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

แจ้งเตือน พบรายงานการโจมตีโดยใช้มัลแวร์ BADCANDY ผ่านช่องโหว่ระดับร้ายแรง (CVE-2023-20198) ของ Cisco IOS XE เพิ่มมากขึ้น

วันที่แจ้งเตือน 3 พฤศจิกายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่าหน่วยงานความมั่นคงไซเบอร์ของออสเตรเลีย (Australian Signals Directorate - ASD) ได้รายงานกรณีมัลแวร์ BADCANDY โจมตีผ่านช่องโหว่ระดับร้ายแรง CVE-2023-20198 ของอุปกรณ์ Cisco IOS XE ที่ยังไม่ได้อัปเดตแพตช์เพิ่มมากขึ้น โดยผู้ไม่ประสงค์ดีสามารถข้ามการพิสูจน์ตัวตน (unauthenticated attacker) และใช้สิทธิ High Privilege ควบคุมอุปกรณ์ Switch และ Router ดังกล่าวจากระยะไกลได้

ASD ประเมินว่ามีอุปกรณ์ในออสเตรเลียจำนวนมากที่ถูกโจมตีด้วยมัลแวร์ BADCANDY และมีแนวโน้มเพิ่มขึ้น มัลแวร์ชนิดนี้มีลักษณะ non-persistent ซึ่งอาจจะหายไปหลังการรีบูต แต่หากอุปกรณ์ยังไม่ได้รับการอัปเดตและยังเปิด Web User Interface ระบบอาจถูกติดตั้งมัลแวร์ซ้ำได้อีก ASD ยังพบว่าผู้โจมตีสามารถตรวจจับได้ เมื่อมัลแวร์ถูกลบออกและจะกลับมาโจมตีใหม่ในอุปกรณ์เดิมที่ยังไม่ได้แพตช์

เพื่อป้องกันและลดความเสี่ยงดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้อุปกรณ์ดังกล่าวพิจารณาดำเนินการ ดังนี้

- ติดตั้ง Security Patch ตามคำแนะนำของ Cisco เพื่อแก้ไขช่องโหว่ CVE-2023-20198 และช่องโหว่อื่น ๆ ที่เกี่ยวข้อง
- จำกัดการเข้าถึง Web User Interface (Web UI) ของอุปกรณ์ Cisco IOS XE ให้เข้าถึงได้เฉพาะจากเครือข่ายที่เชื่อถือได้และจำเป็นเท่านั้น
- ตรวจสอบการตั้งค่าปัจจุบันสำหรับบัญชีผู้ใช้ที่มีสิทธิ์ระดับ High Privilege และลบบัญชีที่ไม่พึงประสงค์หรือที่ไม่ได้รับการอนุมัติออก รวมทั้งตรวจสอบบัญชีที่อาจถูกสร้างโดยผู้ไม่ประสงค์ดี เช่น "cisco_tac_admin," "cisco_support," "cisco_sys_manager," หรือ "cisco" และลบออกหากไม่ใช่บัญชีที่ใช้งานปกติ

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

ข้อมูลอ้างอิง

1. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/badcandy
2. https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/
3. https://thehackernews.com/2025/11/asd-warns-of-ongoing-badcandy-attacks.html
4. https://nvd.nist.gov/vuln/detail/cve-2023-20198
5. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z