แจ้งเตือน	ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : CLEAR
Alert	☒ Financial Damage ☒ Reputation Damage ☒ Non-compliance ☒ Privacy Violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน Google ออก Security Patch แก้ไขช่องโหว่ Zero Day ของเว็บเบราว์เซอร์ Chrome

วันที่แจ้งเตือน 23 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ และพบว่าบริษัท Google ได้ออก Security Patch ฉุกเฉิน เพื่อแก้ไขช่องโหว่ด้านความปลอดภัย Zero Day (CVE-2025-10585) ประเภท Type Confusion ใน V8 JavaScript engine ของ Chrome ซึ่งเป็นส่วนสำคัญที่ใช้ในการประมวลผลโค้ด JavaScript บนเบราว์เซอร์ และผู้ไม่ประสงค์ดีอาจเรียกใช้โค้ดที่เป็นอันตรายได้จากระยะไกล (Remote Code Execution: RCE) ควบคุมระบบได้จากภายนอก Google ได้ออก Security Patch (1) เวอร์ชัน 140.0.7339.185/.186 สำหรับ Windows และ Mac และ (2) เวอร์ชั่น 140.0.7339.185 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 พิจารณาดำเนินมาตรการที่เหมาะสม ดังนี้

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

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/google-patches-sixth-chrome-zero-day-exploited-in-attacks-this-year/
2. https://securityaffairs.com/182322/uncategorized/cve-2025-10585-is-the-sixth-actively-exploited-chrome-zero-day-patched-by-google-in-2025.html