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

Google Chrome ออกแพตช์แก้ไขช่องโหว่ Zero-Day (CVE-2026-125350)

วันที่แจ้งเตือน 11 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Google ได้ออกอัปเดตแพตช์ความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ระดับความรุนแรงสูง (High Severity) ที่ได้รับการยืนยันว่าถูกใช้โจมตีจริงแล้ว (Actively Exploited)

รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
• **ช่องโหว่ CVE-2026-125350** เป็นช่องโหว่ประเภท Use-After-Free เกิดจากข้อผิดพลาดในการจัดการหน่วยความจำ เมื่อโปรแกรมพยายามเข้าถึงหน่วยความจำที่ถูกคืนให้ระบบไปแล้ว ทั้งนี้ หากโจมตีสำเร็จอาจส่งผลให้เกิด (1) Data Corruption: ข้อมูลเสียหาย (2) Application Crash: โปรแกรมหยุดทำงาน (3) Arbitrary Code Execution: ผู้ไม่หวังดีอาจสามารถสั่งรันโค้ดที่ไม่ได้รับอนุญาต • Google แนะนำให้ผู้ใช้งาน Chrome ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามที่ระบุ • นอกจากนี้ผู้ใช้งานเบราว์เซอร์ที่พัฒนาบน Chromium เช่น Microsoft Edge, Brave, Opera และ Vivaldi เป็นต้น ควรติดตามและพิจารณาติดตั้งแพตช์เมื่อผู้พัฒนาแต่ละรายมีการเผยแพร่ Security Patch	• เวอร์ชันที่ได้รับผลกระทบได้แก่ เวอร์ชันก่อนหน้า 157.0.8103.50 • Google แนะนำให้อัปเดต Chrome เป็นเวอร์ชันดังต่อไปนี้

ระบบปฏิบัติการ	เวอร์ชันที่แก้ไขแล้ว
Windows	157.0.8103.50 / .51
macOS	157.0.8103.50 / .51
Linux	157.0.8103.50

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/11/google-issues-chrome-security-update.html
2. https://nvd.nist.gov/vuln/detail/cve-2026-125350

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

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 ออกแพตช์แก้ไขช่องโหว่ 1,094 รายการ และพบช่องโหว่ Zero-Day ใน Outlook ถูกใช้โจมตีจริง

วันที่แจ้งเตือน 11 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft เผยแพร่แพตช์อัปเดตความปลอดภัยประจำเดือนพฤศจิกายน 2026 (Patch Tuesday) เพื่อแก้ไขช่องโหว่จำนวน 1,094 รายการ ครอบคลุมผลิตภัณฑ์หลายประเภท โดยพบช่องโหว่ Zero-Day ใน Microsoft Outlook (CVE-2026-124194) ซึ่ง Microsoft ยืนยันว่าถูกใช้โจมตีจริงแล้ว (Actively Exploited) อาจทำให้ผู้ไม่หวังดีได้รับข้อมูลยืนยันตัวตนของผู้ใช้งาน และนำไปใช้แอบอ้างเป็นผู้ใช้งานได้

รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
• **ช่องโหว่ CVE-2026-124194** เป็นช่องโหว่ประเภท Spoofing ใน Microsoft Outlook เกิดจากโปรแกรมไม่แสดงคำเตือน เมื่อผู้ใช้งานมีการดำเนินการที่อาจไม่ปลอดภัย ซึ่งผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ดังกล่าว เพื่อแอบอ้างตัวตน (Spoofing) ผ่านเครือข่ายได้ โดย (1) ส่งไฟล์ข้อความที่ถูกสร้างขึ้นเป็นพิเศษให้เหยื่อ (2) หลอกให้ผู้ใช้งานเปิดไฟล์ดังกล่าวผ่าน Outlook (3) Outlook เชื่อมต่อไปยังระบบเครือข่ายที่ผู้โจมตีควบคุม โดยไม่แสดงคำเตือนตามปกติ และ (4) ผู้ไม่หวังดีอาจได้รับ NTLMv2 Hash และนำไปใช้แอบอ้างตัวตนของผู้ใช้งาน	เวอร์ชันที่ได้รับผลกระทบ ได้แก่

ผลิตภัณฑ์	เวอร์ชันที่ได้รับผลกระทบ
Microsoft 365 Apps for Enterprise	เวอร์ชันก่อนการอัปเดตความปลอดภัยที่เกี่ยวข้อง
Microsoft Office LTSC 2021	ก่อน 16.0.14334.21048
Microsoft Office LTSC 2024	ก่อน 16.0.17932.21140

ข้อมูลอ้างอิง

1. https://www.securityweek.com/exploited-outlook-zero-day-among-1094-flaws-patched-by-microsoft/
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-124194

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ