Product Security Advisory

21/11/2022

Yale Keyless Smart Lock

(Yale-PA-2022-02)

Overview

As the global leader in access solutions, safety and security are at the core of what we do as a company. Product security is of utmost importance for us, and we take any potential issues regarding our products very seriously.

With this in mind, we have become aware of a potential vulnerability affecting the RFID implementation within certain versions of the Yale Keyless Smart Lock product (YD-01-CON) sold in the United Kingdom and South Africa.

The affected products are mainly used by end users in residential dwellings that typically have an additional security layer in place, such as a secondary lock.

According to a thorough risk analysis by internal experts, the risk to the overall security of our Yale Keyless Smart Lock customers is not high. We are not aware of any instances where the vulnerability has enabled unauthorised access to a property.

Our investigation followed our Product Security Incident Response (PSIR) Policy that outlines a process to identify affected products, assess any potential implications for our customers, determine what mitigation steps should be taken and to notify customers.

As part of this investigation, ASSA ABLOY would like to thank security researchers Sharad Agarwal and Joseph Gardiner (University of Bristol Cyber Security Group) for their expertise and assistance following their responsible disclosure of the potential vulnerability and subsequent collaboration with us in relation to this issue.

Advisory Status

Investigation Complete

While our product investigation is complete, we will continue to monitor any security risks and will provide updates should the situation change.

Product Name		Affected Versions
Keyless Connected	**(YD-01-CON)**	Before 2.0

Vulnerability Description

The implementation of the RFID within certain versions of the Keyless Smart Lock product uses MIFARE CLASSIC® cards which are vulnerable to cloning attacks. Further anti-cloning measures to roll codes introduced in other smart locks, were not added to the Keyless Connected.

IMPACT

According to a thorough risk analysis by internal experts, the risk to the overall security of our Yale Keyless Smart Lock customers is medium.

Successfully cloning a vulnerable credential allows a possible threat actor to gain unauthorised access to the same locks as the original credential holder. Close proximity, or direct physical access, is required to read an unprotected physical credential to obtain its data. Cloning the credential does not allow a possible threat actor to modify the data in such a way as to grant additional access from that stored on the original credential.

We are not aware of any instances where the vulnerability has enabled unauthorised access to a property.

SEVERITY

Severity of the vulnerability calculated according to CVSS v3.1 https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Score 4.6/10 (Medium)
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:F/RL:W

MITIGATION

Based on our risk assessment, we recommend the following mitigation actions in order to reduce the potential risk to our customers:

- Switch to using one of the other credentials available for your smart lock (PIN, App), which are unaffected by this vulnerability.
- Always keep your card out of reach of people you don't know and trust (especially in public places), keep your card safe and secure.

You might also consider the following additional precautions:

- Keyless Smart Locks, like other non-BSI rated night latch products, are best fitted in conjunction with a secondary lock when used on entrance doors, to provide an extra layer of security and limit the exposure if a credential is compromised.
- Never print identifiers such as names or property details on the physical credential itself and ensure users keep the physical credential safe.

OUR COMMITTMENT TO YOU

We are committed to creating safe and reliable products. As part of that commitment, we consistently monitor, assess and optimise our technology to better ensure the safety and security of our customers and products.

Contact Information

For further information, please do not hesitate to contact our Security Team via the following emails:

- security@assaabloy.com
- emeia.productsecurity@assaabloy.com

Thank you for your continued support and trust in Yale products.

The Yale Team

REVISION	DATE	DESCRIPTION
1.0	21/11/2022	Initial publication of the advisory