smartphones Samsung basados en Android, que podrían haber resultado en la extracción de claves criptográficas secretas.

Las vulnerabilidades son el resultado de un análisis del diseño criptográfico y la implementación de Keystore respaldado por hardware de Android en los dispositivos Galaxy S8, S9, S10, S20 y S21 de Samsung, según informaron los investigadores *Alon Shakevsky, Eyal Ronen y Avishai Wool.*

Los entornos de ejecución de confianza (TEE) son una zona segura que proporciona un entorno aislado para la ejecución de aplicaciones de confianza (TA) para llevar a cabo tareas críticas de seguridad para garantizar la confidencialidad y la integridad.

En Android, Keystore respaldado por hardware es un sistema que facilita la creación y el almacenamiento de claves criptográficas dentro del TEE, lo que dificulta su extracción del dispositivo de una forma que evita que el sistema operativo subyacente tenga acceso directo.

En cambio, Android Keystore expone las API en forma de Keymaster TA (aplicación confiable) para realizar operaciones criptográficas dentro de este entorno, incluida la generación segura de claves, el almacenamiento y su uso para la firma y el cifrado digitales. En los dispositivos móviles de Samsing, Keymaster TA se ejecuta en un TEE basado en ARM TrustZone.

Sin embargo, las vulnerabilidades de seguridad descubiertas en la implementación de Samsung significaron que podrían proporcionar a un adversario con privilegios de raíz una ruta viable para recuperar las claves privadas protegidas por hardware del elemento seguro. La lista de problemas identificados es la siguiente:

- Reutilización del vector de inicialización (IV) en Keymaster TA (CVE-2021-25444): Una vulnerabilidad de reutilización IV en Keymaster antes de SMR AUG-2021 Release 1, permite el descifrado de keyblob personalizado con un proceso privilegiado. (Impacto en Galaxy S9, J3 Top, J7 Top, J7 Duo, TabS4, Tab-AS-Lite, A6 Plus y A9S)
- Ataque de degradación en Keymaster TA (CVE-2021-25490): Un ataque de degradación de keyblob en Keymaster antes de SMR Oct-2021 Release 1, permite que un atacante active la vulnerabilidad de reutilización IV con un proceso privilegiado (Impacto en Galaxy S10, S20 y S21)

La explotación exitosa de las vulnerabilidades contra Keymaster TA podría lograr el acceso no autorizado a claves protegidas por hardware y datos asegurados por el TEE. Las implicaciones de un ataque de este tipo podrían variar desde una omisión de autenticación hasta ataques avanzados que pueden romper las garantías de seguridad fundamentales que ofrecen los sistemas criptográficos.

Después de la divulgación responsable en mayo y julio de 2021, los problemas se solucionaron mediante actualizaciones de seguridad enviadas en agosto y octubre de 2021 para los dispositivos afectados. Se espera que los hallazgos se presenten en el Simposio de Seguridad de USENIX a fines de agosto.

> *«Los proveedores, incluidos Samsung y Qualcomm, mantienen en secreto la implementación y el diseño de los sistemas operativos TrustZone y Tas. Los detalles de diseño e implementación deben ser bien auditados y revisados por investigadores independientes y no deben depender de la dificultad de los sistemas patentados de ingeniería inversa»,* dijeron los investigadores.