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 Microsoft ออกแพตช์แก้ไขช่องโหว่ประจำเดือนธันวาคม 2567 ซึ่งรวมถึงแพตซ์ช่องโหว่ Zero Day (CVE-2024-49138)

วันที่แจ้งเตือน 13 ธันวาคม 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

BleepingComputer เว็บไซต์ด้านความปลอดภัยได้เผยแพร่รายงานแพตช์แก้ไขช่องโหว่ของผลิตภัณฑ์ Microsoft ประจำเดือนธันวาคม 2567 (Patch Tuesday) โดยแบ่งเป็นแพตซ์แก้ไขช่องโหว่ Zero Day (CVE-2024-49138) จำนวน 1 รายการ และแพตช์แก้ไขช่องโหว่อื่น ๆ 70 รายการ โดยช่องโหว่ Zero Day เป็นช่องโหว่ใน Windows Common Log File System (CLFS) Driver Heap-based Buffer Overflow ซึ่งส่งผลให้ผู้ไม่หวังดีที่มีสิทธิอยู่ในระดับผู้ใช้งานทั่วไปสามารถยกระดับสิทธิเป็น SYSTEM-level บนอุปกรณ์ Windows และสามารถควบคุมระบบได้อย่างสมบูรณ์ เช่น การเข้าถึงข้อมูลที่สำคัญ การดัดแปลงหรือทำลายข้อมูล และการใช้ระบบเป็น Host ในการโจมตีระบบอื่น ๆ บนเครือข่ายขององค์กร เป็นต้น และพบว่ามีการนำไปใช้ในการโจมตีจริง

ช่องโหว่สำคัญ 70 รายการ ในหลายผลิตภัณฑ์ สามารถแบ่งตามหมวดหมู่ ดังนี้

- Elevation of Privilege จำนวน 27 รายการ (Moderate 1 รายการ, Important 26 รายการ)
- Remote Code Execution จำนวน 30 รายการ (Critical 16 รายการ, Important 14 รายการ)
- Information Disclosure จำนวน 7 รายการ (Important 7 รายการ)
- Denial of Service จำนวน 5 รายการ (Important 5 รายการ)
- Spoofing จำนวน 1 รายการ (Important 1 รายการ)

Microsoft แนะนำให้ผู้ใช้งานติดตั้งแพตช์โดยเร็วที่สุดเพื่อป้องกันการถูกโจมตี นอกจากนี้องค์กรควรตรวจสอบให้แน่ใจว่าระบบได้รับการกำหนดค่าตามแนวทางปฏิบัติที่ดีด้านความปลอดภัยของ Microsoft เพื่อลดความเสี่ยงที่อาจเกิดขึ้น และองค์กรควรตรวจสอบระบบเพื่อหาเหตุการณ์ที่ผิดปกติ โดยเน้นเหตุการณ์ที่เกี่ยวข้องกับการยกระดับสิทธิที่ผิดปกติ

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

ข้อมูลอ้างอิง

1) https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2024-patch-tuesday-fixes-1-exploited-zero-day-71-flaws/
2) https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-49138
3) https://nvd.nist.gov/vuln/detail/CVE-2024-49138
4) https://cybersecuritynews.com/windows-common-log-file-system-zero-day/