



## คำแนะนำสินค้า

2024-12-04

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

### ภาพรวม

ในฐานะผู้นำระดับโลกด้านโซลูชันการควบคุมการเข้าออก ความปลอดภัยและความมั่นคงถือเป็นหัวใจสำคัญของสิ่งที่เราทำเสมอ ความปลอดภัยของผลิตภัณฑ์จึงเป็นเรื่องที่เรายึดถืออย่างจริงจัง และเราดำเนินการอย่างเต็มที่เมื่อพบปัญหาหรือประเด็นที่อาจกระทบกับความปลอดภัยของผลิตภัณฑ์ของเรา

ล่าสุด เราได้รับแจ้งถึงช่องโหว่ด้านความปลอดภัยในระบบ Yale Home Mobile API ซึ่งในบางกรณีอาจนำไปสู่ความเสี่ยงในการถูกยึดบัญชีผู้ใช้งาน

ช่องโหว่นี้ถูกค้นพบและตรวจสอบยืนยันโดยนักวิจัยจากมหาวิทยาลัย University of Modena and Reggio Emilia (อิตาลี) และ University of Bologna (อิตาลี) ได้แก่ Mirco Marchetti, Michele Mosca, Dario Stabili และ Filip Valgimigli เราขอขอบคุณนักวิจัยทุกท่านสำหรับความร่วมมือและการสนับสนุนที่มีคุณค่าในครั้งนี้

การตรวจสอบครั้งนี้เป็นไปตามนโยบายการตอบสนองเหตุการณ์ด้านความปลอดภัยของผลิตภัณฑ์ (PSIR Policy) ซึ่งกำหนดขั้นตอนในการระบุผลิตภัณฑ์ที่ได้รับผลกระทบ ประเมินผลกระทบที่อาจเกิดขึ้นกับลูกค้า กำหนดแนวทางการแก้ไขที่เหมาะสม และแจ้งข้อมูลให้ลูกค้าทราบ

### สถานะ

#### การตรวจสอบเสร็จสมบูรณ์แล้ว

แม้ว่าการตรวจสอบจะเสร็จสิ้นและมีการดำเนินการแก้ไขช่องโหว่นี้เรียบร้อยแล้ว แต่เรายังคงดำเนินการติดตามและเฝ้าระวังช่องโหว่ด้านความปลอดภัยอย่างสม่ำเสมอตามขั้นตอนมาตรฐานของเรา และหากมีข้อมูลเพิ่มเติม เราจะรีบแจ้งให้ลูกค้าทราบโดยเร็วที่สุด

#### รายละเอียดของช่องโหว่

เราพบข้อผิดพลาดในกระบวนการตรวจสอบสิทธิ์ (Authorization Mechanism) ซึ่งในบางสถานการณ์ อาจทำให้ผู้ไม่ประสงค์ดีสามารถเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้ได้โดยไม่ได้รับอนุญาต

โดยผู้ไม่หวังดีอาจใช้ช่องทางการรีเซตรหัสผ่าน ('ลืมรหัสผ่าน') เพื่อเปลี่ยนอีเมลหรือหมายเลขโทรศัพท์ของผู้ใช้งาน หากพวกเขาทราบข้อมูลส่วนตัวเหล่านี้ จากนั้นจึงตั้งรหัสผ่านใหม่ได้ ซึ่งนำไปสู่การยึดบัญชีได้ในที่สุด

## ผลกระทบ (IMPACT)

จากการวิเคราะห์ความเสี่ยงอย่างละเอียดโดยทีมผู้เชี่ยวชาญของเรา  
ระบุว่าความเสี่ยงโดยรวมที่มีต่อความปลอดภัยของลูกค้ายale Home อยู่ในระดับปานกลาง

จนถึงขณะนี้ เรายังไม่พบหลักฐานว่าช่องโหว่นี้ถูกนำไปใช้ในทางที่ผิดแต่อย่างใด นอกจากนี้  
ลูกค้าไม่จำเป็นต้องดำเนินการใด ๆ เพิ่มเติม และสามารถใช้งานแอป Yale Home  
ได้อย่างปลอดภัยเช่นเดิม

## ระดับความรุนแรง (SEVERITY)

ระดับความรุนแรงของช่องโหว่นี้ได้ประเมินตามมาตรฐาน CVSS เวอร์ชัน 4.0 โดยได้คะแนน 6.9 จาก  
10 ซึ่งอยู่ในเกณฑ์ปานกลาง

รายละเอียดเพิ่มเติมสามารถดูได้ที่: <https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf>

คะแนน: 6.9/10 (Medium)

รายละเอียด: 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

## พันธสัญญาของเรา

เรายังคงยึดมั่นในพันธกิจในการสร้างสรรค์ผลิตภัณฑ์ที่ปลอดภัยและเชื่อถือได้  
เพื่อให้ลูกค้าทุกท่านได้รับประสบการณ์การใช้งานที่ดีที่สุด

เรามีการติดตาม ตรวจสอบ และพัฒนาระบบเทคโนโลยีของเราอย่างต่อเนื่อง  
เพื่อให้แน่ใจว่าผลิตภัณฑ์ของเรามีความปลอดภัยและตอบสนองความต้องการของลูกค้าได้อย่างแท้จริง

## ข้อมูลติดต่อ

หากต้องการข้อมูลเพิ่มเติม หรือมีข้อสงสัยเกี่ยวกับความปลอดภัยของผลิตภัณฑ์  
กรุณาติดต่อทีมงานของเราผ่านทางอีเมล: [product.security@assaabloy.com](mailto:product.security@assaabloy.com)

เราขอขอบคุณทุกท่านที่ไว้วางใจในผลิตภัณฑ์ Yale เสมอมา

ขอแสดงความนับถือ

ทีมงาน Yale

## REVISION HISTORY

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