

- Financial Damage
- Reputation Damage
- Non-compliance
- Privacy Violation

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability



Microsoft ออก Security Patch เพื่อแก้ไขช่องโหว่ Zero Day หลายรายการ รวมทั้ง ประกาศยกเลิกฟีเจอร์ Privacy Protection VPN ใน Microsoft Defender

วันที่แจ้งเตือน 14 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบการหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ และได้รับรายงานว่า บริษัท Microsoft ได้ออก Security Patch ประจำเดือนกุมภาพันธ์ 2568 เพื่อแก้ไขช่องโหว่จำนวน 55 รายการ โดยในจำนวนนี้ มีช่องโหว่ที่กำลังถูกใช้โจมตีในปัจจุบัน จำนวน 2 รายการ ได้แก่

CVE ID	CVE Title
CVE-2025-21391	Windows Storage Elevation of Privilege Vulnerability
CVE-2025-21418	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

และมีช่องโหว่ระดับวิกฤต (Critical) แบบ Zero-day จำนวน 4 รายการ ได้แก่

CVE ID	CVE Title
CVE-2025-21177	Microsoft Dynamics 365 Sales Elevation of Privilege Vulnerability
CVE-2025-21381	Microsoft Excel Remote Code Execution Vulnerability
CVE-2025-21379	DHCP Client Service Remote Code Execution Vulnerability
CVE-2025-21376	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ผู้ประกอบธุรกิจควรพิจารณาดำเนินการติดตั้ง Security Patch ตามคำแนะนำของผู้ออกผลิตภัณฑ์ ตรวจสอบและเฝ้าระวังกิจกรรมที่ผิดปกติในระบบ โดยเฉพาะการพยายามยกระดับสิทธิ์หรือการเข้าถึงระบบที่ไม่ได้รับอนุญาต สำรองข้อมูลสำคัญอย่างสม่ำเสมอ และจัดทำแผนรับมือเหตุการณ์ฉุกเฉิน กรณีพบการโจมตี

นอกจากนี้ พบว่า Microsoft ได้ประกาศยกเลิกฟีเจอร์ Privacy Protection VPN ในแอปพลิเคชัน Microsoft Defender ซึ่งจะผลิตตั้งแต่วันที่ 28 กุมภาพันธ์ 2568 เป็นต้นไป โดยฟีเจอร์ดังกล่าวเป็นส่วนหนึ่งของบริการ Microsoft 365 Personal และ Family ที่ช่วยปกป้องความเป็นส่วนตัวส่วนต่อเชื่อมต่อกับ Wi-Fi สาธารณะ

ทั้งนี้ ฟีเจอร์ Privacy Protection VPN เป็นระบบที่ช่วยป้องกันการโจมตีแบบ Man-in-the-Middle (MITM) และ Evil Twin โดยเฉพาะเมื่อใช้งานเครือข่าย Wi-Fi สาธารณะ ซึ่งผู้ใช้งานจะได้รับโควตาการใช้งาน VPN 50 GB ต่อเดือน การยกเลิกฟีเจอร์นี้อาจส่งผลกระทบโดยเพิ่มความเสี่ยงในการถูกดักจับข้อมูลหรือการโจมตีทางไซเบอร์ โดยเฉพาะเมื่อผู้ใช้งานต้องใช้งานเครือข่าย Wi-Fi สาธารณะในการปฏิบัติงาน ซึ่งอาจนำไปสู่การรั่วไหลของข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคล หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบการในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. <https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2025-patch-tuesday-fixes-4-zero-days-55-flaws/>
2. <https://www.securityweek.com/microsoft-patches-wormable-windows-flaw-and-file-deleting-zero-day/>
3. <https://www.bleepingcomputer.com/news/microsoft/microsoft-kills-off-defender-privacy-protection-vpn-feature/>