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

ช่องโหว่ระดับร้ายแรงใน Apache Tika (CVE-2025-66516) และ WinRAR (CVE-2025-6218)

วันที่แจ้งเตือน 16 ธันวาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการประกาศแจ้งเตือนช่องโหว่ระดับร้ายแรงในผลิตภัณฑ์ Apache Tika และ WinRAR ดังนี้

1. **Apache Tika** : ช่องโหว่ CVE-2025-66516 เป็นประเภท XML External Entity (XXE) injection ซึ่งเกิดจากการประมวลผลข้อมูล XML หรือ XFA ที่ถูกฝังอยู่ในไฟล์ PDF ส่งผลให้ผู้ไม่ประสงค์ดีอาจใช้ช่องโหว่นี้เพื่อส่งไฟล์ PDF เข้าสู่ระบบเมื่อมีการประมวลผลทำให้สามารถเข้าถึงข้อมูลหรือทรัพยากรภายในเครือข่ายขององค์กรและทำให้เกิดความเสียหายได้ เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้น แนะนำให้ผู้ประกอบธุรกิจที่มีการใช้ Apache Tika พิจารณาอัปเดตเป็นเวอร์ชันที่มีการแก้ไขช่องโหว่หรือพิจารณาดำเนินการที่เหมาะสม เพื่อลดโอกาสทำให้เกิดความเสี่ยงจากกรณีที่ยังไม่สามารถอัปเดตเวอร์ชั่นของซอฟต์แวร์ได้

2. **WinRAR** : ช่องโหว่ CVE-2025-6218 เป็นประเภท path traversal ซึ่งได้ถูกนำไปใช้โจมตีจริงโดยกลุ่มผู้ไม่ประสงค์ดีหลายกลุ่ม โดยถูกนำไปใช้เพื่อหลอกลวงให้ผู้ใช้งานเปิดไฟล์หรือเข้าถึงเนื้อหาที่เป็นอันตราย ส่งผลให้ผู้ไม่ประสงค์ดีสามารถวางไฟล์และรันโค้ดภายใต้สิทธิ์ของผู้ใช้งานได้ ทั้งนี้ บริษัทผู้พัฒนาซอฟต์แวร์ได้ออก Security Patch เพื่อแก้ไขช่องโหว่แล้วใน WinRAR เวอร์ชัน 7.12 ซึ่งช่องโหว่ดังกล่าวมีผลเฉพาะกับระบบปฏิบัติการ Windows เท่านั้น จึงขอแนะนำให้ผู้ประกอบธุรกิจ ตรวจสอบและอัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด หลีกเลี่ยงการเปิดไฟล์แนบหรือไฟล์บีบอัดจากแหล่งที่ไม่น่าเชื่อถือ และเสริมมาตรการเฝ้าระวังด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อลดความเสี่ยงจากการถูกโจมตีและผลกระทบที่อาจเกิดขึ้นต่อระบบและข้อมูลสำคัญของบริษัทท่าน

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

ข้อมูลอ้างอิง

Apache Tika

1. https://securityaffairs.com/185710/security/atlassian-fixed-maximum-severity-flaw-cve-2025-66516-in-apache-tika.html
2. https://nvd.nist.gov/vuln/detail/CVE-2025-66516

WinRAR

1. https://thehackernews.com/2025/12/warning-winrar-vulnerability-cve-2025.html
2. https://nvd.nist.gov/vuln/detail/CVE-2025-6218

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ