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 ออก Security Patch เพื่อแก้ไขช่องโหว่ Zero-Day หลายรายการ

วันที่แจ้งเตือน 20 สิงหาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ Zero-Day หลายรายการ ได้แก่

รายละเอียดช่องโหว่	ข้อเสนอแนะ
1. **ช่องโหว่ CVE-2026-68820** เป็นช่องโหว่ประเภท Elevation of Privilege ใน Windows Function Drive for WinSock หรือ AFD.sys เกิดจากปัญหา Use-After-Free ซึ่งทำให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบหรือเครื่องเป้าหมาย จากนั้นเรียกใช้โปรแกรมที่สร้างขึ้นเพื่อทำให้เกิด Race Condition และยกระดับสิทธิเป็น System ได้ 2. **ช่องโหว่ CVE-2026-62832** เป็นช่องโหว่ประเภท Elevation of Privilege ใน Windows Uses Profile Service เกิดจากการจัดการ link ก่อนเข้าถึงไฟล์ อย่างไม่ถูกต้อง ทำให้ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนและมีข้อมูล Credential สามารถเรียกใช้โปรแกรมที่สร้างขึ้นเพื่อโหลด Registry Hive ของผู้ใช้งานรายอื่น และยกระดับสิทธิเป็น Administrator ได้โดยไม่ต้องมีการโต้ตอบจากผู้ใช้งาน 3. **ช่องโหว่ CVE-2026-72971** เป็นช่องโหว่ประเภท Tampering ใน Windows Container Isolation FS Filter Drive หรือ unionfs.sys เกิดจากการจัดการ link ก่อนเข้าถึงไฟล์อย่างไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถใช้โปรแกรมที่สร้างขึ้นเพื่อเข้าถึงและแก้ไขข้อมูลในระบบได้	ควรพิจารณาดำเนินการตรวจสอบระบบ Windows ที่ใช้งาน และติดตั้ง Update ตามคำแนะนำของผู้ผลิต นอกจากนี้ควรติดตามและเฝ้าระวังพฤติกรรมการใช้งานที่ผิดปกติ โดยเฉพาะบัญชีผู้ใช้งานสิทธิ์สูง เพื่อให้สามารถตรวจพบและตอบสนองต่อเหตุการณ์ที่มีความเสี่ยงได้อย่างรวดเร็ว

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2026-68820
2. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-68820
3. https://nvd.nist.gov/vuln/detail/CVE-2026-62832
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62832
5. https://nvd.nist.gov/vuln/detail/CVE-2026-72971
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72971
7. https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2026-patch-tuesday-fixes-400-flaws-3-zero-days/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ