แจ้งเตือน : ช่องโหว่

High

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

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน เพื่อพิจารณาอัปเดต Patch แก้ไขช่องโหว่ Windows Wi-Fi Driver RCE (CVE-2024-30078)

วันที่แจ้งเตือน 24 มิถุนายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ไมโครซอฟท์ ได้ออกโปรแกรมแก้ไขช่องโหว่ (Patch) เพื่อแก้ไขช่องโหว่ผลกระทบระดับสูง (CVE-2024-30078) ของ Windows Wi-Fi Driver ซึ่งผู้ไม่หวังดีอาจใช้ช่องโหว่ดังกล่าวเข้าโจมตีในลักษณะ Remote Code Execution (RCE) และส่งคำสั่งเข้าสู่ระบบโดยไม่ได้รับอนุญาตผ่านการเชื่อมต่อ Wi-Fi Network ส่งผลให้ผู้ใช้งานที่ใช้งาน Laptop เชื่อมต่อ Wi-Fi network สาธารณะ เช่น สนามบิน หรือ ร้านกาแฟ มีความเสี่ยงในการถูกโจมตีผ่านช่องโหว่นี้ ซอฟต์แวร์ที่ได้รับผลกระทบ ได้แก่

Product	Affected Version	Product	Affected Version
Windows 10 version 1507	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.10240.20680	Windows Server 2008 SP2	ตั้งแต่เวอร์ชัน 6.0.0 ไปจนถึงก่อนเวอร์ชัน 6.0.6003.22720
Windows 10 version 1607	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.14393.7070	Windows Server 2008 R2 SP1	ตั้งแต่เวอร์ชัน 6.0.0 ไปจนถึงก่อนเวอร์ชัน 6.1.7601.27170
Windows 10 version 1809	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.17763.5936	Windows Server 2012	ตั้งแต่เวอร์ชัน 6.2.0 ไปจนถึงก่อนเวอร์ชัน 6.2.9200.24919
Windows 10 version 21H2	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.19044.4529	Windows Server 2012 R2	ตั้งแต่เวอร์ชัน 6.3.0 ไปจนถึงก่อนเวอร์ชัน 6.3.9600.22023
Windows 10 version 22H2	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.19045.4529	Windows Server 2016	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.14393.7070
Windows 11 version 21H2	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.22000.3019	Windows Server 2019	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.17763.5936
Windows 11 version 22H2	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.22621.3737	Windows Server 2022	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.20348.2522
Windows 11 version 23H2	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.22631.3737	Windows Server 2022, 23H2	ตั้งแต่เวอร์ชัน 10.0.0 ไปจนถึงก่อนเวอร์ชัน 10.0.25398.950

ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาติดตั้ง Patch และตั้งค่าระบบตามที่ไมโครซอฟต์แนะนำ (ตามข้อมูลอ้างอิง 2) โดยประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง พร้อมทั้งจัดให้มีมาตรการควบคุมอย่างเหมาะสม เพื่อป้องกันผลกระทบที่อาจเกิดขึ้น

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุนจึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสมเพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) https://www.theverge.com/2024/6/19/24181908/microsoft-windows-pc-update-wi-fi-vulnerability
2) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30078
3) https://nvd.nist.gov/vuln/detail/CVE-2024-30078
4) https://www.cve.org/CVERecord?id=CVE-2024-30078