

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

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



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

วันที่แจ้งเตือน 14 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบการธุรกิจหลักทรัพย์และผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่เกี่ยวกับช่องโหว่ที่พบในซอฟต์แวร์ Cisco Unified Industrial Wireless สำหรับอุปกรณ์ Ultra-Reliable Wireless Backhaul (URWB) ที่มีความเสี่ยงสูงสุด CVE-2024-20418 (คะแนน CVSS 10.0) ช่องโหว่นี้เกิดจากความบกพร่องในการตรวจสอบข้อมูลนำเข้าของระบบจัดการผ่านเว็บ (web interface) ส่งผลให้ผู้โจมตีสามารถเข้าถึงระบบจากระยะไกลได้โดยไม่ต้องยืนยันตัวตน และสามารถดำเนินการโจมตีด้วยการส่งคำขอ HTTP ที่ถูกดัดแปลงไปยังส่วนติดต่อผู้ใช้ระบบ เมื่อการโจมตีสำเร็จ ผู้โจมตีจะสามารถเรียกใช้คำสั่งใด ๆ ในระบบได้ด้วยสิทธิ์สูงสุด (root) ที่ถูกดัดแปลง ซึ่งอาจนำไปสู่การรั่วไหลของข้อมูล การหยุดชะงักของบริการ การเปลี่ยนแปลงการตั้งค่า และการติดตั้งซอฟต์แวร์ที่เป็นอันตราย

โดย Cisco ได้ออกอัปเดตซอฟต์แวร์เพื่อแก้ไขช่องโหว่ ซึ่งอุปกรณ์ที่ได้รับผลกระทบได้แก่

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

คำแนะนำมาตรการป้องกันที่ครอบคลุมสำหรับผู้ใช้งานอุปกรณ์ Cisco URWB โดยสิ่งแรกที่ควรดำเนินการคือการอัปเดตเฟิร์มแวร์เป็นเวอร์ชันล่าสุด พร้อมกับตรวจสอบประวัติการเข้าถึงระบบย้อนหลัง เพื่อให้มั่นใจว่าไม่มีการเข้าถึงที่ผิดปกติ รวมถึงการเปิดใช้งานการเข้ารหัสและระบบยืนยันตัวตนแบบ MFA พร้อมทั้งหมั่นตรวจสอบ logs ของระบบเพื่อเฝ้าระวังกิจกรรมที่น่าสงสัย และเตรียมแผนรับมือกับภัยคุกคามที่อาจเกิดขึ้น

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบการในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบการทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

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>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ