แจ้งเตือน : ช่องโหว่

Critical

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน Cisco ออกอัปเดตเพื่อแก้ไขช่องโหว่ระดับ Critical ในอุปกรณ์สื่อสารไร้สาย Cisco Ultra-Reliable Wireless Backhaul (URWB)

วันที่แจ้งเตือน 15 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่เกี่ยวกับช่องโหว่ที่พบในซอฟต์แวร์ Cisco Unified Industrial Wireless สำหรับอุปกรณ์สื่อสารไร้สาย Ultra-Reliable Wireless Backhaul (URWB) ที่มีความเสี่ยงสูงสุด CVE-2024-20418 (คะแนน CVSS 10.0) ช่องโหว่นี้เกิดจากความบกพร่องในการตรวจสอบข้อมูลนำเข้าของระบบจัดการผ่านเว็บ (web interface) ส่งผลให้ผู้โจมตีสามารถเข้าถึงระบบจากระยะไกลได้โดยใช้ command injection และสามารถดำเนินการโจมตีด้วยการส่งคำขอ HTTP ที่ถูกดัดแปลงไปยังส่วนติดต่อผู้ใช้ระบบ เมื่อการโจมตีสำเร็จ ผู้โจมตีสามารถเรียกใช้คำสั่งใด ๆ ในระบบได้ด้วยสิทธิ์สูงสุด (root) ซึ่งอาจนำไปสู่การรั่วไหลของข้อมูล การหยุดชะงักของบริการ การเปลี่ยนแปลงการตั้งค่า และการติดตั้งซอฟต์แวร์ที่เป็นอันตราย

โดย Cisco ได้ออกอัปเดตซอฟต์แวร์เพื่อแก้ไขช่องโหว่นี้แล้ว ซึ่งอุปกรณ์ที่ได้รับผลกระทบ ได้แก่

- Cisco Catalyst IW9165D Heavy Duty Access Points
- Cisco Catalyst IW9165E Rugged Access Points
- Cisco Catalyst IW9167E Heavy Duty Access Points

คำแนะนำมาตรการป้องกันที่ครอบคลุมสำหรับผู้ใช้งานอุปกรณ์สื่อสารไร้สาย Cisco URWB โดยสิ่งแรกที่ควรดำเนินการคือการอัปเดตเฟิร์มแวร์เป็นเวอร์ชันล่าสุดทันที พร้อมกับตรวจสอบประวัติการเข้าถึงระบบย้อนหลังเพื่อให้มั่นใจว่าไม่มีการเข้าถึงที่ผิดปกติ รวมถึงการเปิดใช้งานการเข้ารหัสและระบบยืนยันตัวตนแบบ MFA พร้อมทั้งหมั่นตรวจสอบ logs ของระบบเพื่อเฝ้าระวังกิจกรรมที่น่าสงสัย และเตรียมแผนรับมือกับภัยคุกคามที่อาจเกิดขึ้น

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 8 พ.ย. 2567
2) https://nvd.nist.gov/vuln/detail/CVE-2024-20418
3) https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sabackhaul-ap-cmdinj-R7E28Ecs