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 Trend Micro (CVE-2025-54948 และ CVE-2025-54987) และ Adobe (CVE-2025-54253 และ CVE-2025-54254)

วันที่แจ้งเตือน 15 สิงหาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ Zero Day ที่มีผลกระทบร้ายแรงของ 2 ผลิตภัณฑ์ ได้แก่

No.	ผลิตภัณฑ์ที่ได้รับผลกระทบ	รายละเอียดช่องโหว่	ผลกระทบ
1.	**Trend Micro Endpoint Security** - Trend Micro Apex One (on-premise) - Trend Micro Apex One as a Service - Trend Vision One Endpoint Security – Standard Endpoint Protection	CVE-2025-54948 และ CVE-2025-54987 เป็นช่องโหว่ command injection	ส่งผลให้ผู้ไม่หวังดีสามารถอัปโหลดโค้ดอันตรายและรันคำสั่งบนระบบโดยไม่จำเป็นต้องผ่านการยืนยันตัวตน
แนวทางการป้องกันเบื้องต้น: Trend Micro ได้ออกคำแนะนำให้ผู้ใช้งานและผู้ดูแลระบบทำการติดตั้งเครื่องมือแก้ไขชั่วคราว (FixTool) เพื่อลดความเสี่ยงจากช่องโหวทันที ทั้งนี้ Trend Micro มีแผนจะออกอัปเดตด้านความปลอดภัยในช่วงกลางเดือนสิงหาคม 2568			
2.	**Adobe** - Adobe Experience Manager Form (AEM) บน JEE เวอร์ชัน 6.5.23 และเวอร์ชันก่อนหน้า	CVE-2025-54253: ช่องโหว่เกิดจากการตั้งค่าผิดพลาด (Misconfiguration) CVE-2025-54254: ช่องโหว่ประเภท Improper Restriction of XML External Entity Reference (XXE)	ส่งผลให้ผู้โจมตีสามารถรันโค้ดจากระยะไกล (Remote Code Execution) บนระบบได้โดยตรง และอาจขยายการโจมตีส่วนอื่นของระบบ ส่งผลให้ผู้โจมตีสามารถเข้าถึงไฟล์สำคัญในระบบได้โดยไม่ต้องมีการโต้ตอบจากผู้ใช้งาน เสี่ยงต่อการรั่วไหลของข้อมูลสำคัญ
แนวทางการป้องกันเบื้องต้น: แนะนำให้อัปเดตแพตช์ล่าสุดที่ Adobe เผยแพร่เพื่อแก้ไขช่องโหว่ หากไม่สามารถอัปเดตได้ทันที ควรดำเนินการลดความเสี่ยง ดังนี้ - จำกัดการเข้าถึง AEM Forms จากเครือข่ายภายนอก - กำหนดสิทธิ์ผู้ใช้งานและแอปพลิเคชันให้น้อยที่สุดเท่าที่จำเป็น (Least Privilege)			

ThaiCERT แนะนำให้หน่วยงานควรเฝ้าระวังและตรวจสอบช่องโหว่ภายในบริษัท และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของบริษัทเป็นประจำสม่ำเสมอ

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 15 ส.ค. 2568
2) https://success.trendmicro.com/en-US/solution/KA-0020652
3) https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html