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 ช่องโหว่ร้ายแรงของผลิตภัณฑ์ Cisco ISE (CVE-2025-20124 และ CVE-2025-20125)

วันที่แจ้งเตือน 10 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

Cisco บริษัทผู้ให้บริการโซลูชันด้านความปลอดภัยทางไซเบอร์ ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Cisco Identity Services Engine (ISE) 2 รายการ ได้แก่ CVE-2025-20124 (Insecure Java Deserialization) และ CVE-2025-20125 (Authorization Bypass) ส่งผลให้ผู้ไม่หวังดีที่ครอบครองสิทธิระดับผู้ดูแลระบบ (read-only admin) สามารถยกระดับสิทธิเป็น root และสามารถส่งคำสั่งที่ไม่เหมาะสมเข้าสู่ระบบ รวมถึง สามารถแก้ไขการตั้งค่าในระบบ และ restart ระบบได้

ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Cisco ISE และ Cisco ISE Passive Identity Connector (ISE-PIC) ทั้งนี้ Cisco ได้ออกคำแนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว ทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่ Cisco แนะนำโดยเร็วที่สุด ดังนี้

Cisco ISE Software Release	First Fixed Release
3.0 and earlier	Migrate to a fixed release
3.1	3.1P10
3.2	3.2P7
3.3	3.3P4
3.4	Not vulnerable

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

ข้อมูลอ้างอิง

1) https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF#vp
2) https://www.bleepingcomputer.com/news/security/critical-cisco-ise-bug-can-let-attackers-run-commands-as-root/
3) https://nvd.nist.gov/vuln/detail/CVE-2025-20124
4) https://nvd.nist.gov/vuln/detail/CVE-2025-20125