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 ออกอัปเดตด้านความมั่นคงปลอดภัยแก้ไขช่องโหว่ Cisco Identity Services Engine (CVE-2026-20029)

วันที่แจ้งเตือน 14 มกราคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Cisco ได้ประกาศเผยแพร่การอัปเดตซอฟต์แวร์เพื่อแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยร้ายแรง (CVE-2026-20029) ในผลิตภัณฑ์ Cisco Identity Services Engine (ISE) และ Cisco ISE Passive Identity Connector (ISE-PIC)

ช่องโหว่ดังกล่าวเกิดจากการประมวลผลข้อมูล XML ในระบบบริหารจัดการผ่านเว็บ (Web-based Management Interface) อย่างไม่เหมาะสม ซึ่งเปิดโอกาสให้ผู้ไม่ประสงค์ดีใช้ช่องโหว่นี้เพื่ออัปโหลด malicious file และอาจทำให้เกิดความเสียหายกับระบบและข้อมูลของหน่วยงานได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้ผลิตภัณฑ์ Cisco ISE และ Cisco ISE-PIC พิจารณาดำเนินการอัปเดตซอฟต์แวร์ เพื่อแก้ไขช่องโหว่ตามที่บริษัทผู้พัฒนาผลิตภัณฑ์แนะนำ พร้อมทั้งทบทวนการกำหนดสิทธิ์ผู้ดูแลระบบ รวมถึงจัดให้มีการเฝ้าระวังพร้อมตรวจสอบบันทึกการใช้งาน (Logs) เพื่อให้สามารถตรวจพบและรับมือกับพฤติกรรมที่อาจบ่งชี้ถึงการใช้งานที่ผิดปกติได้อย่างทันท่วงที และติดตามประกาศด้านความมั่นคงปลอดภัยจากผู้พัฒนาผลิตภัณฑ์อย่างใกล้ชิด

Cisco ISE or ISE-PIC Release	First Fixed Release
Earlier than 3.2	Migrate to a fixed release.
3.2	3.2 Patch 8
3.3	3.3 Patch 8
3.4	3.4 Patch 4
3.5	Not vulnerable.

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/cisco-warns-of-identity-service-engine-flaw-with-exploit-code/
2. https://nvd.nist.gov/vuln/detail/CVE-2026-20029
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-jWSbSDKt