แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Microsoft และ Google ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 4 มิถุนายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft และ Google ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ ได้แก่

ผู้ผลิต	รายละเอียด	ผลกระทบ
Microsoft	• Microsoft ออก Security Patch เพื่อแก้ไขช่องโหว่ Improper Access Control ในแอปพลิเคชัน Microsoft 365 บนระบบปฏิบัติการ Android จำนวน 4 รายการ ได้แก่ (1) CVE-2026-41100 ใน Microsoft 365 Copilot (2) CVE-2026-41101 ใน Microsoft Word (3) CVE-2026-41102 ใน Microsoft PowerPoint และ (4) CVE-2026-42832 ใน Microsoft Excel เกิดจาก Microsoft SDK ที่ถูกนำไปใช้งานร่วมกันในหลายผลิตภัณฑ์ โดยแอปพลิเคชันบางรายการถูกเผยแพร่พร้อมการตั้งค่าสำหรับการพัฒนา (Development Flag) ส่งผลให้แอปพลิเคชันอื่นบนอุปกรณ์เดียวกันสามารถขโมย Account Token ของผู้ใช้งานได้โดยไม่มีการแจ้งเตือนหรือขออนุญาต	แอปพลิเคชันที่ได้รับผลกระทบ ได้แก่ Microsoft 365 Copilot, Microsoft Word, Microsoft PowerPoint และ Microsoft Excel (รวมถึง Microsoft Loop และ OneNote)
	• Microsoft ออก Security Patch เพื่อแก้ไขช่องโหว่ Stack-Based Buffer Overflow (CVE-2026-41089) ใน Windows Netlogon เปิดโอกาสให้ผู้ไม่หวังดีทำ Remote Code Execution (RCE) หรือสั่งรันโค้ดจากระยะไกลบน Domain Controller เป้าหมาย ได้โดยไม่จำเป็นต้องเข้าสู่ระบบก่อน และไม่ต้องมีบัญชีผู้ใช้งานหรือมีสิทธิ์ใด ๆ ภายในระบบมาก่อน โดยหน่วยงาน Centre for Cybersecurity Belgium (CCB) ออกประกาศเตือนว่ามีกลุ่มผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ดำเนินการโจมตีระบบจริง	ส่งผลกระทบต่อ Windows Server ทุกเวอร์ชันที่ยังอยู่ในระยะการสนับสนุนจาก Microsoft รวมถึง Windows Server 2025

ข้อมูลอ้างอิง Microsoft

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41100
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41101
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41102
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42832
5. https://thehackernews.com/2026/06/microsoft-365-android-apps-let-any-app.html
6. https://enclave.ai/blog/flagleft-microsoft-365-android-forgotten-flag-account-takeover
7. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089
8. https://www.bleepingcomputer.com/news/microsoft/critical-windows-netlogon-remote-code-execution-flaw-now-exploited-in-attacks/?

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 และ Google ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 4 มิถุนายน 2569

ผู้ผลิต	รายละเอียด	ผลกระทบ
Google	• Google ออก Security Patch เพื่อแก้ไขช่องโหว่ Integer Overflow (CVE-2025-48595) ใน Android Framework ทำให้ผู้ไม่หวังดีสามารถรันโค้ดที่เป็นอันตรายบนอุปกรณ์เป้าหมาย และยกระดับสิทธิ์การเข้าถึงระบบ (Privilege Escalation) ได้โดยไม่จำเป็นต้องมีสิทธิ์ระดับสูง จากนั้นจะเข้าถึงข้อมูลสำคัญภายในเครื่อง ติดตั้งสปายแวร์ ดักจับข้อมูลการสื่อสาร อ่านข้อความ เข้าถึงข้อมูลส่วนบุคคล หรือควบคุมการทำงานของอุปกรณ์ได้	ส่งผลกระทบต่ออุปกรณ์ที่ใช้ระบบปฏิบัติการ Android 14, 15, 16 และ Android 16 QPR2

ข้อมูลอ้างอิง Google

1. https://nvd.nist.gov/vuln/detail/CVE-2025-48595
2. https://source.android.com/docs/security/bulletin/2026/2026-06-01
3. https://securityaffairs.com/193057/breaking-news/google-patches-actively-exploited-android-flaw-affecting-millions-of-devices.html