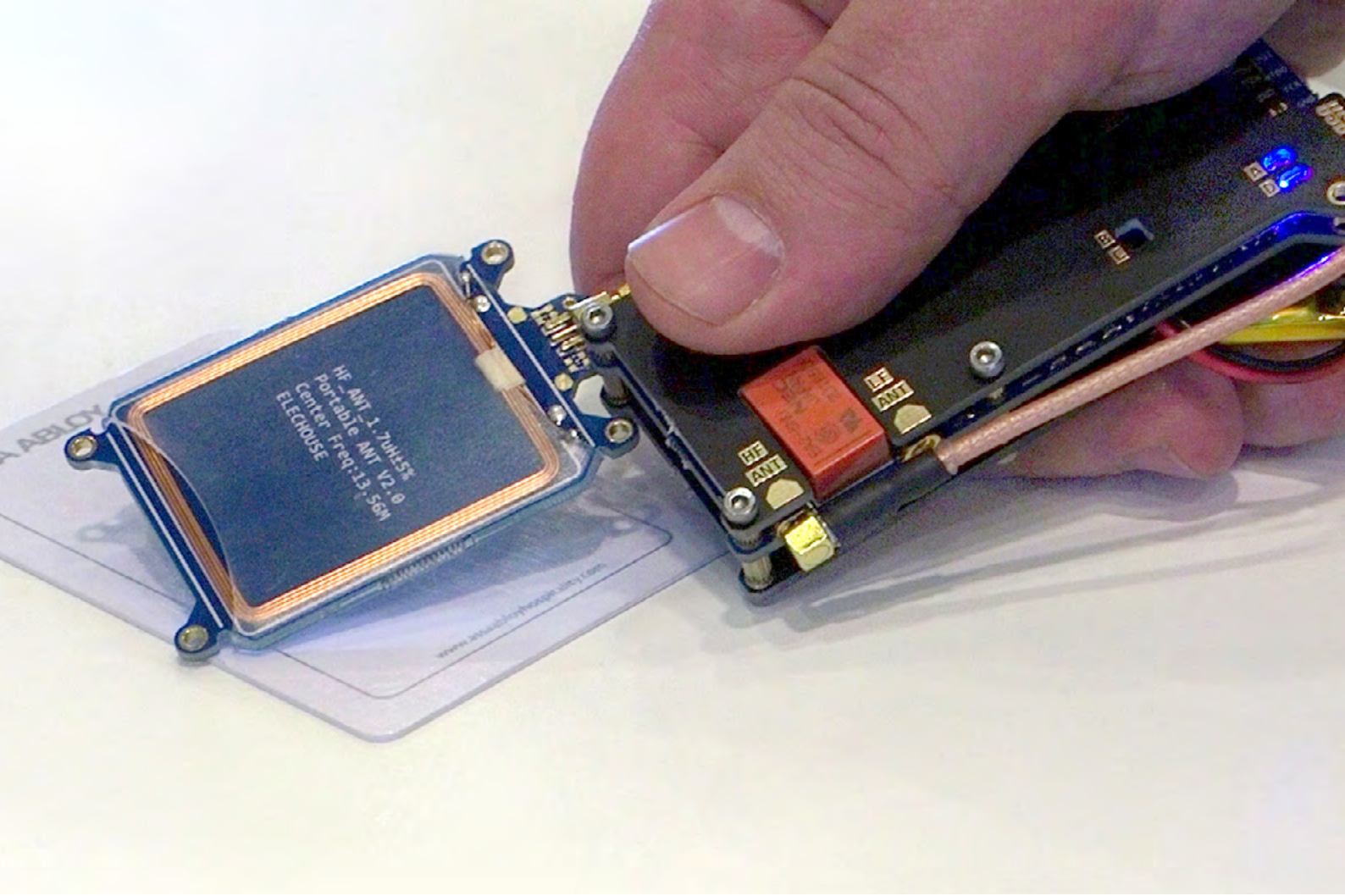

FAQ

VULNÉRABILITÉ GHOST IN THE LOCKS

F-Secure a trouvé un défaut de conception dans un système de serrures électroniques utilisé par des établissements hôteliers du monde entier. Cette faille permet d'ouvrir les portes des chambres d'hôtel, sans se faire remarquer.

EN QUOI CONSISTE LE PROBLÈME DE SÉCURITÉ OBSERVÉ ?

Tomi Tuominen et Timo Hirvonen, chercheurs chez F-Secure, ont découvert des défauts de conception dans le logiciel du système de fermeture Vision de VingCard.

COMMENT UN PIRATE PEUT-IL EXPLOITER CES DÉFAUTS DE CONCEPTION ?

Tout d'abord, l'attaquant doit commencer par obtenir une clé électronique, appartenant à l'établissement ciblé. Il peut s'agir de n'importe quelle clé de chambre ou utilisée pour accéder à des espaces secondaires comme un placard. De

plus, la clé n'a pas besoin d'être en cours de validité – une carte périmée depuis des années marchera.

Un attaquant lira la clé et utilisera un petit appareil spécialisé pour attribuer à ladite clé les droits nécessaires pour ouvrir toutes les portes de l'établissement. En quelques minutes, l'appareil est capable de générer une clé 'maître'. Cet appareil peut être utilisé à la place d'une clé classique pour ouvrir toutes les serrures de l'établissement, ou alternativement remplacer une clé existante par la clé 'maître'.

QUELS SONT LES AUTRES RÉSULTATS DE CETTE RECHERCHE ?

En outre, Tomi Tuominen et Timo Hirvonen ont également découvert au cours de leurs recherches que le logiciel Vision pouvait être exploité et permettre l'accès à des données-clients sensibles.

QU'EST-CE QUE L'ENTREPRISE ASSA ABLOY ET POURQUOI CELLE-CI A-T-ELLE ÉTÉ CHOISIE ?

Basé en Suède, Assa Abloy est le plus grand fabricant de serrures au monde. Assa Abloy Hospitality est la branche de l'entreprise chargée de fournir aux hôtels, bateaux de croisière et autres structures, des systèmes de serrures électroniques. Le logiciel Vision, concerné par l'expérimentation, n'est utilisé que dans les hôtels et sur les paquebots de croisière. Les chercheurs ont décidé de cibler Assa Abloy car cette marque de serrure est réputée pour sa qualité et sa sécurité.
https://www.assaabloyhospitality.com/fr/aah/com/solutions/

LE PROBLÈME A-T-IL ÉTÉ RÉSOLU ?

Assa Abloy a patché le logiciel Vision et publié des mises à jour. Les hôtels ayant installé les mises à jour sur leurs systèmes ne sont plus vulnérables.

Plus d'informations sur le patch ici :
https://assaabloyhospitality.service-now.com/user_registration_request.do?sys_id=-1&sysparm_view=ess

QUELLES SONT LES CHAINES D'HÔTELS POUVANT ÊTRE IMPACTÉES ?

Tous les hôtels utilisant le logiciel Vision d'Assa Abloy (système largement répandu) sont concernés. Le logiciel Vision est utilisé par des hôtels indépendants et des chaînes hôtelières locales ainsi que par certaines chaines mondiales bien connues.

En savoir plus :
https://www.assaabloyhospitality.com/en/aah/com/case-studies/case-studies-and-references/

Assa Abloy dispose également d'autres systèmes logiciels destinés à l'hôtellerie mais ceux-là ne sont pas concernés.

POURQUOI LES CHERCHEURS F-SECURE ONT-ILS MENÉ CETTE RECHERCHE ?

Les chercheurs F-Secure ont commencé à s'intéresser au piratage de serrures dans les hôtels il y a dix ans, lorsque l'ordinateur portable d'un collègue a été dérobé dans une chambre, lors d'une conférence en cyber sécurité. Lorsque les chercheurs ont signalé le vol, le personnel de l'hôtel n'a pas pris leur plainte pour vol au sérieux, expliquant que la chambre ne présentait aucun signe d'effraction.

Cela a amené nos chercheurs à se demander s'il était possible d'entrer par effraction dans une chambre d'hôtel sans se faire remarquer, en manipulant le système de verrouillage.

POURQUOI L'ENTREPRISE F-SECURE CHOISIT-ELLE AUJOURD'HUI DE RÉVÉLER CES VULNÉRABILITÉS ?

La recherche des vulnérabilités est essentielle à l'amélioration des produits. Elle permet de nous assurer, à tous, une meilleure sécurité. Nous nous engageons à signaler les problèmes de sécurité, via une approche coordonnée et constructive. Nous veillons à trouver un équilibre entre la nécessité d'informer le public et le temps dont le fournisseur peut avoir besoin pour remédier efficacement au problème.

POURQUOI LES CHERCHEURS ONT-ILS EU BESOIN DE DIX ANS POUR MENER À BIEN CETTE EXPÉRIMENTATION ?

Il était très compliqué de comprendre comment fonctionnement un système de serrure électronique : les clés et le logiciel sont très complexes. Construire ou briser un système de contrôle d'accès électronique s'avère en pratique très difficile : de nombreux aspects sont à prendre en compte. Assa Abloy est un fabricant de serrures très réputé et, en dehors de ces quelques défauts de sécurité en apparence inoffensifs présents au sein du logiciel, leurs produits sont bien conçus.

Les défauts de conception mis en évidence n'avaient rien de flagrant. Il a fallu une compréhension approfondie de la conception de l'ensemble du système pour identifier ces points faibles. Ce n'est qu'en exploitant l'ensemble de ces petits défauts que les chercheurs ont pu créer une attaque efficace. La recherche a nécessité plusieurs milliers d'heures et un nombre considérable d'essais-erreurs.

CES DÉFAUTS DE CONCEPTION ONT-ILS DÉJÀ ÉTÉ EXPLOITÉS PAR DES PIRATES EN CONDITIONS RÉELLES ?

Nous n'avons jusque-là reçu aucun rapport d'incidents mentionnant le piratage de serrures Assa Abloy Vingcard. Nous n'avons connaissance d'aucun cas de piratage de ce type en conditions réelles. Bien entendu, il reste impossible d'affirmer avec certitude que ces défauts de conception n'ont jamais été exploités.

LES CLIENTS DES HÔTELS CONCERNÉS SONT-ILS EN DANGER ?

Il y a des méthodes plus faciles pour accéder à une chambre d'hôtel. Les détails de la méthode d'attaque utilisée ne seront pas révélés, et les outils logiciels ne seront bien entendu pas mis à disposition. Si des criminels cherchaient à pénétrer par effraction dans des chambres d'hôtel en piratant ainsi le système de serrure, ils auraient besoin de connaissances techniques approfondies et d'un temps considérable, comme le démontre notre travail. Il serait toutefois dangereux de supposer que personne d'autre ne fera la même découverte que nous. L'installation de la mise à jour logiciel est donc fortement recommandée.