แจ้งเตือน : ช่องโหว่

Alert

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ระดับร้ายแรงในผลิตภัณฑ์ WatchGuard Firewall (CVE-2025-14733)

วันที่แจ้งเตือน 24 ธันวาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท WatchGuard Technology แจ้งเตือนช่องโหว่ระดับร้ายแรง (CVE-2025-14733) ในผลิตภัณฑ์ไฟร์วอลล์ WatchGuard Firebox ซึ่งผู้ไม่ประสงค์ดีได้นำไปใช้จริง

ช่องโหว่นี้เป็นประเภท Out-of-Bounds Write ที่ผู้ไม่ประสงค์ดีใช้เพื่อรันโค้ดอันตรายจากระยะไกล (Remote Code Execution) โดยไม่ต้องพิสูจน์ตัวตน (Unauthenticated attacker) ทำให้สามารถเข้าควบคุม WatchGuard Firebox ที่ใช้ระบบปฏิบัติการ Fireware OS ซึ่งมีช่องโหว่ดังกล่าว

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

เวอร์ชันที่กระทบ	เวอร์ชันที่แก้ไข
2025.1	2025.1.4
12.X	12.11.6
12.5.X (รุ่น T15 และ T35)	12.5.15
12.3.1 (Release FIPS-certified)	12.3.1_update4 (B728352)
11.XX	End of Life

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2025/12/watchguard-warns-of-active-exploitation.html
2. https://nvd.nist.gov/vuln/detail/CVE-2025-14733
3. https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027