แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Framework เจาะระบบอัตโนมัติ “CAIRN” ถูกใช้เป็นแคมเปญโจมตี

วันที่แจ้งเตือน 24 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงาน กรณีทีม Threat Intelligence ของ Amazon ตรวจพบผู้ไม่หวังดีใช้ CAIRN ซึ่งเป็น Open-source Autonomous AI Penetration-testing Framework ในการโจมตีเป้าหมาย โดยกำหนดคำสั่งให้ AI Agent เข้าถึง Shell หลังจากนั้น AI Agent สามารถ วางแผน ดำเนินการ และปรับเปลี่ยนวิธีการโจมตีได้ด้วยตนเอง โดยอัตโนมัติและไม่ต้องอาศัยมนุษย์

รายงานระบุว่า CAIRN ถูกใช้ในแคมเปญที่มุ่งเป้าไปยัง IP Address ของหลายองค์กรโดยใช้เวลาโจมตีประมาณ 48 ชั่วโมง โดย AI Agent ดังกล่าวเจาะระบบอัตโนมัติ ซึ่งมีทั้งกรณีที่พยายามเข้าถึงโดยดำเนินการสำรวจระบบ ทดลองเทคนิคการโจมตี และเปลี่ยนวิธีการได้อย่างต่อเนื่องโดยดำเนินการประมาณ 16 ชั่วโมงและทดลองวิธีโจมตี 148 รูปแบบ รวมทั้งกรณีที่เจาะระบบได้สำเร็จ โดย AI Agent ได้วิเคราะห์ Application Framework และสำรวจ API Endpoint ของ Open-source medical imaging AI application และได้ทดสอบพารามิเตอร์ดังกล่าวเพื่อหาช่องโหว่ประเภท Path Traversal และพบว่าพารามิเตอร์นั้น มีช่องโหว่จริง ซึ่งเปิดทางให้สามารถเขียนไฟล์ลงบน Server ได้โดยใช้เวลาประมาณ 11 นาทีตั้งแต่เริ่มสำรวจ API จนสามารถเขียนไฟล์ได้สำเร็จ

Amazon ประเมินว่าช่องโหว่ดังกล่าวเป็น Zero-day เนื่องจากยังไม่พบ Patch, Security Advisory หรือข้อมูลเกี่ยวกับช่องโหว่ที่ได้รับผลกระทบ โดยภายหลังได้แจ้งผู้ดูแลโครงการและมีการเผยแพร่ Patch และ Security Advisory แล้ว นอกจากนี้ผู้ไม่หวังดียังนำช่องโหว่เดียวกันไปใช้เป็นช่องทางเข้าสู่เครือข่ายขององค์กรอีกแห่งและสั่งให้ AI Agent ขยายการเข้าถึงไปยังระบบอื่นภายในเครือข่าย

เหตุการณ์ดังกล่าวสะท้อนให้เห็นว่า Autonomous AI Agent สามารถช่วยเพิ่ม ความเร็ว ความต่อเนื่อง และความสามารถในการปรับเปลี่ยนวิธีการโจมตี ตั้งแต่การสำรวจระบบ ค้นหาช่องโหว่ ทดลองวิธีโจมตี ไปจนถึงการขยายสิทธิและเข้าถึงระบบ โดยเฉพาะกรณีที่ AI Agent สามารถค้นพบและใช้ประโยชน์จากช่องโหว่ Zero-day ได้ภายในเวลาไม่กี่นาที ซึ่งอาจทำให้การโจมตีดำเนินไปเร็วกว่ากระบวนการตรวจสอบ Alert และตอบสนองของทีม Security แบบเดิม

ข้อมูลอ้างอิง

1. https://aws.amazon.com/it/blogs/security/chinese-nexus-actors-cairn-ai-agents-found-a-zero-day-on-their-own/
2. https://github.com/Project-MONAI/MONAILabel/security/advisories/GHSA-qc22-rmgc-vg94
3. https://gambit.security/blog-posts/autonomous-ai-agents-online-retailers-25-a-company
4. https://securityaffairs.com/203664/ai/cairn-ai-framework-used-in-autonomous-zero-day-exploitation.html

แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Framework เจาะระบบอัตโนมัติ “CAIRN” ถูกใช้เป็นแคมเปญโจมตี

วันที่แจ้งเตือน 24 พฤศจิกายน 2569

ผู้ประกอบธุรกิจ ควรพิจารณาดำเนินการมาตรการป้องกันและลดความเสี่ยง ดังนี้

1. **ลดพื้นที่เสี่ยงของระบบที่เปิดให้เข้าถึงจากภายนอก** โดยตรวจสอบ Internet-facing Service, Management Interface, API Endpoint และ Database พร้อมปิด Service ที่ไม่จำเป็นและแก้ไขระบบที่ไม่มี Authentication หรือมีการตั้งค่าที่ไม่ปลอดภัย เนื่องจากเหตุการณ์พบทั้ง Cairn Instance และ Redis Server ที่เปิดใช้งานโดยไม่มีการยืนยันตัวตน
2. **เพิ่มการตรวจสอบ Web Application และ API อย่างต่อเนื่อง** โดยให้ความสำคัญกับ Upload Function, Path Traversal และ SSRF เนื่องจาก AI Agent สามารถสำรวจ API และค้นพบช่องโหว่ที่ใช้เขียนไฟล์ลงบน Server ได้
3. **เพิ่มการตรวจจับพฤติกรรมการโจมตีแบบอัตโนมัติ** โดยเฝ้าระวังการ Scan หรือ Request จำนวนมาก การทดลอง Credentials อย่างต่อเนื่อง การเปลี่ยน Attack Technique ภายในระยะเวลาสั้น ตลอดจนการสร้างไฟล์ Process หรือ Reverse Shell ที่ผิดปกติบน Server
4. **ควบคุมการเชื่อมต่อและการเคลื่อนย้ายภายในเครือข่าย** โดยจำกัดการเข้าถึงบริการสำคัญ เช่น Redis, PostgreSQL, SSH และ VPN รวมถึงเฝ้าระวังการใช้ Proxy Tunnel หรือการเชื่อมต่อระหว่างระบบที่ผิดปกติ เพื่อลดโอกาสที่ผู้ไม่หวังดีจะใช้ระบบที่ถูกโจมตีเป็นช่องทางขยายผลไปยังระบบอื่น
5. **ยกระดับการตรวจจับและตอบสนองให้ทันต่อ Autonomous AI Attack** โดยให้ความสำคัญกับ Detection ที่มีความเชื่อมั่นสูงและสามารถกระตุ้น Automated Response ได้ พร้อมให้บุคลากรกำกับและตรวจสอบผลลัพธ์ แทนการตรวจสอบกิจกรรมทุกขั้นตอนด้วยตนเอง เพื่อให้สามารถตอบสนองต่อการโจมตีที่มีความเร็วสูงได้อย่างทันท่วงที

สำนักงาน ก.ล.ต. และ TCM-CERT ตระหนักถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศและความต่อเนื่องในการดำเนินธุรกิจของหน่วยงานในภาคตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวเพื่อให้หน่วยงานท่านพิจารณาดำเนินการเฝ้าระวังและเตรียมความพร้อมรับมือ เพื่อป้องกันหรือลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินธุรกิจ รวมทั้งการประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้แก่ สำนักงาน ก.ล.ต. หรือหน่วยงานควบคุมหรือกำกับดูแลอื่น ๆ เพื่อให้หน่วยงานท่านสามารถตอบสนองได้อย่างทันท่วงที

ข้อมูลอ้างอิง

1. https://aws.amazon.com/it/blogs/security/chinese-nexus-actors-cairn-ai-agents-found-a-zero-day-on-their-own/
2. https://github.com/Project-MONAI/MONAILabel/security/advisories/GHSA-qc22-rmgc-vg94
3. https://gambit.security/blog-posts/autonomous-ai-agents-online-retailers-25-a-company
4. https://securityaffairs.com/203664/ai/cairn-ai-framework-used-in-autonomous-zero-day-exploitation.html

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

ช่องโหว่ใน Apache Tomcat เสี่ยงถูกนำไปใช้ในการโจมตี (CVE-2026-133325)

วันที่แจ้งเตือน 24 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Apache Software Foundation ได้เปิดเผยช่องโหว่ระดับ Critical ใน Apache Tomcat ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีจากระยะไกลเข้าร่วม Trusted Server Cluster โดยไม่ผ่านการยืนยันตัวตน

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Apache	• **ช่องโหว่ CVE-2026-133325** เป็นช่องโหว่ใน Apache Tomcat Cluster ที่ใช้ TLS 1.3 ร่วมกับ Pre-Shared Key (PSK) เกิดจาก Tomcat ไม่ตรวจสอบตัวตนของ Server ที่อยู่ปลายทางของการเชื่อมต่อ ทำให้การเชื่อมต่อสามารถถูกเข้ารหัสได้โดยไม่มีการยืนยันว่า Server ดังกล่าวได้รับอนุญาตให้เข้าร่วม Cluster ส่งผลให้ผู้ไม่หวังดีจากระยะไกลที่สามารถเข้าถึง Service สำหรับการสื่อสารระหว่าง Cluster Member ผ่านเครือข่าย อาจเข้าร่วม Trusted Server Cluster โดยไม่ต้องผ่านการยืนยันตัวตน • Apache Software Foundation แนะนำวิธีแก้ไขชั่วคราว (Workaround) เปลี่ยนการตั้งค่าการเข้ารหัสของ Cluster จาก TLS 1.3 ไปใช้ TLS 1.2 ร่วมกับ TLS-PSK และจำกัดการเข้าถึงเครือข่ายตั้งค่า Firewall เพื่อจำกัดการเข้าถึงพอร์ตสื่อสารของ Cluster	• ส่งผลกระทบต่อ Apache Tomcat เวอร์ชัน ▪ 11.0.28 - 10.0.29 ▪ 10.1.62 ▪ 9.0.124 • รุ่นที่ได้รับการแก้ไข ได้แก่ 11.0.30, 10.1.63 และ 9.0.125 ตามลำดับ

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/cve-2026-133325
2. https://lists.apache.org/thread/b53dmjwf81667pw1r27zxx8s6hw71bdn
3. https://tomcat.apache.org/security-11.html
4. https://cybersecuritynews.com/critical-apache-tomcat-flaw/