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

แจ้งเตือน ช่องโหว่ระดับร้ายแรงในโปรแกรม 7-Zip (CVE-2025-11001) ที่พบการโจมตีจริง

วันที่แจ้งเตือน 28 พฤศจิกายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่าหน่วยงาน NHS England Digital ของสหราชอาณาจักร ได้ออกประกาศเตือนถึงช่องโหว่ระดับร้ายแรง CVE-2025-11001 ในโปรแกรมบีบอัดไฟล์ 7-Zip และได้มีการได้ยืนยันว่า ช่องโหว่ดังกล่าวถูกนำไปใช้ในการโจมตีจริง ซึ่งทำให้ผู้โจมตีสามารถสั่งให้ระบบประมวลผลโค้ดได้จากระยะไกล (Remote Code Execution – RCE)

ช่องโหว่ดังกล่าวมีต้นเหตุมาจากการจัดการ symbolic link ภายในไฟล์ ZIP ที่ไม่ถูกต้อง ซึ่งเปิดโอกาสให้ไฟล์ ZIP ที่ถูกสร้างขึ้นเปิดช่องให้สามารถเข้าถึงไดเรกทอรีที่ไม่ควรเข้าถึง (directory traversal) และอาจถูกนำไปใช้รันโค้ดในสิทธิ์ของ service account ได้ โดยผู้ผลิตได้แก้ไขปัญหานี้แล้วในเวอร์ชัน 25.00 ซึ่งครอบคลุมทั้งช่องโหว่ CVE-2025-11001 และ CVE-2025-11002 ที่มีสาเหตุจากการจัดการ symbolic link ลักษณะเดียวกัน ทั้งสองช่องโหว่นี้ปรากฏอยู่ในซอฟต์แวร์ตั้งแต่เวอร์ชัน 21.02 ทำให้ผู้ใช้งานที่ยังไม่ได้อัปเดตเวอร์ชันมีความเสี่ยงต่อการถูกโจมตีเพิ่มขึ้น

มาตรการป้องกันและแนวทางปฏิบัติ เพื่อป้องกันภัยคุกคามจากช่องโหว่นี้ สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่นำ software ดังกล่าวมาใช้งานภายในองค์กร ดำเนินการตรวจสอบและเสริมมาตรการด้านความมั่นคงปลอดภัย โดยอัปเดตโปรแกรม 7-Zip เป็นเวอร์ชัน 25.00 หรือใหม่กว่า ควบคู่กับการตรวจสอบเครื่องผู้ใช้งาน โดยเฉพาะอุปกรณ์ที่ใช้สิทธิ์ระดับสูงหรือเปิดโหมด Developer เพื่อค้นหาการตั้งค่าที่อาจผิดปกติ พร้อมทั้งแจ้งให้ผู้ใช้งานภายในองค์กรท่าน ทราบถึงความเสี่ยงนี้ และหลีกเลี่ยงการเปิดไฟล์ ZIP ที่มาจากแหล่งที่ไม่สามารถตรวจสอบได้ และเพิ่มการเฝ้าระวังกิจกรรมที่ผิดปกติผ่านระบบตรวจจับภัยคุกคามขององค์กร นอกจากนี้ควรตรวจสอบ service account ที่เชื่อมโยงกับระบบงานที่อาจมีการสร้าง แก้ไข หรือเพิ่มขึ้นโดยไม่ได้รับอนุญาต เพื่อให้สามารถจำกัดความเสียหายและลดความเสี่ยงจากการถูกโจมตีได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2025/11/hackers-actively-exploiting-7-zip.html
2. https://nvd.nist.gov/vuln/detail/CVE-2025-11001