แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือน ช่องโหว่ความปลอดภัยระดับวิกฤตในระบบ SonicWall (CVE-2025-23006)

**วันที่แจ้งเตือน 24 มกราคม 2568**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ จึงขอแจ้งเตือนเกี่ยวกับช่องโหว่ความปลอดภัยระดับวิกฤตที่พบในระบบ SonicWall (Firewall & Secure Mobile Access) SMA1000 Appliance Management Console (AMC) และ Central Management Console (CMC) ซึ่งกำลังถูกใช้โจมตีแบบ Zero-day ในปัจจุบัน

Microsoft Threat Intelligence Center ได้ค้นพบช่องโหว่ที่มีความรุนแรงสูง (CVSS v3: 9.8) ประเภท Pre-authentication Deserialization (CVE-2025-23006) ซึ่งเป็นช่องโหว่ที่อาจทำให้ผู้ไม่ประสงค์ดีสามารถเรียกใช้คำสั่งระบบปฏิบัติการได้โดยไม่จำเป็นต้องยืนยันตัวตน ช่องโหว่นี้ส่งผลกระทบต่อเฟิร์มแวร์ของ SonicWall SMA1000 ดังกล่าว ทุกเวอร์ชันจนถึง 12.4.3-02804 โดยจากการสำรวจพบว่า มีอุปกรณ์ที่ได้รับผลกระทบและเปิดให้เข้าถึงจากอินเทอร์เน็ตมากกว่า 2,380 เครื่องทั่วโลก

SonicWall SMA1000 ใช้สำหรับการเข้าถึงเครือข่ายองค์กรผ่าน VPN ที่ใช้งานอย่างแพร่หลายซึ่งการถูกโจมตีผ่านช่องโหว่นี้อาจส่งผลให้ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมระบบและใช้เป็นช่องทางในการบุกรุกเครือข่ายภายในขององค์กรได้

ทั้งนี้ Sonic wall ออกแจ้งเตือนให้องค์กรหรือผู้ดูแลระบบ ซึ่งใช้งาน SonicWall SMA1000 ดังกล่าว ควรพิจารณาดำเนินการอัปเกรดเฟิร์มแวร์เป็นเวอร์ชัน 12.4.3-02854 (platform-hotfix) หรือสูงกว่าโดยทันที รวมถึงดำเนินการตามคำแนะนำตามข้อมูลอ้างอิง นอกจากนี้ ควรทำการตรวจสอบประวัติการเข้าถึงระบบย้อนหลัง เพื่อหาร่องรอยการถูกโจมตี และพิจารณาจำกัดการเข้าถึงระบบบริหารจัดการจากระบบเครือข่ายที่เชื่อถือได้เท่านั้น

ด้วยปัญหาฝุ่น PM2.5 ในช่วงนี้ ผู้ประกอบธุรกิจบางแห่งอาจมีการอนุญาตให้พนักงานขององค์กรทำงานจากที่บ้าน (Work From Home) หรือ Remote Working จากระยะไกล สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสมเพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท


**ข้อมูลอ้างอิง**

1. https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-sma1000-rce-flaw-exploited-in-zero-day-attacks/
2. https://www.helpnetsecurity.com/2025/01/23/sonicwall-sma-1000-exploited-zero-day-cve-2025-23006/
3. https://www.sonicwall.com/support/knowledge-base/sma-1000-best-practices-securing-the-network-configuration-on-sma-cms/250121134535667