แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ Zero-Day ใน Adobe Reader ถูกใช้โจมตีผ่านไฟล์ PDF

วันที่แจ้งเตือน 10 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานกรณีตรวจพบการใช้ประโยชน์จากช่องโหว่แบบ Zero-Day ใน Adobe Reader ผ่านไฟล์ PDF ที่ถูกสร้างขึ้น ซึ่งถูกใช้ในการโจมตีจริง

รายงานดังกล่าวระบุว่าไฟล์ PDF ที่ใช้ในการโจมตีถูกออกแบบเพื่อหลอกให้ผู้ใช้งาน (Social Engineering) เปิดไฟล์ที่เรียกใช้ JavaScript อัตโนมัติ เพื่อรวบรวมข้อมูลจากระบบและติดต่อกับเซิร์ฟเวอร์ภายนอกเพื่อรับ payload รวมถึงส่งข้อมูลออกไปยังเซิร์ฟเวอร์ของผู้ไม่หวังดี และอาจถูกใช้ในการโจมตีขั้นสูงต่อไป

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาสร้างความตระหนักรู้แก่ผู้ใช้งานในองค์กรให้หลีกเลี่ยงการเปิดไฟล์ PDF จากแหล่งที่ไม่น่าเชื่อถือ โดยเฉพาะไฟล์ที่มีลักษณะเป็นเอกสารทางธุรกิจ รวมทั้งเฝ้าระวังพฤติกรรมผิดปกติ เช่น การเรียกใช้งาน JavaScript ภายใน PDF หรือการเชื่อมต่อไปยังเซิร์ฟเวอร์ภายนอก เป็นต้น รวมทั้งควรเฝ้าระวัง log และพฤติกรรมของแอปพลิเคชัน Adobe อย่างใกล้ชิด และเตรียมมาตรการตอบสนองเหตุการณ์ (Incident Response) อย่างเหมาะสม

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/adobe-reader-zero-day-exploited-via.html
2. https://justhaifei1.blogspot.com/2026/04/expmon-detected-sophisticated-zero-day-adobe-reader.html