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

พบ Zero-Days 3 ช่องโหว่ใน Microsoft Defender ถูกใช้โจมตีจริง

วันที่แจ้งเตือน 20 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับ Zero-Days 3 ช่องโหว่ใน Microsoft Defender ได้แก่ (1) BlueHammer (CVE-2026-33825) (2) RedSun และ (3) UnDefend ถูกนำไปใช้ในการโจมตีจริง

โดย (1) BlueHammer และ (2) RedSun เป็นช่องโหว่ประเภท local privilege escalation (LPE) ที่ทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ์เป็นระดับ SYSTEM บนเครื่องที่ถูกโจมตี ขณะที่ช่องโหว่ (3) UnDefend ผู้ไม่หวังดีสามารถใช้ปิดระบบการป้องกัน ทำให้ไม่สามารถอัปเดต signature ได้อย่างเต็มประสิทธิภาพ ทั้งนี้ Microsoft ได้ดำเนินการการแก้ไขช่องโหว่ BlueHammer แล้วในชุดอัปเดต Patch Tuesday ประจำเดือนเมษายน 2569 **อย่างไรก็ดี ช่องโหว่ RedSun และ UnDefend ยังไม่มีการออกแพตช์แก้ไข** ทำให้ระบบยังคงมีความเสี่ยงต่อการถูกโจมตี

สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินมาตรการที่เหมาะสม โดยพิจารณาดำเนินการอัปเดตระบบตามคำแนะนำของผู้พัฒนาผลิตภัณฑ์ พร้อมทั้งพิจารณาตรวจสอบบันทึกการทำงานของระบบ (logs) เพื่อค้นหาพฤติกรรมหรือการเข้าถึงที่ผิดปกติ รวมถึงทบทวนมาตรการควบคุมสิทธิ์การเข้าถึงระบบให้เหมาะสมกับระดับความเสี่ยง และควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง โดยเฉพาะ Zero-Days ยังไม่มีการออกแพตช์แก้ไข

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/three-microsoft-defender-zero-days.html
2. https://nvd.nist.gov/vuln/detail/CVE-2026-33825
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825