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

แจ้งเตือน เจ้าของผลิตภัณฑ์ Cisco ออก Security Patch แก้ไขช่องโหว่ Zero-day ใน Cisco ASA และ FTD

วันที่แจ้งเตือน 29 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ และพบว่าบริษัท Cisco ได้ออกและติดตั้ง Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรงที่มีผลกระทบต่ออุปกรณ์ Cisco Security Firewall Adaptive Security Appliance (ASA) และ Firepower Threat Defense (FTD) ดังนี้

- CVE-2025-20333 ช่องโหว่การตรวจสอบ input ใน WebVPN ที่ผู้ไม่ประสงค์ดีที่ผ่านการพิสูจน์ตัวตนสามารถรันโค้ดในสิทธิ root บนอุปกรณ์ได้
- CVE-2025-20362 ช่องโหว่ผู้ไม่ประสงค์ดีใช้เข้าถึง endpoint URL ที่ถูกจำกัดได้โดยไม่ต้องพิสูจน์ตัวตน

นอกจากนี้ Cisco ยังได้ออก Security Patch เพื่อแก้ไขช่องโหว่ CVE-2025-20363 ที่เกี่ยวข้อง ซึ่งช่วยป้องกันการรันโค้ดโดยผู้ไม่ประสงค์ดีที่ไม่ผ่านการพิสูจน์ตัวตน

เพื่อป้องกันภัยคุกคามจากช่องโหว่นี้ สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินมาตรการเพื่อลดความเสี่ยงจากการโจมตีช่องโหว่ Cisco ASA และ FTD คือ อัปเกรดซอฟต์แวร์ให้เป็นเวอร์ชันที่ Cisco ออก security patch ล่าสุด พร้อมทั้งติดตามการใช้งานกรณีที่มีการใช้อุปกรณ์ที่ End of Support ตรวจสอบบันทึกเหตุการณ์ (log) และเพิ่มการเฝ้าระวังพฤติกรรมเครือข่ายที่มีลักษณะผิดปกติ รวมถึงการจำกัดสิทธิ์การเข้าถึงอุปกรณ์เครือข่ายเท่าที่จำเป็นและเสริมด้วยการใช้การยืนยันตัวตนหลายปัจจัย (MFA) สำหรับบัญชีผู้ดูแลระบบ เพื่อเสริมความมั่นคงปลอดภัยและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอย่างมีประสิทธิภาพ

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/cisa-orders-agencies-to-patch-cisco-flaws-exploited-in-zero-day-attacks/
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
4. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O