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 แก้ไขช่องโหว่ในผลิตภัณฑ์ IMC และ SMM (CVE-2026-20093 และ CVE-2026-20160)

วันที่แจ้งเตือน 3 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cisco ออก Security Patch เพื่อแก้ไขช่องโหว่ความรุนแรงระดับวิกฤตในผลิตภัณฑ์ จำนวน 2 รายการ ได้แก่

(1) ช่องโหว่ CVE-2026-20093 ในผลิตภัณฑ์ Cisco Integrated Management Controller (IMC) เกิดจากการจัดการคำขอเปลี่ยนรหัสผ่านที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถส่งคำขอ HTTP ที่ถูกสร้างขึ้นเพื่อหลบเลี่ยงกระบวนการยืนยันตัวตน (authentication bypass) และเปลี่ยนรหัสผ่านของผู้ใช้งานรวมถึงบัญชีผู้ดูแลระบบ ทำให้ผู้ไม่หวังดีเข้าควบคุมระบบได้

(2) ช่องโหว่ CVE-2026-20160 ในผลิตภัณฑ์ Cisco Smart Software Manager On-Prem (SMM) ซึ่งเกิดจาก Internal service exposure ทำให้ผู้ไม่หวังดีสามารถส่งคำสั่งไปยัง API ที่เกี่ยวข้องและรันคำสั่งบนระบบปฏิบัติการพื้นฐานด้วยสิทธิระดับสูง (High privileges) จากระยะไกลโดยไม่ต้องผ่านการยืนยันตัวตนเพื่อควบคุมระบบได้

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าวสำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานอุปกรณ์หรือระบบที่เกี่ยวข้อง พิจารณาดำเนินการอัปเดต Security Patch ผลิตภัณฑ์ IMC และ SMM เป็นเวอร์ชันล่าสุดตามคำแนะนำของผู้ผลิต เฝ้าระวังและติดตามพฤติกรรมการเข้าถึงที่ผิดปกติ ควบคู่กับการเฝ้าระวังและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง และควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสมเพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2026-20093
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
3. https://nvd.nist.gov/vuln/detail/CVE-2026-20160
4. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ