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

Cisco ออกอัปเดตด้านความมั่นคงปลอดภัยแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ (CVE-2025-20113, CVE-2025-20152)

วันที่แจ้งเตือน 4 มิถุนายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างใกล้ชิด และพบว่า Cisco ได้ประกาศเผยแพร่การอัปเดตซอฟต์แวร์ เพื่อแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยในผลิตภัณฑ์ ได้แก่ Cisco Unified Intelligence Center, Cisco Unified Contact Center Express และ Cisco Identity Services Engine

<u>รายละเอียดของช่องโหว่</u>

- CVE-2025-20113 เป็นช่องโหว่ที่เปิดโอกาสให้ผู้ไม่ประสงค์ดีที่ผ่านกระบวนการยืนยันตัวตนจากระยะไกลสามารถยกระดับสิทธิในระบบได้ (Privilege Escalation)
- CVE-2025-20152 เป็นช่องโหว่ที่เปิดโอกาสให้ผู้ไม่ประสงค์ดีใช้เพื่อโจมตีแบบ Denial-of-Service (DoS) ซึ่งจะส่งผลให้ระบบหยุดชะงัก กระทบต่อการให้บริการ

<u>ผลิตภัณฑ์ที่ได้รับผลกระทบ</u>

- Cisco Unified Intelligence Center เวอร์ชัน 12.5 และ 12.6
- Cisco Unified Contact Center Express เวอร์ชั่น 12.5(1) SU3 และเวอร์ชันก่อนหน้า
- Cisco Identity Services Engine เวอร์ชัน 3.4

เพื่อป้องกันความเสี่ยงที่อาจส่งผลต่อความมั่นคงปลอดภัยของระบบและข้อมูลหน่วยงานท่าน สำนักงาน ก.ล.ต. และ TCM-CERT ขอแนะนำให้หน่วยงานของท่านที่ใช้ผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการอัปเดตซอฟต์แวร์ตามที่ Cisco ให้คำแนะนำให้เป็นเวอร์ชันล่าสุด จากนั้นตรวจสอบกิจกรรมที่อาจมีลักษณะผิดปกติหรือน่าสงสัยในระบบ พร้อมทั้งทบทวนมาตรการควบคุมสิทธิการเข้าถึงให้เหมาะสม และควรติดตามข่าวสารเกี่ยวกับช่องโหว่และแนวโน้มภัยคุกคามใหม่ ๆ จากผู้ผลิตและหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ เพื่อให้สามารถป้องกันความเสี่ยงและรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

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

<u>ข้อมูลอ้างอิง</u>

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-049
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-priv-esc-3Pk96SU4
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-restart-ss-uf986G2Q

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ