

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 ออก Security Patch แก้ไขช่องโหว่ Zero Day (CVE-2025-13223)

ของเว็บเบราว์เซอร์ Chrome

วันที่แจ้งเตือน 24 พฤศจิกายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพ์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพ์และตลาดหลักทรัพ์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่าบริษัท Google ได้ออก Security Patch ถูกเงินเพื่อแก้ไขช่องโหว่ด้านความปลอดภัย Zero Day (CVE-2025-13223) ประเภท Type Confusion ใน JavaScript Engine V.8 ของ Chrome ซึ่งเป็นส่วนสำคัญที่ใช้ในการประมวลผลโค้ด JavaScript บนเบราว์เซอร์ ซึ่ง Google ได้ยืนยันว่าช่องโหว่ดังกล่าวถูกนำไปใช้ในการโจมตีจริง แต่ยังไม่มีการเปิดเผยข้อมูลเพิ่มเติมเกี่ยวกับลักษณะของการโจมตี

Google ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ดังกล่าว ใน Chrome (1) เวอร์ชัน 142.0.7444.175/.176 สำหรับ Windows (2) เวอร์ชัน 142.0.7444.176 สำหรับ macOS และ (3) เวอร์ชัน 142.0.7444.175 สำหรับ Linux โดย Chrome จะทำการอัปเดตอัตโนมัติ แต่เพื่อความมั่นใจว่าระบบได้รับการป้องกันอย่างทันท่วงที ผู้ใช้สามารถตรวจสอบและเร่งการอัปเดตได้เองผ่านเมนู Help จากนั้นเลือกเมนู About Google Chrome และเลือก “Relaunch” เพื่อเริ่มต้นใช้งานเวอร์ชันล่าสุดทันที

มาตรการป้องกันและแนวทางปฏิบัติ เพื่อป้องกันภัยคุกคามจากช่องโหว่นี้ สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบ พิจารณาดำเนินมาตรการที่เหมาะสมดังนี้

- อัปเดตซอฟต์แวร์ Chrome เป็นเวอร์ชันล่าสุด
- เฝ้าระวังกิจกรรมผิดปกติในเครือข่าย ตรวจสอบและบันทึกกิจกรรมที่อาจบ่งชี้ถึงการบุกรุก
- สำรองข้อมูลอย่างเป็นระบบ จัดทำแผนสำรองข้อมูลที่ปลอดภัยและสามารถกู้คืนได้ในกรณีฉุกเฉิน
- ตรวจสอบและอัปเดตนโยบายการตั้งค่าความปลอดภัยของระบบ ปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคามล่าสุด

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

ข้อมูลอ้างอิง

1. <https://www.bleepingcomputer.com/news/security/google-fixes-new-chrome-zero-day-flaw-exploited-in-attacks/>
2. https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html
3. <https://nvd.nist.gov/vuln/detail/CVE-2025-13223>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ