แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณีพบส่วนขยายเว็บเบราว์เซอร์ Chrome บางรายการมีโค้ดที่เป็นอันตราย และพบช่องโหว่ที่สำคัญหลายรายการในผลิตภัณฑ์ Apache

วันที่แจ้งเตือน 10 มกราคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

จากการติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ ของสำนักงาน ก.ล.ต. และ การแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เกี่ยวกับกรณีพบการโจมตีในหลายรูปแบบ จากการใช้งานส่วนขยาย (extension) ของโปรแกรม Chrome Web Browser ถูกผู้ไม่ประสงค์ดีใช้วิธีการฟิชชิ่งเพื่อเข้าถึงบัญชีผู้ดูแลระบบ รวมทั้งพบช่องโหว่สำคัญที่ทำให้ผู้ไม่ประสงค์ดี สามารถข้ามขั้นตอนการยืนยันตัวตนแบบ 2FA ได้ โดยการขโมย session cookies ซึ่งทำให้สามารถปลอมตัวเป็นผู้ใช้งานที่ได้รับสิทธิ์ถูกต้อง โดยไม่จำเป็นต้องใช้รหัส 2FA และล่าสุดยังตรวจพบส่วนขยาย Chrome อีก 25 รายการที่ถูกแทรกโค้ดอันตราย เพื่อขโมยข้อมูลส่วนบุคคลของผู้ใช้งาน (เอกสารแนบ ThaiCERT 1 – Chrome Extension)

นอกจากนี้ ยังมีการแจ้งเตือน กรณีพบการรายงานช่องโหว่ที่สำคัญหลายรายการใน ผลิตภัณฑ์ Apache จำนวน 3 รายการที่อาจส่งผลกระทบต่อระบบ ดังนี้

1. ช่องโหว่หมายเลข CVE-2024-43441 การใช้ประโยชน์จากช่องโหว่นี้ใน Apache HugeGraph-Server ซึ่งเป็นเซิร์ฟเวอร์ฐานข้อมูลกราฟ อาจอนุญาตให้ผู้โจมตีสามารถข้ามกลไกการตรวจสอบสิทธิ์ที่มีอยู่ ส่งผลให้สามารถเข้าถึงระบบได้โดยไม่ได้รับอนุญาต

2. ช่องโหว่หมายเลข CVE-2024-45387 การใช้ประโยชน์จากช่องโหว่นี้ใน Traffic Ops ใน Apache Traffic Control ซึ่งเป็นเครื่องมือสำหรับการจัดการและเพิ่มประสิทธิภาพเครือข่ายการส่งเนื้อหา (CDN) อาจอนุญาตให้ผู้โจมตีทำ SQL injection ได้

3. ช่องโหว่หมายเลข CVE-2024-52046 การใช้ประโยชน์จากช่องโหว่นี้ใน Apache MINA ซึ่งเป็นเฟรมเวิร์กของแอปพลิเคชันเครือข่าย อาจอนุญาตให้ผู้โจมตีสามารถใช้ประโยชน์จากกระบวนการ deserialization ซึ่งอาจนำไปสู่การโจมตีการเรียกใช้โค้ดระยะไกล

ช่องโหว่เหล่านี้ส่งผลกระทบต่อผลิตภัณฑ์ ดังนี้

- Apache HugeGraph - Server เวอร์ชันก่อน 1.5.0
- Apache Traffic Control เวอร์ชัน 8.0.0 ถึง 8.0.1
- Apache MINA core เวอร์ชันก่อน 2.0.27, 2.1.10 และ 2.24

เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ ขอแนะนำให้องค์กร ดำเนินการการอัปเดตระบบปฏิบัติการและส่วนขยายที่ใช้งานให้เป็นเวอร์ชันล่าสุดอยู่เสมอ ควรพิจารณาถอนการติดตั้งส่วนขยายหรือจำกัดการใช้ส่วนขยาย (extension) เท่าที่จำเป็น ตรวจสอบสิทธิ์การเข้าถึงที่ส่วนขยายร้องขอก่อนติดตั้ง พร้อมทั้งเปลี่ยนรหัสผ่านสำหรับ บัญชีที่สำคัญ และติดตามการอัปเดตความปลอดภัยจากบริษัทผู้ผลิต และดำเนินการตรวจสอบความน่าเชื่อถือของแหล่งที่มาแอปพลิเคชันก่อนดำเนินการดาวน์โหลด

แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ทั้งนี้ เมื่อตรวจพบหรือสงสัยว่าองค์กรกำลังเผชิญกับการโจมตีทางไซเบอร์ ขอแนะนำพิจารณาแนวทางการดำเนินการดังต่อไปนี้

1. ควรรีบดำเนินการตัดการเชื่อมต่อของระบบหรืออุปกรณ์ที่ถูกโจมตีออกจากเครือข่ายทันที เพื่อป้องกันการแพร่กระจายของการโจมตีไปยังระบบอื่น พร้อมทั้งเก็บหลักฐานทางดิจิทัลที่เกี่ยวข้องไว้เพื่อการตรวจสอบ

2. แจ้งเหตุการณ์ไปยังทีมตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Response Team) หรือผู้รับผิดชอบด้านความมั่นคงปลอดภัยขององค์กรโดยทันที เพื่อประเมินสถานการณ์และวางแผนรับมือ

3. ป้องกันการเข้าถึงข้อมูล โดยพิจารณาเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานทั้งหมดที่อาจได้รับผลกระทบ โดยเฉพาะบัญชีที่มีสิทธิในระดับผู้ดูแลระบบ รวมถึงเพิ่มความเข้มงวดในการตรวจสอบสิทธิ์การเข้าถึงระบบ

4. กู้คืนระบบ ควรดำเนินการโดยผู้เชี่ยวชาญ เริ่มจากการสำรวจความเสียหาย ตรวจสอบช่องโหว่ที่ถูกใช้ในการโจมตี และดำเนินการปิดช่องโหว่ดังกล่าว ก่อนทำการกู้คืนระบบจากข้อมูลสำรองที่เชื่อถือได้

5. ภายหลังการแก้ไขเหตุการณ์ที่เกิดขึ้น ควรจัดทำรายงานวิเคราะห์เหตุการณ์อย่างละเอียด เพื่อหาสาเหตุที่แท้จริงและวางมาตรการป้องกันในระยะยาว พร้อมทั้งปรับปรุงแผนรับมือภัยคุกคามไซเบอร์ขององค์กรให้มีประสิทธิภาพมากขึ้น

6. ควรจัดการฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานทุกระดับอย่างต่อเนื่อง เพื่อลดความเสี่ยงจากการถูกโจมตีในอนาคต และสร้างวัฒนธรรมความปลอดภัยที่เข้มแข็งภายในองค์กร

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2024/12/16-chrome-extensions-hacked-exposing.html
2. https://www.bleepingcomputer.com/news/security/cybersecurity-firms-chrome-extension-hijacked-to-steal-users-data/
3. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-146