เอกสารการแจ้งเตือนกรณี Microsoft ออกแพตช์แก้ไขช่องโหว่ Zero-Click ใน Microsoft Outlook

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Microsoft ออกแพตช์แก้ไขช่องโหว่ Zero-Click ใน Microsoft Outlook

Microsoft ได้ออกอัปเดตเพื่อแก้ไขช่องโหว่ Zero-Click สามารถ Remote Code Execution (RCE) ที่ช่องโหว่หมายเลข CVE-2025-21298 ระดับ Critical (มีคะแนน CVSS 9.8) ซึ่งเกิดจากข้อผิดพลาด double-free memory management ในไฟล์ ole32.dll ของระบบปฏิบัติการ Windows โดยช่องโหว่ดังกล่าวทำให้ผู้โจมตีสามารถส่งไฟล์ Rich Text Format (RTF) ที่ถูกสร้างขึ้นเป็นพิเศษผ่านอีเมล และเมื่อผู้ใช้ Outlook เปิดดูตัวอย่างไฟล์โค้ดอันตราย สามารถรันโค้ดได้โดยอัตโนมัติโดยไม่ต้องมีการโต้ตอบใดๆ จากผู้ใช้ ช่องโหว่ดังกล่าวส่งผลกระทบต่อระบบปฏิบัติการ Windows 10, Windows 11 และ Windows server ตั้งแต่ปี 2551 จนถึงเวอร์ชันล่าสุดในปี 2568

Microsoft ได้ออกแพตช์แก้ไขช่องโหว่ในรอบการอัปเดตเดือนมกราคม 2568 และแนะนำให้ผู้ใช้งานดำเนินการอัปเดตแพตช์โดยเร็วที่สุดเพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ดังกล่าว โดยมีแนวทางดังนี้ [1]

1. อัปเดตระบบปฏิบัติการ Windows ให้เป็นเวอร์ชันล่าสุดที่มีการแก้ไขช่องโหว่ดังกล่าว
2. ปิดการแสดงตัวอย่างไฟล์ Rich Text Format (RTF) ในโปรแกรม Microsoft Outlook เป็นการชั่วคราว หากยังไม่สามารถอัปเดตได้ทันที
3. ใช้ระบบตรวจจับภัยคุกคามขั้นสูงสำหรับไฟล์แนบเพื่อเพิ่มระดับการป้องกันและลดความเสี่ยงจากการโจมตี

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://cybersecuritynews.com/outlook-zero-click-rce-vulnerability-cve-2025-21298/?fbclid=IwZXh0bgNhZW0CMTEAAR0sZlCMabrLgsdoxBEjlsOTJnuAp_mBwVonE45zLcIqfiivF-nNl4x9HQU_aem_VqnIgoEOC_4xfjJOh0jp6A