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 แก้ไขช่องโหว่ใน Firewall Management Center จำนวน 2 รายการ (CVE-2026-20079 และ CVE-2026-20131)

วันที่แจ้งเตือน 5 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Cisco ประกาศออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์ Cisco Secure Firewall Management Center (FMC) จำนวน 2 รายการ ได้แก่ (1) ช่องโหว่ CVE-2026-20079 เป็นประเภท Authentication Bypass ซึ่งเกิดขึ้นในส่วนของ Web Interface ของระบบ FMC โดยผู้ไม่ประสงค์ดีสามารถโจมตีจากระยะไกลโดยไม่ต้องมีการยืนยันตัวตน ทำให้สามารถส่งคำร้อง HTTP ที่ถูกสร้างขึ้นเพื่อข้ามกระบวนการตรวจสอบสิทธิ์และเรียกใช้สคริปต์บนระบบ เพื่อเข้าถึงสิทธิ์ระดับ root บนระบบปฏิบัติการของอุปกรณ์ได้ และ (2) ช่องโหว่ CVE-2026-20131 เป็นประเภท Remote Code Execution (RCE) ซึ่งเกิดจากกระบวนการ Java Deserialization ที่ไม่เหมาะสม ภายใน Web Interface ของระบบ FMC โดยผู้ไม่ประสงค์ดีจากระยะไกลและส่งคำสั่ง Serialized Java Object ที่ถูกสร้างขึ้น เพื่อรันโค้ดตามต้องการบนอุปกรณ์ และยกระดับสิทธิ์เป็นระดับ root และส่งผลกระทบต่อระบบ Cisco Security Cloud Control (SCC) Firewall Management อีกด้วย

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานอุปกรณ์หรือระบบที่เกี่ยวข้อง พิจารณาตรวจสอบการใช้งานระบบ Cisco Secure Firewall Management Center (FMC) ดำเนินการอัปเดตแพตช์ความปลอดภัยหรือซอฟต์แวร์เป็นเวอร์ชันล่าสุดตามคำแนะนำของผู้ผลิต ควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง

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

ข้อมูลอ้างอิง

1. https://securityaffairs.com/188921/security/cisco-fixes-maximum-severity-secure-fmc-bugs-threatening-firewall-security.html
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2
3. https://nvd.nist.gov/vuln/detail/cve-2026-20079
4. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
5. https://nvd.nist.gov/vuln/detail/cve-2026-20131