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 เผย Zero-Day ในผลิตภัณฑ์ถูกนำไปใช้โจมตีจริง

วันที่แจ้งเตือน 25 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft ได้เปิดเผยช่องโหว่ในผลิตภัณฑ์ถูกนำไปใช้โจมตีจริง ได้แก่

ผู้ผลิต	รายละเอียด	ผลกระทบ
Microsoft	• ช่องโหว่ CVE-2026-45585 เป็น Zero-Day ของ Windows BitLocker ที่อนุญาตให้ผู้ไม่หวังดีสามารถข้าม (Bypass) การทำงานของระบบเข้ารหัสไดรฟ์ (BitLocker) ได้ ทำให้ผู้ไม่หวังดีเข้าถึงข้อมูล และควบคุมอุปกรณ์ได้ โดยผ่านการใช้ FsTx Auto Recovery Utility ใน Windows และทำงานผ่านโหมด Windows Recovery Environment (WinRE) เพื่อเข้าถึง Drive ที่จัดเก็บข้อมูลโดยไม่จำกัดแม้จะมีการป้องกันด้วย BitLocker • **Microsoft ให้คำแนะนำในการแก้ไข แต่ยังไม่ได้เผยแพร่แพตช์แก้ไขอย่างเป็นทางการ**	ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Windows 11 และ Windows Server 2022/2025 ที่เปิดใช้งาน BitLocker ร่วมกับ Trusted Platform Module (TPM)
	• ช่องโหว่ CVE-2026-41091 เป็น Zero-Day ประเภทการยกระดับสิทธิ์ (Elevation of Privilege - EoP) ใน Microsoft Defender เกิดจากข้อผิดพลาดประเภท Improper Link Resolution Before File Access หรือ การจัดการ Link Reference ไม่เหมาะสม ทำให้ผู้ไม่หวังดีเข้าถึงไฟล์หรือ Resource ที่ถูกเปลี่ยนเส้นทางผ่าน Symbolic Link หรือ Hard Link ส่งผลให้สามารถยกระดับสิทธิ์เป็น SYSTEM ซึ่งเป็นสิทธิ์สูงสุดของ Windows ได้ • **Microsoft ได้เผยแพร่แพตช์แก้ไขแล้ว**	ส่งผลกระทบต่อ Microsoft Malware Protection Engine เวอร์ชัน 1.1.26030.3008 และเวอร์ชันก่อนหน้า
	• ช่องโหว่ CVE-2026-45498 เป็น Zero-Day ประเภท Denial-of-Service (DoS) ใน Microsoft Defender ทำให้ผู้ไม่หวังดีสามารถใช้ประโยชน์จากช่องโหว่นี้ได้ จะทำให้ระบบ Windows ที่ยังไม่ได้ติดตั้งแพตช์เกิดอาการหยุดทำงาน ไม่สามารถให้บริการหรือไม่สามารถทำงานได้ตามปกติ • **Microsoft ได้เผยแพร่แพตช์แก้ไขแล้ว**	ส่งผลกระทบต่อ Microsoft Defender Antimalware Platform เวอร์ชัน 4.18.26030.3011 และเวอร์ชันก่อนหน้า

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2026-45585
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585
3. https://securityaffairs.com/192449/hacking/microsoft-issues-yellowkey-mitigation-no-patch-yet.html
4. https://nvd.nist.gov/vuln/detail/CVE-2026-41091
5. https://www.bleepingcomputer.com/news/security/microsoft-warns-of-new-defender-zero-days-exploited-in-attacks/
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091
7. https://nvd.nist.gov/vuln/detail/CVE-2026-45498
8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45498