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

Microsoft ออก Security Patch เพื่อแก้ไขช่องโหว่ Zero Day หลายรายการ

วันที่แจ้งเตือน 12 มีนาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ และได้รับรายงานว่า บริษัท Microsoft ได้ออก Security Patch ประจำเดือนมีนาคม 2568 เพื่อแก้ไขช่องโหว่สำคัญ จำนวน 57 รายการ รวมถึงช่องโหว่ Zero-Days จำนวน 6 รายการที่อาจถูกใช้โจมตีครอบคลุมผลิตภัณฑ์หลายตัว เช่น Dynamics Business Central, Desktop Window Manager, SharePoint Server, Streaming Service และ Windows Hyper-V เป็นต้น และมีช่องโหว่ที่มีความรุนแรงระดับวิกฤต เช่น ช่องโหว่ประเภทการยกระดับสิทธิ (Privilege Escalation) ที่อาจทำให้ผู้ไม่ประสงค์ดีสามารถควบคุมระบบได้จากระยะไกล (Remote Code Execution) และยกระดับสิทธิให้สูงขึ้นทำให้ควบคุมระบบขององค์กรได้ เป็นต้น

ทั้งนี้ Security Patch เพื่อแก้ไขช่องโหว่ระดับวิกฤต (Critical) แบบ Zero-days จำนวน 6 รายการ ได้แก่

CVE ID	CVE Title
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability
CVE-2025-24985	Windows Fast FAT File System Driver Remote Code Execution Vulnerability
CVE-2025-24991	Windows NTFS Information Disclosure Vulnerability
CVE-2025-24993	Windows NTFS Remote Code Execution Vulnerability
CVE-2025-26633	Microsoft Management Console Security Feature Bypass Vulnerability

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ผู้ประกอบธุรกิจควรพิจารณาดำเนินการติดตั้ง Patch ตามคำแนะนำของผู้ออกผลิตภัณฑ์ ตรวจสอบและเฝ้าระวังกิจกรรมที่ผิดปกติในระบบ โดยเฉพาะการพยายามยกระดับสิทธิ์หรือการเข้าถึงระบบที่ไม่ได้รับอนุญาต สำรองข้อมูลสำคัญอย่างสม่ำเสมอ และจัดทำแผนรับมือเหตุการณ์ฉุกเฉินกรณีพบการโจมตี

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2025-patch-tuesday-fixes-7-zero-days-57-flaws/
2. https://msrc.microsoft.com/update-guide
3. https://nvd.nist.gov/vuln/detail/CVE-2025-24983
4. https://nvd.nist.gov/vuln/detail/CVE-2025-24984
5. https://nvd.nist.gov/vuln/detail/CVE-2025-24985
6. https://nvd.nist.gov/vuln/detail/CVE-2025-24991
7. https://nvd.nist.gov/vuln/detail/CVE-2025-24993
8. https://nvd.nist.gov/vuln/detail/CVE-2025-26633
9. https://nvd.nist.gov/vuln/detail/CVE-2025-26630