แจ้งเตือน

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

ช่องโหว่ UI ของ Nginx (CVE-2026-33032) ถูกนำไปใช้โจมตีจริง

วันที่แจ้งเตือน 16 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับช่องโหว่ใน Nginx UI (CVE-2026-33032) ซึ่งเป็นอินเทอร์เฟซการบริหารจัดการ Nginx Server ผ่าน web interface ถูกนำไปใช้โจมตีจริงได้โดยไม่ต้องผ่านการยืนยันตัวตน

ช่องโหว่นี้เกี่ยวข้องกับ MCP integration ซึ่งผู้ไม่หวังดีสามารถใช้ส่งคำขอ (HTTP Request) ที่ถูกสร้างขึ้นเพื่อเข้าควบคุม Nginx Server ได้โดยตรง โดยไม่ต้องผ่านการยืนยันตัวตน (Bypass authentication) เพื่อติดตั้ง Backdoor เปลี่ยนเส้นทางผู้ใช้งานหรือขโมยข้อมูลสำคัญ โดยช่องโหว่นี้ยังสัมพันธ์ช่องโหว่อื่น 2 รายการ ได้แก่ (1) CVE-2026-27944 ซึ่งผู้ไม่หวังดีสามารถดาวน์โหลดข้อมูลสำรองโดยไม่ต้องผ่านการยืนยันตัวตน และ (2) CVE-2026-33030 ซึ่งผู้ไม่หวังดีสามารถเข้าถึง แก้ไข หรือ ลบข้อมูลของผู้ใช้งานรายอื่นได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาตรวจสอบการใช้งาน Nginx UI และดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่บริษัทผู้ผลิตแนะนำ (เวอร์ชัน 2.3.4 หรือสูงกว่า) พร้อมทั้งตรวจสอบระบบที่เปิดให้เข้าถึงจากภายนอก (internet-facing systems) เฝ้าระวังพฤติกรรมการร้องขอ (HTTP requests) ที่ผิดปกติ และติดตามตรวจสอบบันทึกเหตุการณ์ (Log Monitoring) เพื่อให้สามารถตรวจจับและตอบสนองต่อความพยายามโจมตีที่อาจใช้ประโยชน์จากช่องโหว่ดังกล่าวได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://www.securityweek.com/exploited-vulnerability-exposes-nginx-servers-to-hacking/
2. https://nvd.nist.gov/vuln/detail/CVE-2026-33032
3. https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-h6c2-x2m2-mwhf

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ