แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Cisco ออก Security Patch แก้ไขช่องโหว่ CVE-2026-20188

วันที่แจ้งเตือน 7 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cisco ออก Security Patch เพื่อแก้ไขช่องโหว่ CVE-2026-20188 ในผลิตภัณฑ์ Cisco Crosswork Network Controller (CNC) และ Cisco Network Services Orchestrator (NSO) ซึ่งทำให้อุปกรณ์หรือระบบไม่สามารถทำงานได้ และต้องใช้การ manual reboot เพื่อให้ระบบกลับมาทำงานได้

ช่องโหว่ดังกล่าวเป็นประเภท Denial-of-Service (DoS) เกิดจากการกำหนดการจำกัดอัตราการเชื่อมต่อขาเข้าไม่เหมาะสม ทำให้ผู้ไม่หวังดีเข้าถึงระบบได้โดยไม่ต้องผ่านการยืนยันตัวตน เพื่อส่งคำขอเข้าถึงระบบจำนวนมาก ทำให้ระบบไม่สามารถควบคุมจำนวนทราฟฟิกการเข้าถึงระบบ และไม่สามารถรองรับคำขอจากผู้ใช้งานจริงได้ ทั้งนี้ Cisco ได้ออก security patch แก้ไขช่องโหว่ ดังนี้

Cisco CNC Release	First Fixed Release
7.1 and earlier	Migrate to a fixed release.
7.2	Not vulnerable.

Cisco NSO Release	First Fixed Release
6.3 and earlier	Migrate to a fixed release.
6.4	6.4.1.3
6.5	Not vulnerable.

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานอุปกรณ์หรือระบบที่เกี่ยวข้อง พิจารณาตรวจสอบการใช้งานระบบ CNC และ NSO ดำเนินการอัปเดตแพตช์ความปลอดภัยหรือซอฟต์แวร์เป็นเวอร์ชันล่าสุดตามคำแนะนำของผู้ผลิต ทบทวนการเปิดให้บริการระบบจากเครือข่ายภายนอก พร้อมทั้งเฝ้าระวังปริมาณทราฟฟิกเข้าสู่ระบบที่ผิดปกติ ที่อาจบ่งชี้ถึงความพยายามโจมตีแบบ Denial-of-Service รวมถึงควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้ทันต่อเหตุภัยคุกคามไซเบอร์ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/new-cisco-dos-flaw-requires-manual-reboot-to-revive-devices/
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-dos-7Egqyc
3. https://nvd.nist.gov/vuln/detail/CVE-2026-20188

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ