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 ช่องโหว่ Zero Day ระดับร้ายแรง บนอุปกรณ์ Palo Alto Networks Firewall

วันที่แจ้งเตือน 25 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ด้วยพบการรายงานของผู้ผลิต กรณีพบช่องโหว่ที่สามารถ bypass การยืนยันตัวตนในระบบจัดการ Web interface ของระบบปฏิบัติการของอุปกรณ์ Palo Alto Networks Firewall (PAN-OS management web interface) และช่องโหว่ที่สามารถยกระดับสิทธิเป็น root ซึ่งผู้ไม่หวังดีใช้ช่องโหว่ดังกล่าวโจมตีองค์กรมากกว่า 2,000 แห่ง รวมถึงประเทศไทย (CVE-2024-0012 และ CVE-2024-9474) ระบบปฏิบัติการ PAN-OS ที่ได้รับผลกระทบ ได้แก่

- PAN-OS 10.2 ก่อนเวอร์ชัน 10.2.12-h2
- PAN-OS 11.0 ก่อนเวอร์ชัน 11.0.6-h1
- PAN-OS 11.1 ก่อนเวอร์ชัน 11.1.5-h1
- PAN-OS 11.2 ก่อนเวอร์ชัน 11.2.4-h1

ผู้ผลิตแนะนำให้ อัปเดตระบบปฏิบัติการเป็นเวอร์ชัน PAN-OS 10.2.12-h2, PAN-OS 11.0.6-h1, PAN-OS 11.1.5-h1, PAN-OS 11.2.4-h1 และเวอร์ชันล่าสุด

องค์กรควรพิจารณาดำเนินการตามคำแนะนำของผู้ผลิต และยกระดับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงและผลกระทบต่อองค์กรและผู้ใช้บริการ จากเหตุภัยคุกคามทางไซเบอร์โดยจัดให้มีการป้องกันด้วยการจำกัดการเข้าถึงระบบเฉพาะเครือข่ายที่เชื่อถือได้ ปรับปรุงซอฟต์แวร์ให้ทันสมัย และตรวจสอบการใช้งานสม่ำเสมอ เฝ้าระวังและติดตามประกาศด้านความมั่งคงปลอดภัยและตรวจจับภัยคุกคามอยู่เสมอ พร้อมทั้งเตรียมแผนรับมือเหตุฉุกเฉินและระบบสำรองที่มีประสิทธิภาพ

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

ข้อมูลอ้างอิง

1) https://www.bleepingcomputer.com/news/security/over-2-000-palo-alto-firewalls-hacked-using-recently-patched-bugs/
2) https://security.paloaltonetworks.com/CVE-2024-0012
3) https://security.paloaltonetworks.com/CVE-2024-9474