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

ช่องโหว่ Zero Day ใน SonicWall (CVE-2025-40602) และ Cisco (CVE-2025-20393)

วันที่แจ้งเตือน 18 ธันวาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการประกาศแจ้งเตือนช่องโหว่ระดับร้ายแรงในผลิตภัณฑ์ Sonicwall และ Cisco ดังนี้

1. **Sonicwall** : พบช่องโหว่ Zero-day (CVE-2025-40602) เป็นช่องโหว่ Local Privilege Escalation ในระบบ SonicWall SMA1000 Appliance Management Console (AMC) ที่ผู้ไม่ประสงค์ดีได้นำไปใช้โจมตีแล้ว โดยการเชื่อมโยงหลายช่องโหว่เข้าด้วยกัน ทั้งนี้ SonicWall ระบุว่าช่องโหว่ดังกล่าวไม่ส่งผลกระทบต่อการให้บริการ SSL-VPN บนอุปกรณ์ไฟร์วอลล์ อย่างไรก็ดี พบว่าผู้ไม่ประสงค์ดีสามารถเชื่อมโยงการใช้ช่องโหว่ดังกล่าวเข้ากับช่องโหว่ระดับร้ายแรง (CVE-2025-23006) ในระบบ SMA1000 เพื่อสั่งรันคำสั่งของระบบปฏิบัติการจากระยะไกล ทั้งนี้ช่องโหว่ CVE-2025-23006 ได้รับการแก้ไขแล้วในซอฟต์แวร์เวอร์ชัน 12.4.3-02854 (platform-hotfix) และเวอร์ชันที่ใหม่กว่า โดย SonicWall ได้แนะนำให้ผู้ใช้งานผลิตภัณฑ์ SMA1000 ดำเนินการอัปเกรดเป็นเวอร์ชันที่มีการแก้ไขช่องโหว่โดยเร็ว เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบสารสนเทศขององค์กร

2. **Cisco** : พบช่องโหว่ Zero-day (CVE-2025-20393) ในระบบ Cisco AsyncOS ที่ผู้ไม่ประสงค์ดีได้นำไปใช้โจมตีแล้ว โดยมีผลกระทบต่ออุปกรณ์ Cisco Secure Email Gateway (SEG) และ Cisco Secure Email and Web Manager (SEWM) ที่เปิดใช้งานฟังก์ชัน Spam Quarantine และเปิดให้เข้าถึงจากเครือข่ายอินเทอร์เน็ตโดยตรง ส่งผลให้ผู้ไม่ประสงค์ดีเข้าโจมตีได้ ทั้งนี้ Cisco ได้เผยแพร่รายการ IoCs เพื่อใช้ประกอบการตรวจสอบ และในระหว่างที่ยังไม่มีแพตช์แก้ไข ขอให้ผู้ดูแลระบบจำกัดการเข้าถึงอุปกรณ์ที่มีความเสี่ยง ลดการเปิดเผยต่ออินเทอร์เน็ต เสริมมาตรการควบคุมการเข้าถึง ตรวจสอบบันทึกการทำงานของระบบอย่างใกล้ชิด และปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยที่ Cisco แนะนำอย่างเคร่งครัด

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

ข้อมูลอ้างอิง

Sonicwall

1. https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-new-sma1000-zero-day-exploited-in-attacks/
2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

Cisco

1. https://www.bleepingcomputer.com/news/security/cisco-warns-of-unpatched-asyncos-zero-day-exploited-in-attacks/
2. https://nvd.nist.gov/vuln/detail/CVE-2025-20393
3. https://github.com/Cisco-Talos/IOCs/tree/main/2025/12