Se identificaron fallas de seguridad en los modelos Xiaomi Redmi Note 9T y Redmi Note 11, que podría ser explotadas para deshabilitar el mecanismo de pago móvil e incluso, falsificar transacciones a través de una aplicación de Android no autorizada instalada en los dispositivos.

Check Point dijo que encontró las vulnerabilidades en los dispositivos alimentados por conjuntos de chips MediaTek durante un análisis de seguridad del entorno de ejecución confiable (TEE) *«Kinibi»* del fabricante chino de teléfonos móviles.

Un TEE se refiere a un enclave seguro dentro del procesador principal que se usa para procesar y almacenar información confidencial, como claves criptográficas, para garantizar la confidencialidad y la integridad.

Específicamente, la compañía de ciberseguridad israelí descubrió que una aplicación confiable en un dispositivo Xiaomi puede degradarse debido a la falta de control de versiones, lo que permite a un atacante reemplazar una versión más nueva y segura de una aplicación con una variante más antigua y vulnerable.

> *«Por lo tanto, un atacante puede eludir las correcciones de seguridad realizadas por Xiaomi o MediaTek en aplicaciones confiables al degradarlas a versiones sin parches»,* dijo el investigador de Check Point, Slava Makkaeveev.

Además, se identificaron varias vulnerabilidades en *«thhadmin»*, una aplicación confiable que es responsable de la administración de la seguridad, que podría ser abusada por una aplicación maliciosa para filtrar claves almacenadas o ejecutar código arbitrario en el contexto de la aplicación.

> *«Descubrimos un conjunto de vulnerabilidades que podrían permitir la falsificación de paquetes de pago o la desactivación del sistema de pago directamente desde una aplicación de Android sin privilegios»,* dijo Makkaveev en un comunicado.

Las vulnerabilidades apuntan a una aplicación confiable desarrollada por Xiaomi para implementar operaciones criptográficas relacionadas con un servicio llamada *Tencent Soter*, que es un *«estándar biométrico»* que funciona como un marco de pago móvil integrado para autorizar transacciones en aplicaciones de terceros que usan WeChat y Alipay.

Pero una vulnerabilidad de desbordamiento de montón en la aplicación de confianza soter significaba que podría ser explotada para inducir una denegación de servicio por parte de una aplicación de Android que no tiene permisos para comunicarse directamente con el TEE.

Además, al encadenar el ataque de degradación antes mencionado para reemplazar la aplicación de confianza de soter a una versión anterior que contenía una vulnerabilidad de lectura arbitraria, Check Point descubrió que era posible extraer las claves privadas utilizadas para firmar paquetes de pago.

> *«La vulnerabilidad compromete por completo la plataforma soter de Tencent, lo que permite que un usuario no autorizado firme paquetes de pago falsos»,* dijo la compañía.

Xiaomi, después de una divulgación responsable, lanzó parches para abordar CVE-2020-14125 el 6 de junio de 2022. *«El problema de degradación, que Xiaomi confirmó que pertenece a un proveedor externo, se está solucionando»*, dijo Check Point.