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 ช่องโหว่ร้ายแรงของผลิตภัณฑ์ Microsoft Office CVE-2025-53730, CVE-2025-53731 และ CVE-2025-53740

วันที่แจ้งเตือน 25 สิงหาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงาน ก.ล.ต. ร่วมกับ TCM-CERT ได้ติดตามข่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์พบช่องโหว่ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ Microsoft Office จำนวน 3 รายการ ซึ่งผู้ไม่หวังดีอาจใช้ช่องโหว่ดังกล่าว เข้าควบคุมระบบจากระยะไกล (Remote Code Execution) ได้ โดยมีรายละเอียด ดังนี้

Severity/ CVE ID	ผลิตภัณฑ์ที่ได้รับผลกระทบ	รายละเอียดช่องโหว่	ผลกระทบ
Critical : CVE-2025-53731 CVE-2025-53740 Important : CVE-2025-53730	Microsoft Office 2016 (32 & 64 bit) Microsoft Office 2019 (32 & 64 bit) Microsoft Office LTSC for Mac 2024 Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC 2024 (32 & 64 bit) Microsoft Office LTSC 2021 (32 & 64 bit) Microsoft 365 Apps for Enterprise (32 & 64 bit)	เป็นช่องโหว่เกี่ยวกับการจัดการหน่วยความจำแบบ use-after-free ส่งผลให้ผู้ไม่หวังดีสามารถแก้ไขหน่วยความจำและรันโค้ดอันตรายในสิทธิระดับสูงได้	ส่งผลให้ผู้ไม่หวังดีสามารถรันคำสั่งบนระบบได้จากระยะไกล (Remote Code Execution) ทำให้สามารถขโมยข้อมูล ติดตั้งมัลแวร์ หรือเข้ายึดเครื่องของผู้ใช้งาน เพื่อขยายการโจมตีไปยังระบบอื่น ๆ ได้

แนวทางการป้องกัน:

1. พิจารณาดำเนินการอัปเดตแพตช์ความปลอดภัยล่าสุดที่ Microsoft แนะนำทันที
2. ผู้ดูแลระบบควรติดตามประกาศด้านความปลอดภัยของ Microsoft อย่างใกล้ชิด
3. พิจารณาดำเนินการแบ่งส่วนเครือข่าย (network segmentation) และ กำหนดมาตรการควบคุมการเข้าถึง (access controls) ที่เหมาะสม

ผู้ไม่หวังดีสามารถสร้างไฟล์เอกสารที่ฝังโค้ดอันตรายไว้ แล้วผ่านอีเมลโดยแนบไฟล์ ลิงก์ดาวน์โหลด หรือการแชร์ผ่านบริการออนไลน์ เมื่อเปิดไฟล์ หรือพรีวิวผ่าน Outlook ช่องโหว่ก็จะถูกเรียกใช้งานทันที ทำให้ผู้ไม่หวังดีสามารถรันโค้ดบนเครื่องของเหยื่อ ขโมยข้อมูลส่วนตัว ปล่อยมัลแวร์ หรือแม้กระทั่งยึดเครื่อง เพื่อใช้เป็นฐานโจมตีเครือข่ายต่อไปได้

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

ข้อมูลอ้างอิง

1) https://cyberpress.org/microsoft-office-flaws-could-let-hackers-execute-remote-code/
2) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53730
3) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53731
4) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53740