แจ้งเตือน : ช่องโหว่

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

CISA เตือนช่องโหว่ระดับร้ายแรงในผลิตภัณฑ์ WatchGuard Firewall (CVE-2025-9242)

วันที่แจ้งเตือน 14 พฤศจิกายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cybersecurity and Infrastructure Security Agency (CISA) ของสหรัฐอเมริกาได้ออกคำเตือนเกี่ยวกับช่องโหว่ระดับร้ายแรง (CVE-2025-9242) ในผลิตภัณฑ์ไฟร์วอลล์ WatchGuard Firebox ซึ่งถูกนำไปใช้จริงและหน่วยงานควรให้ความสำคัญแก้ไขช่องโหว่

ผู้ไม่ประสงค์ดีใช้ช่องโหว่เพื่อรันโค้ดอันตรายจากระยะไกล (Remote Code Execution) โดยไม่ต้องพิสูจน์ตัวตน (Unauthenticated attacker) ทำให้สามารถเข้าควบคุม WatchGuard Firebox ที่ใช้ระบบปฏิบัติการ Fireware OS ซึ่งมีช่องโหว่ได้แก่ เวอร์ชั่น 11.10.2 ถึง 11.12.4_Update1, เวอร์ชัน 12.0 ถึง 12.11.3, รวมถึง 2025.1

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้อุปกรณ์ไฟร์วอลล์ WatchGuard Firebox ที่มีช่องโหว่ดังกล่าว พิจารณาแก้ไขตามที่เจ้าของผลิตภัณฑ์แนะนำ ได้แก่ ติดตั้งแพตช์เวอร์ชันล่าสุด 2025.1.1, 12.11.4, 12.5.13 และ 12.3.1_Update3 (B722811) พร้อมทั้งทบทวนสถานะการสนับสนุน (End of Support) ของอุปกรณ์ หากพบว่าเป็นรุ่นที่หมดอายุการสนับสนุนแล้ว ควรประเมินตามกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเพื่อให้อยู่ในระดับที่ยอมรับได้และตรวจสอบ ทบทวนหรือปรับปรุงการตั้งค่าอุปกรณ์ให้มีความมั่นคงปลอดภัยอยู่เสมอ เพื่อลดโอกาสและผลกระทบจากความเสี่ยงที่ผู้ไม่ประสงค์ดีอาจใช้ช่องโหว่ดังกล่าวได้

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/cisa-warns-of-watchguard-firewall-flaw-exploited-in-attacks/
2. https://nvd.nist.gov/vuln/detail/CVE-2025-9242
3. https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015