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 ออก Security Patch แก้ไขช่องโหว่ Zero Day (CVE-2025-20393) ในผลิตภัณฑ์ Secure E-mail Gateway

วันที่แจ้งเตือน 19 มกราคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Cisco ประกาศออก Security Patch เพื่อแก้ไขช่องโหว่ Zero-day (CVE-2025-20393) ในผลิตภัณฑ์ Cisco Secure Email Gateway (SEG) และ Cisco Secure Email and Web Manager (SEWM) ที่ใช้ระบบปฏิบัติการ Cisco AsyncOS

ช่องโหว่ดังกล่าวเป็นประเภท Remote Command Execution (RCE) ที่มีกระบวนการตรวจสอบคำร้องขอ HTTP ที่ไม่เหมาะสม ซึ่งผู้ไม่ประสงค์ดีอาจสั่งรันคำสั่งบนระบบปฏิบัติการของอุปกรณ์ที่มีการเปิดใช้งานฟีเจอร์ Spam Quarantine

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานอุปกรณ์หรือระบบที่เกี่ยวข้อง พิจารณาดำเนินการติดตั้ง Security Patch ตามคำแนะนำของผู้ผลิต และดำเนินมาตรการด้านความมั่นคงปลอดภัย เช่น การจำกัดการเข้าถึงระบบจากเครือข่ายที่ไม่ปลอดภัย การปิดบริการหรือฟังก์ชันที่ไม่จำเป็น การเฝ้าระวังบันทึกการใช้งานระบบ (log) เพื่อค้นหาความผิดปกติ และใช้วิธีการยืนยันตัวตนที่มีความเข้มแข็งสำหรับผู้ดูแลระบบ เป็นต้น

Cisco Email Security Gateway

Cisco AsyncOS Software Release	First Fixed Release
14.2 and earlier	15.0.5-016
15.0	15.0.5-016
15.5	15.5.4-012
16.0	16.0.4-016

Secure Email and Web Manager

Cisco AsyncOS Software Release	First Fixed Release
15.0 and earlier	15.0.2-007
15.5	15.5.4-007
16.0	16.0.4-010

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/01/cisco-patches-zero-day-rce-exploited-by.html
2. https://nvd.nist.gov/vuln/detail/CVE-2025-20393
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ