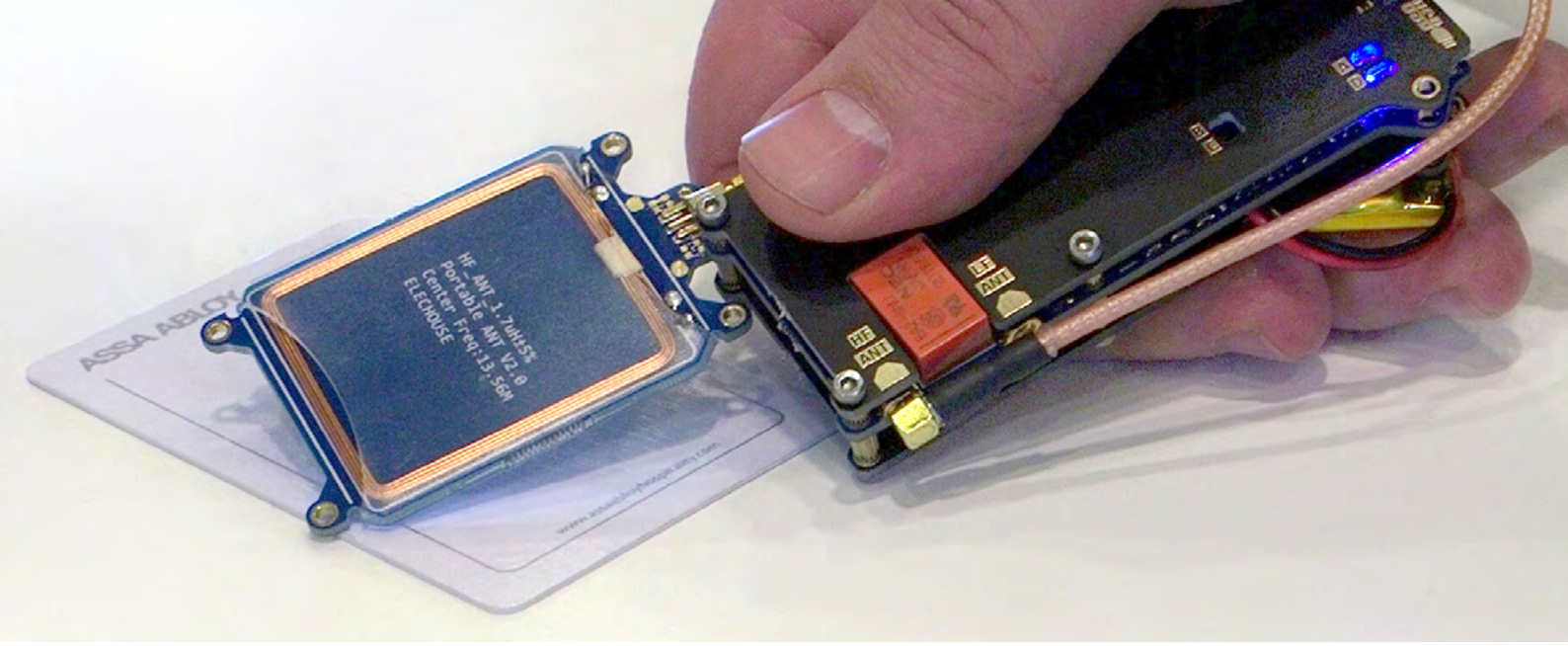

FAQ

GHOST IN THE LOCKS

F-Secure has found a design flaw which allows opening hotel room doors across the world without being noticed

WHAT IS THE SECURITY ISSUE?

F-Secure researchers, Tomi Tuominen and Timo Hirvonen, found critical design flaws in Assa Abloy Hospitality's widely deployed hotel lock software system, Vision by Vingcard.

HOW WOULD AN ATTACKER EXPLOIT THE FLAWS?

First an attacker needs to get access to an electronic key to the target facility. Literally any key will do, be it a room key or a key to a storage closet or garage. What's more, the key does not need to be currently active - even an expired key from a stay five years ago will work.

An attacker will read the key and use a small hardware device to derive more keys to the facility. These derived keys can be tested against any lock in the facility. Within minutes, the device is able to generate a master key to the facility. The device can then be used in place of a key to bypass any lock in the facility, or alternatively overwrite an existing key to contain the master key.

WHAT ELSE WAS FOUND?

In addition, during their research Tuominen and Hirvonen found that the Vision software could be exploited within the same network to get access to sensitive customer data.

WHO IS ASSA ABLOY AND WHY WAS THE BRAND CHOSEN?

Based in Sweden, Assa Abloy is the world's largest lock manufacturer. Assa Abloy Hospitality is the division of the company that provides lock systems for hotels, cruise ships and other industries. However, the software Vision, which is impacted by the attack, is used in hotels and cruise ships only. The researchers decided to target Assa Abloy, a brand of lock known for quality and security.
https://www.assaabloyhospitality.com/en/aah/com/solutions/

HAS THE PROBLEM BEEN FIXED?

Assa Abloy has fixed the flaws in the Vision software and issued software updates. Hotels that have applied the updates to their systems are not vulnerable.

More information on the fix can be found here:
https://assaabloyhospitality.service-now.com/user_registration_request.do?sys_id=-1&sysparm_view=ess

WHICH HOTEL BRANDS ARE IMPACTED?

Hotels using Assa Abloy's widely deployed Vision software system are affected. The Vision software is used by independent hotels and local hotel chains as well as some well-known global brands.

Read more:
https://www.assaabloyhospitality.com/en/aah/com/case-studies/case-studies-and-references/

Assa Abloy also has other hospitality software systems which are not affected.

WHY DID F-SECURE DO THIS RESEARCH?

Our researchers' interest in hotel locks was sparked more than a decade ago when a colleague's laptop was stolen from a locked hotel room. There was no hint of unauthorized entry physically in the hotel room or digitally in the software logs, so the hotel staff didn't take their theft complaint seriously. This got our researchers wondering if it's really possible to break into a hotel room without being noticed by manipulating the lock system.

WHY IS F-SECURE DISCLOSING VULNERABILITIES?

Vulnerability research is vital to improve products and provide better security to everyone - security through obscurity doesn't work. We are committed to addressing and reporting security issues through a coordinated and constructive approach for which we aim to balance the need of the public to be informed of security issues with vendors' needs for time to respond effectively.

WHY DID THE RESEARCH TAKE OVER A DECADE TO COMPLETE?

Figuring out the complexities of how the lock system, software and keys worked was very complicated. Building, and breaking, an electronic access control system is very difficult because there are many facets to get right. Assa Abloy is a highly reputed lock manufacturer and aside from the seemingly innocuous security oversights in the software, their products are well designed.

These security oversights were not gaping obvious holes. It took a thorough understanding of the design of the whole system to be able to identify small flaws in the system. The researchers then creatively combined these flaws to produce the attack.

HAVE THESE DESIGN FLAWS EVER BEEN EXPLOITED IN THE WILD?

We have no reports of any incidents currently that involves hacking of Assa Abloy Vingcard locks and do not know of any particular cases where these same flaws have been exploited in the wild. But of course we can not say with certainty that they have not been exploited.

ARE HOTEL CUSTOMERS AT RISK?

There are easier ways to access a hotel room. Full details of the attack method will not be revealed, and the software tools will not be made available. In addition, criminals who are interested in breaking into hotel rooms by hacking into the lock system this way need deep technical knowledge and a considerable time investment, as our work demonstrates. However, we should never assume that no one else has made the same discovery we have, so applying the software update is highly recommended.