แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Microsoft แก้ไขช่องโหว่ใน Windows Shell (CVE-2026-32202) ซึ่งถูกนำไปใช้โจมตีจริง

วันที่แจ้งเตือน 28 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft ได้แก้ไขช่องโหว่ใน Windows Shell (CVE-2026-32202) ที่ถูกนำไปใช้โจมตีจริง

ช่องโหว่ดังกล่าวเป็นประเภท Spoofing เกิดจากความล้มเหลวของกระบวนการป้องกันในระบบ ซึ่งถูกใช้เพื่อหลอกให้ระบบทำการตรวจสอบเส้นทางและความน่าเชื่อถือของไฟล์อย่างไม่ถูกต้อง โดยผู้ไม่หวังดีจะส่งไฟล์ที่เป็นอันตรายไปยังเหยื่อ และบางกรณีอาจไม่ต้องมีการโต้ตอบจากผู้ใช้งาน ผ่านไฟล์ประเภท LNK (zero-click) ที่ถูกประมวลผลโดยอัตโนมัติ ทำให้ข้อมูลส่งออกไปยังผู้ไม่หวังดีและเข้าถึงระบบโดยไม่ได้รับอนุญาต ทั้งนี้ ช่องโหว่ดังกล่าวมีความเชื่อมโยงกับช่องโหว่ใน Windows Shell (CVE-2026-21510) ที่ผู้ไม่หวังดีสามารถหลบเลี่ยงการตรวจจับความปลอดภัยผ่านเครือข่าย และช่องโหว่ใน MSHTML Framework (CVE-2026-21513) ที่ถูกใช้ร่วมกันในลักษณะ exploit chain แม้ว่าช่องโหว่ที่เกี่ยวข้องถูกแก้ไขแล้วโดย Microsoft ในเดือนกุมภาพันธ์ 2026 แต่ยังคงมีช่องโหว่เหลืออยู่

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลพิจารณาติดตั้งอัปเดตผลิตภัณฑ์ตามคำแนะนำของผู้ผลิต รวมถึงเฝ้าระวังและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง พร้อมทั้งตรวจสอบและอัปเดตนโยบายการตั้งค่าความปลอดภัยของระบบ และปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคามล่าสุดเพื่อให้สามารถตรวจจับและรับมือกับภัยคุกคามได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/microsoft-confirms-active-exploitation.html
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32202
3. https://nvd.nist.gov/vuln/detail/CVE-2026-32202
4. https://nvd.nist.gov/vuln/detail/CVE-2026-21510
5. https://nvd.nist.gov/vuln/detail/CVE-2026-21513