Product Advisory
2024-12-04

Yale Home Mobile API
(Yale-YH-PA-2024-01)

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 recently became aware of a security vulnerability in the Yale Home mobile API which could have potentially led to an account takeover.

The vulnerability was identified and verified in cooperation with university researchers affiliated with the University of Modena and Reggio Emilia (Italy) and the University of Bologna (Italy): Mirco Marchetti, Michele Mosca, Dario Stabili, and Filip Valgimigli, whom we would like to thank for their valuable collaboration and support provided.

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.

Advisory Status

Investigation Complete

While our investigation is complete and a solution for the vulnerability has been deployed, we will continue to monitor any potential security vulnerabilities as part of our regular process and procedures and will provide updates where necessary.

Vulnerability Description

An error to the authorisation mechanism was identified that, under certain circumstances, could have led to potential unauthorised modification of the user account. A potential threat actor could have manipulated the forgot password flow to change a Yale Home user's email address and phone number, if one of those values was known to them. This would have potentially enabled them to change the password, which would have then led to an account takeover.

IMPACT

According to a thorough risk analysis by internal experts, the risk to the overall security of our Yale Home customers was medium. To our knowledge we are not aware of any instances of the vulnerability being actively misused. No actions are required to be taken by users of Yale Home and customers can continue to use the Yale Home app safely and securely.

SEVERITY

The severity of the vulnerability has been calculated according to CVSS v4.0
https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf

Score 6.9/10 (Medium)
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

OUR COMMITMENT 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:

- product.security@assaabloy.com

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

The Yale Team

REVISION HISTORY

REVISION	DATE	DESCRIPTION
1.0	2024-12-04	Initial publication of the advisory