Investigadores de ciberseguridad han descubierto una puerta trasera en el hardware de un modelo específico de tarjetas sin contacto MIFARE Classic, lo que podría permitir la autenticación con una clave desconocida y abrir puertas de oficinas y habitaciones de hotel.

Se han demostrado ataques contra el modelo FM11RF08S, una nueva variante de MIFARE Classic lanzada por Shanghai Fudan Microelectronics en 2020.

> *«La puerta trasera del FM11RF08S permite que cualquier persona que tenga conocimiento de ella comprometa todas las claves definidas por el usuario en estas tarjetas, incluso si están completamente diversificadas, simplemente accediendo a la tarjeta durante unos minutos»*, explicó Philippe Teuwen, investigador de Quarkslab.

La investigación reveló que la clave secreta no solo es común a las tarjetas FM11RF08S existentes, sino que *«los ataques podrían ejecutarse de inmediato por una entidad con la capacidad de realizar un ataque en la cadena de suministro.»*

Para complicar aún más la situación, se ha identificado una puerta trasera similar en la generación anterior, FM11RF08, protegida con una clave diferente. Esta puerta trasera ha sido detectada en tarjetas emitidas desde noviembre de 2007.

Una versión mejorada del ataque podría acelerar el proceso de descifrado de una clave entre cinco y seis veces mediante la ingeniería inversa parcial del mecanismo de generación de nonce.

> *«La puerta trasera [...] permite clonar instantáneamente tarjetas inteligentes RFID utilizadas para abrir puertas de oficinas y habitaciones de hotel en todo el mundo»*, indicó la empresa en un comunicado.

> *«Aunque la puerta trasera requiere solo unos minutos de proximidad física a una tarjeta afectada para realizar un ataque, un atacante que tenga la capacidad de llevar a cabo un ataque en la cadena de suministro podría ejecutar estos ataques de forma instantánea y a gran escala.»*

Se recomienda a los usuarios verificar si están en riesgo, especialmente dado que estas tarjetas se utilizan ampliamente en hoteles de los Estados Unidos, Europa e India.

La puerta trasera y su clave *«nos permiten realizar nuevos ataques para volcar y clonar estas tarjetas, incluso si todas sus claves están debidamente diversificadas»,* señaló Teuwen.

No es la primera vez que se descubren problemas de seguridad en sistemas de cierre utilizados en hoteles. A principios de marzo, se encontró que las cerraduras electrónicas RFID Saflok de Dormakaba presentaban fallas graves que podrían ser explotadas por actores malintencionados para falsificar tarjetas clave y abrir puertas.