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

เหตุข้อมูลรั่วไหล (Data Breach) จากการโจมตีผ่านช่องโหว่ Zero-Day ของ Third-Party Software

วันที่แจ้งเตือน 19 พฤศจิกายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบกรณีบริษัท Logitech International S.A. รายงานต่อสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ของสหรัฐอเมริกา กรณีข้อมูลรั่วไหล (Data Breach) จากการโจมตีโดยกลุ่ม Clop ผ่านช่องโหว่ Zero-Day ของ Third-Party Software

Logitech เปิดเผยว่าเหตุการณ์ดังกล่าวเกิดจากการนำข้อมูลออกจากระบบ (Data Exfiltration) ผ่านช่องโหว่ Zero-Day ในซอฟต์แวร์ของผู้ให้บริการภายนอก โดยบริษัทระบุว่า เหตุการณ์นี้ไม่ส่งผลกระทบต่อผลิตภัณฑ์ กระบวนการผลิต หรือการให้บริการหลักของบริษัท แต่มีข้อมูลบางส่วนของพนักงาน ลูกค้าและคู่ค้า ซึ่งมิได้เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ถูกเข้าถึง จึงไม่ปรากฏว่าได้รับผลกระทบอย่างมีนัยสำคัญ รวมทั้ง ได้ทำ Security Patch ทันที

เหตุการณ์ครั้งนี้อาจมีความเชื่อมโยงกับช่องโหว่ Zero-Day ของ Oracle E-Business Suite (CVE-2025-61882) ซึ่งกลุ่ม Clop เคยใช้โจมตีองค์กรต่าง ๆ มาแล้ว และเป็นกลุ่มที่มีประวัติใช้ประโยชน์จากช่องโหว่ Zero-Day หลายรายการ ซึ่งส่งผลกระทบเป็นวงกว้าง เหตุการณ์นี้แม้จะเกิดกับบริษัทต่างประเทศ แต่สะท้อนถึงความเสี่ยงขององค์กรซึ่งพึ่งพาผู้ให้บริการ ภายนอกด้านซอฟต์แวร์ โดยเฉพาะระบบที่จัดเก็บข้อมูลลูกค้า พนักงาน หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ Third-Party Software ดังกล่าว ผู้ประกอบธุรกิจควรพิจารณา อัปเดต Security Patch ตามที่เจ้าของผลิตภัณฑ์แนะนำ ควบคู่กับการประเมินความเสี่ยงของผู้ให้บริการภายนอก ตรวจสอบบัญชีผู้ใช้งานและการควบคุมสิทธิ์ให้รัดกุม เฝ้าระวังความผิดปกติเกี่ยวกับการส่งข้อมูลจำนวนมากผ่านระบบเครือข่าย และทบทวนแผนตอบสนองเหตุการณ์ฉุกเฉินให้ครอบคลุมความเสี่ยงจาก Third-Party รวมถึงการปรับปรุงให้มีประสิทธิภาพอยู่เสมอ

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/logitech-confirms-data-breach-after-clop-extortion-attack/
2. https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
3. https://nvd.nist.gov/vuln/detail/CVE-2025-61882