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 5 รายการในโซลูชัน Expedition ของ Palo Alto Networks (CVE-2024-9463, CVE-2024-9464, CVE-2024-9465, CVE-2024-9466 และ CVE-2024-9467)

วันที่แจ้งเตือน 18 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่รายงานช่องโหว่จำนวน 5 รายการ ในโซลูชัน Expedition ของ Palo Alto Networks (CVE-2024-9463, CVE-2024-9464, CVE-2024-9465, CVE-2024-9466 และ CVE-2024-9467) ซึ่งมีผลกระทบระดับร้ายแรง โดยโซลูชัน Expedition ของ Palo Alto Networks ใช้สำหรับช่วยในการย้ายค่า configuration จากผู้จำหน่ายอื่น ๆ ที่รองรับ (เช่น Checkpoint หรือ Cisco เป็นต้น) โดยช่องโหว่ดังกล่าวทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่มีความสำคัญในฐานข้อมูลของ Expedition รวมถึงสามารถอ่านและเขียนไฟล์ในระบบ Expedition ได้ และเข้าควบคุมบัญชีของผู้ดูแลระบบได้

ซอฟต์แวร์เวอร์ชันที่ได้รับผลกระทบได้แก่ Palo Alto Networks Expedition versions 1.2.96 และเวอร์ชันก่อนหน้า

ช่องโหว่	คำอธิบาย
CVE-2024-9463	ช่องโหว่ OS Command Injection ทำให้ผู้ไม่หวังดีสามารถส่งคำสั่งด้วยสิทธิระดับ root บน Expedition ส่งผลให้ข้อมูลต่าง ๆ ถูกเปิดเผย เช่น ชื่อผู้ใช้, รหัสผ่าน, การกำหนดค่าอุปกรณ์ และ API keys ของอุปกรณ์ไฟร์วอลล์ PAN-OS
CVE-2024-9464	
CVE-2024-9465	ช่องโหว่ SQL injection ทำให้ผู้ไม่หวังดีสามารถเปิดเผยเนื้อหาในฐานข้อมูล Expedition เช่น Password Hashes, ชื่อผู้ใช้, การกำหนดค่าอุปกรณ์ และ API keys และสามารถสร้างและอ่านไฟล์ใด ๆ บนระบบ Expedition ได้
CVE-2024-9466	ช่องโหว่ Cleartext storage of sensitive information ทำให้ผู้โจมตีที่ได้รับการยืนยันตัวตนสามารถเปิดเผย Usernames Password และ API keys ที่สร้างขึ้นได้
CVE-2024-9467	ช่องโหว่ Reflected XSS ทำให้ผู้โจมตีสามารถส่ง Link ที่เป็นอันตรายให้แก่ผู้ใช้งานระบบ Expedition และขโมย Session ของผู้ใช้งานระบบ Expedition ได้

Palo Alto แนะนำให้ผู้ใช้งานและผู้ดูแลระบบที่ใช้งานโซลูชัน Expedition ดำเนินการ

1. อัปเดตเป็นเวอร์ชันล่าสุดทันที
2. พิจารณาดำเนินการปิดกั้นการเข้าถึงอินเทอร์เฟซการจัดการ PAN-OS ของไฟร์วอลล์จากอินเทอร์เน็ต และ
3. อนุญาตการเชื่อมต่อจาก IP address ภายในที่เชื่อถือได้เท่านั้น

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 15 พ.ย. 2567
2) https://security.paloaltonetworks.com/PAN-SA-2024-0010
3) https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431