Product Advisory
5th Nov 2025

Yale ENTR
(Yale-EN-PA-2025-01)

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 two potential vulnerabilities affecting the Bluetooth communication for the discontinued Yale ENTR Smart Lock product series, previously sold globally before November 2021 and in Israel before May 2024.

The affected products are mainly used by end users in residential dwellings that typically have an additional security layer in place, such as unlocking by PIN code or by fingerprint.

We are not aware of any instances where the vulnerabilities have been successful in the field. 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 researcher Tobias Funke for his expertise and assistance following a responsible disclosure of the vulnerabilities and subsequent collaboration with us in relation to mitigating this issue.

Advisory Status

Investigation Complete

Whilst our investigation is complete, we will continue to monitor and assess the situation as part of our ongoing product security procedures.

Vulnerability Description

Product Name: Yale ENTR Smart Lock product series

The implementation of the Bluetooth communication between the ENTR lock and the user's smartphone is potentially vulnerable to a local attacker being able to take control of an authorized user’s existing Bluetooth session if in close proximity to the ENTR lock. The Bluetooth implementation is also potentially vulnerable to a local adversary that is able to record an authorized user’s Bluetooth session establishment to reproduce it at a later point in time. In both cases the attack needs to be initiated within Bluetooth range of the lock, when an authorized user is interacting with the lock.

IMPACT

According to a thorough risk analysis by internal experts, the risk to the overall security of our Yale ENTR customers is medium. Successfully performing an attack using the vulnerabilities in the Bluetooth implementation requires an adversary to be in close proximity to the lock and successfully record an active Bluetooth communication between a user's phone and the lock. A successful attack on one lock does not grant success to any other locks, thus limiting the possibility to scale up any attacks. We are not aware of any instances where the vulnerability has enabled unauthorised access to a property.

SEVERITY

Severity of the vulnerabilities are calculated according to CVSS v3.1 https://www.first.org/cvss/v3.1/specification-document

Score 5.9 (Medium)

CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L

Score 6.7 (Medium)

CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:L

MITIGATION

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

- To install the latest updated version of the ENTR app, which reduces the likelihood of a successful incident.

- Switch to using one of the other credentials available for your lock (PIN-code or Fingerprint), which are unaffected by this vulnerability.

- Always be aware of any unknown electronic devices placed near your property, especially in proximity to your door.

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

- product.security@assaabloy.com

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

The Yale Team