Investigadores de seguridad cibernética revelaron una vulnerabilidad no reparada en Apple Pay, que los hackers pueden abusar para realizar un pago Visa no autorizado con un iPhone bloqueado aprovechando el modo Express Travel configurado en la billetera del dispositivo.

> *«Un atacante sólo necesita un iPhone robado en su poder. Las transacciones también pueden ser transmitidas desde un iPhone dentro de la bolsa de alguien, sin su consentimiento. El atacante no necesita ayuda del comerciante y los controles de detección de fraude de backend no han detenido ninguno de nuestros pagos de prueba»,* dijo un grupo de académicos de la Universidad de Birmingham y la Universidad de Surrey.

Express Travel es una función que permite a los usuarios de iPhone y Apple Watch realizar pagos rápidos sin contacto para el transporte público sin tener que activar o desbloquear el dispositivo, abrir una aplicación o incluso validar con Face ID, Touch ID o una contraseña.

El ataque de repetición y retransmisión del hombre en el medio (MitM), que implica eludir la pantalla de bloqueo para realizar un pago a cualquier lector EMV de forma ilícita, es posible debido a una combinación de fallas en el sistema de Apple Pay y Visa, y no afecta a Mastercard en Apple Pay o tarjetas Visa en Samsung Pay.

El modus operandi se basa en imitar una transacción de puerta de tránsito mediante el uso de un dispositivo Proxmark que actúa como un lector de tarjetas EMV que se comunica con el iPhone de la víctima y una aplicación de Android habilitada para NFC que funciona como un emulador de tarjeta para transmitir señales a una terminal de pago.

Específicamente, aprovecha un código único, también conocido como Magic Bytes, transmitido por las puertas de tránsito para desbloquear Apple Pay, lo que da como resultado un escenario en el que, al reproducir la secuencia de bytes, el dispositivo Apple es engañado para autorizar una transacción no autorizada como si se hubiera originado en la barrera de los billetes, cuando en realidad, se ha activado por medio de una terminal de pago sin contacto bajo el control del atacante.

Al mismo tiempo, también se engaña al lector EMV para que crea que se ha realizado la autenticación del usuario en el dispositivo, lo que permite realizar pagos de cualquier monto sin el conocimiento del usuario del iPhone.

Apple y Visa fueron alertados sobre la vulnerabilidad en octubre de 2020 y mayo de 2021, respectivamente, dijeron los investigadores, y agregaron que *«ambas partes reconocen la gravedad de la vulnerabilidad, pero no han llegado a un acuerdo sobre qué parte debería implementar una solución».*

En un comunicado compartido con la BBC, Visa dijo que este tipo de ataque era *«poco práctico»*, y agregó que: *«las variaciones de los esquemas de fraude sin contacto se han estudiado en entornos de laboratorio durante más de una década y han demostrado ser imprácticas para ejecutar a escala en el mundo real».*

> *«Esta es una preocupación con el sistema Visa, pero Visa no cree que este tipo de fraude pueda ocurrir en el mundo real dadas las múltiples capas de seguridad existentes»*, dijo un portavoz de Apple a la emisora nacional del Reino Unido.

Por otro lado, esta forma de pago se está implementando cada vez más en diversos países. Recientemente la Ciudad de México implementó máquinas de pago con tecnología sin contacto para el Metrobus de la ciudad.