Dormakaba ha emitido una *«alerta de seguridad urgente»* el viernes, advirtiendo que dos versiones de su popular cerradura electrónica de RFID, Saflok, utilizada en hoteles, han sido comprometidas con código malicioso diseñado para permitir el acceso remoto no autorizado.

Estas vulnerabilidades han sido bautizadas conjuntamente como «*Unsaflok*» por un grupo de investigadores compuesto por Lennert Wouters, Ian Carroll, rqu, BusesCanFly, Sam Curry, sshell y Will Caruana. El problema fue reportado a la empresa con sede en Zúrich en septiembre de 2022.

> *«La combinación de las debilidades identificadas permite a un atacante desbloquear todas las habitaciones de un hotel utilizando un único par de tarjetas llave falsificadas»,* explicaron.

Por razones de seguridad, los detalles técnicos completos sobre las vulnerabilidades han sido retenidos y se espera que se publiquen en el futuro.

Estos problemas afectan a más de tres millones de cerraduras de hotel distribuidas en 13,000 propiedades en 131 países. Esto incluye modelos como Saflok MT, Quantum, RT, Saffire y Confidant, que se utilizan en conjunto con software de gestión como System 6000, Ambiance y Community.

Según estimaciones, Dormakaba ha actualizado o reemplazado el 36% de las cerraduras afectadas hasta marzo de 2024 como parte de un proceso de implementación iniciado en noviembre de 2023. Algunas de estas cerraduras vulnerables han estado en uso desde 1988.

> *«Un atacante solo necesita leer una tarjeta llave de la propiedad para llevar a cabo el ataque en cualquier puerta de la propiedad. Esta tarjeta llave puede ser de su propia habitación o incluso una tarjeta llave caducada tomada de la caja de recolección de check-out exprés»,* destacaron los investigadores.

Para crear las tarjetas falsificadas, se puede utilizar cualquier tarjeta MIFARE Classic o herramientas RFID comerciales que sean capaces de escribir en estas tarjetas. Alternativamente, dispositivos como Proxmark3, Flipper Zero o incluso un teléfono Android con NFC pueden ser utilizados en lugar de las tarjetas.

En una entrevista con Andy Greenberg de WIRED, los investigadores explicaron que el ataque implica leer un código específico de la tarjeta y crear un par de tarjetas falsificadas utilizando el método mencionado anteriormente: una para reprogramar los datos de la cerradura y otra para abrir la puerta mediante la descifrado del sistema de encriptación de la Función de Derivación de Claves (KDF) de Dormakaba.

> *«Con solo dos toques rápidos, abrimos la puerta»,* señaló Wouters.

Otro paso importante implica el análisis inverso de los dispositivos de programación de cerraduras distribuidos por Dormakaba en hoteles y el software de recepción utilizado para gestionar las tarjetas llave. Esto permitió a los investigadores falsificar una llave maestra de trabajo que podría ser utilizada para abrir cualquier puerta.

Aunque no se ha confirmado ningún caso de explotación de estos problemas en la naturaleza, los investigadores no descartan la posibilidad de que las vulnerabilidades hayan sido descubiertas o utilizadas por otros.

> *«Es posible detectar ciertos ataques mediante la auditoría de los registros de entrada/salida de la cerradura. El personal del hotel puede realizar esta auditoría a través del dispositivo HH6 y buscar registros de entrada/salida sospechosos. Debido a la vulnerabilidad, los registros de entrada/salida podrían ser atribuidos incorrectamente a la tarjeta llave o al miembro del personal»,* agregaron.

Este descubrimiento se produce después de la identificación de tres vulnerabilidades críticas

de seguridad en Dispositivos Electrónicos de Registro (ELDs) comúnmente utilizados en la industria del transporte de camiones, que podrían ser aprovechadas para obtener un control no autorizado sobre los sistemas del vehículo y manipular datos y operaciones del vehículo de manera arbitraria.

Más preocupante aún, una de las fallas podría abrir el camino para un gusano auto-propagante de camión a camión, lo que podría causar interrupciones generalizadas en las flotas comerciales y tener graves consecuencias de seguridad.