

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

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



ฝ้าระวังภัยคุกคามทางไซเบอร์จาก AI ที่มุ่งโจมตีผ่านทาง API

วันที่แจ้งเตือน 19 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบการธุรกิจหลักทรัพ์และผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล

สำนักงานได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีพบการนำความสามารถของ AI มาพัฒนาแนวทางการโจมตีทางไซเบอร์ที่ซับซ้อนและรวดเร็วยิ่งขึ้นอย่างต่อเนื่อง และปัจจุบันสำนักงานพบรายงานการโจมตีทางไซเบอร์ผ่านทาง Application Programming Interface (API) มากขึ้นอย่างต่อเนื่องทั้งในประเทศและต่างประเทศโดย API เป็นตัวเชื่อมโยงระบบงานสำคัญ ข้อมูลลูกค้า และธุรกรรมทางการเงินเข้าด้วยกัน จึงเป็นเป้าหมายหลักของผู้ไม่หวังดีที่มุ่งโจมตี ซึ่งอาจกระทบต่อระบบและข้อมูลของหน่วยงาน

รายละเอียดด้านความเสี่ยงและแนวโน้มภัยคุกคาม:

ผู้ไม่หวังดีมักตรวจสอบหรือค้นหา API ที่บริษัทเปิดให้บริการอยู่ และใช้ประโยชน์จากจุดอ่อนของ API เช่น ด้านการยืนยันตัวตน การตรวจสอบสิทธิ หรือการตั้งค่าระบบที่ไม่รัดกุม เป็นต้น เพื่อเข้าถึงข้อมูลหรือสั่งการระบบโดยไม่ได้รับอนุญาต

ผลกระทบที่อาจเกิดขึ้น:

- ข้อมูลส่วนบุคคลของลูกค้ารั่วไหล
- ข้อมูลหรือธุรกรรมถูกแก้ไข
- ระบบถูกใช้ส่งข้อความในนามบริษัท และ
- การให้บริการหยุดชะงัก ซึ่งกระทบทั้งลูกค้าและความน่าเชื่อถือของบริษัท

แนวทางป้องกัน: ผู้ประกอบการธุรกิจควรพิจารณาดำเนินการ ทบทวน การควบคุมการใช้งาน API ทั้งที่เปิดให้บุคคลภายนอกใช้และที่ใช้ภายใน โดยอาจพิจารณา OWASP API Security Top 10 เป็นแนวทางการดำเนินการอย่างน้อยดังนี้

1. API1: Broken Object Level Authorization

ตรวจสอบสิทธิการเข้าถึง Object ทุกครั้งที่มีการอ้างอิงข้อมูลด้วย ID จากผู้ใช้ และไม่ไว้วางใจค่าที่ส่งมาจาก Client โดยตรง

2. API2: Broken Authentication

ใช้กลไกยืนยันตัวตนที่รัดกุม จัดการ Token อย่างปลอดภัย และป้องกันการสวมรอยหรือขโมยข้อมูลรับรองตัวตน

3. API3: Broken Object Property Level Authorization

กำหนดสิทธิการเข้าถึงและแก้ไขข้อมูลในระดับ Field อย่างเหมาะสม และเปิดเผยเฉพาะข้อมูลที่เป็นที่จำเป็น

4. API4: Unrestricted Resource Consumption

กำหนด Rate Limiting, Quota และ ขนาดคำขอสูงสุด เพื่อลดความเสี่ยงจาก DoS และการใช้ทรัพยากรเกินความจำเป็น

5. API5: Broken Function Level Authorization

ตรวจสอบสิทธิทุกฟังก์ชันตามบทบาทผู้ใช้งาน และแยกสิทธิผู้ดูแลระบบออกจาก ผู้ใช้ทั่วไปอย่างชัดเจน

6. API6: Unrestricted Access to Sensitive Business Flows

เพิ่มการควบคุมธุรกรรมสำคัญ เช่น Rate Limiting หรือ Anti-Bot เป็นต้น เพื่อป้องกันการใช้งานแบบอัตโนมัติที่ส่งผลกระทบต่อธุรกิจ

7. API7: Server Side Request Forgery (SSRF) ตรวจสอบและ

จำกัด URL หรือ ปลายทางที่ API สามารถเชื่อมต่อได้ เพื่อลดความเสี่ยงจากการเข้าถึงระบบภายในโดยไม่ได้รับอนุญาต

8. API8: Security Misconfiguration

ใช้การตั้งค่าที่ปลอดภัยตามมาตรฐาน ปิดบริการที่ไม่จำเป็น และหลีกเลี่ยงการใช้ค่าทดสอบหรือค่าเริ่มต้นในระบบ Production

9. API9: Improper Inventory Management

จัดทำทะเบียน API, Host และ Version ให้เป็นปัจจุบัน พร้อมยกเลิก API ที่เลิกใช้งานหรือไม่มีการดูแลแล้ว

10. API10: Unsafe Consumption of APIs

ตรวจสอบและยืนยันความถูกต้องของข้อมูลจาก Third-Party API ก่อนประมวลผล และไม่เชื่อถือข้อมูลจากภายนอกโดยอัตโนมัติ

ข้อมูลอ้างอิง

- <https://api-security.owasp.org/>
- <https://api-security.owasp.org/editions/2023/en/0x11-t10/>