แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ Zero Day ของผลิตภัณฑ์ Apple (CVE-2025-43300)

วันที่แจ้งเตือน 29 สิงหาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ Zero Day ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ Apple ดังนี้

Severity/ CVE ID	ผลิตภัณฑ์ที่ได้รับผลกระทบ	รายละเอียดช่องโหว่	ผลกระทบ
Critical: CVE-2025-43300	**Iphone iOS** เวอร์ชันก่อนหน้า 18.6.2 **iPadOS** เวอร์ชันก่อนหน้า 17.7.10 และ เวอร์ชัน 18.0 ถึงเวอร์ชันก่อน 18.6.2 **macOS Sonoma** เวอร์ชันก่อนหน้า 14.7.8 **macOS Ventura** เวอร์ชันก่อนหน้า 13.7.8 **macOS Sequoia** เวอร์ชันก่อนหน้า 15.6.1	ช่องโหว่ประเภท Out-of-Bounds Write ใน Image I/O Framework ของ Apple ซึ่งเป็นองค์ประกอบพื้นฐานของระบบปฏิบัติการ Apple ที่ใช้จัดการและประมวลผลรูปภาพ โดยมีการยืนยันว่าช่องโหว่ดังกล่าวถูกนำไปใช้โจมตีในแบบ Targeted Attacks แล้ว	ส่งผลให้ผู้ไม่หวังดีสามารถสั่งรันโค้ดที่เป็นอันตราย (Arbitrary Code Execution) ผ่านไฟล์ภาพที่ถูกสร้างขึ้นมาได้ และอาจเข้าควบคุมอุปกรณ์ที่ได้รับผลกระทบได้

แนวทางการป้องกันเบื้องต้น:

Apple แนะนำให้ผู้ใช้งานทุกคนพิจารณาอัปเดตระบบปฏิบัติการเป็นเวอร์ชันล่าสุดทันที ผ่านฟังก์ชัน Software Update ใน Settings ของอุปกรณ์ เพื่อป้องกันการตกเป็นเป้าหมายของการโจมตี

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 28 ส.ค. 2568
2) https://nvd.nist.gov/vuln/detail/CVE-2025-43300
3) https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-084
4) https://cybersecuritynews.com/apple-0-day-vulnerability-actively-exploited/