เอกสารการแจ้งเตือนกรณี Palo Alto Networks ออกอัปเดตเพื่อแก้ไขช่องโหว่หลายรายการที่ส่งผลกระทบต่อผลิตภัณฑ์ Palo Alto Networks Expedition

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีช่องโหว่หลายรายการใน Palo Alto Networks มี 5 รายการ ดังนี้

- ช่องโหว่หมายเลข CVE-2024-9463 เป็นช่องโหว่ OS Command Injection หากถูกโจมตีได้สำเร็จอาจทำให้ผู้โจมตีสามารถเรียกใช้คำสั่ง OS โดยสิทธิ์ระดับ root บน Expedition ซึ่งส่งผลให้ข้อมูลต่าง ๆ ถูกเปิดเผย เช่น Usernames, Cleartext Passwords, Device Configurations และ Device API keys ของ PAN-OS firewall ซึ่งช่องโหว่นี้มีความเป็นไปได้สูงที่จะถูกนำมาใช้โจมตี[1]

- ช่องโหว่หมายเลข CVE-2024-9464 เป็นช่องโหว่ OS Command Injection โดยสิทธิ์ระดับ root บน Expedition ซึ่งส่งผลให้ข้อมูลต่าง ๆ ถูกเปิดเผย เช่น Usernames, Cleartext Passwords, Device Configurations และ Device API keys บน PAN-OS firewall [2]

- ช่องโหว่หมายเลข CVE-2024-9465 เป็นช่องโหว่ SQL injection ที่หากถูกโจมตีได้สำเร็จอาจทำให้ผู้โจมตีที่ไม่ได้รับการยืนยันตัวตนสามารถเปิดเผยเนื้อหาฐานข้อมูล Expedition เช่น Password Hashes, Usernames, Device Configurations, and Device API keys ด้วยวิธีนี้ ผู้โจมตียังสามารถสร้างและอ่านไฟล์ใด ๆ บนระบบ Expedition ได้[3]

- ช่องโหว่หมายเลข CVE-2024-9466 เป็นช่องโหว่การจัดเก็บข้อมูลที่ละเอียดอ่อนแบบข้อความธรรมดาสำเร็จ ทำให้ผู้โจมตีที่ได้รับการยืนยันตัวตนสามารถเปิดเผย Usernames Password และ API keys ที่สร้างขึ้นโดยใช้ข้อมูลเหล่านี้ได้[4]

- ช่องโหว่หมายเลข CVE-2024-9467 เป็นช่องโหว่ XSS ที่หากถูกโจมตีได้สำเร็จอาจทำให้ผู้โจมตีสามารถรันสคริปต์ JavaScript ที่เป็นอันตรายได้ในบริบทของเบราว์เซอร์ของผู้ใช้ Expedition ที่ได้รับการยืนยันตัวตนหากผู้ใช้นั้นคลิกบนลิงก์ที่เป็นอันตราย ซึ่งอาจนำไปสู่การขโมยเซสชันของ Expedition ได้ผ่านการโจมตีแบบฟิชชิ่ง[5]

ช่องโหว่เหล่านี้ส่งผลกระทบต่อผลิตภัณฑ์ดังต่อไปนี้:

- Palo Alto Networks Expedition versions 1.2.96 and earlier

วิธีแก้ไขปัญหาทาง Palo Alto Networks ได้แนะนำให้ผู้ใช้และผู้ดูแลระบบบล็อกการเข้าถึงอินเทอร์เฟซการจัดการ PAN-OS ของไฟร์วอลล์จากอินเทอร์เน็ต และอนุญาตเฉพาะการเชื่อมต่อจากที่อยู่ IP ภายในที่เชื่อถือได้เท่านั้น[6]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบ กิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2024-9463
2. https://nvd.nist.gov/vuln/detail/cve-2024-9464
3. https://nvd.nist.gov/vuln/detail/cve-2024-9465
4. https://nvd.nist.gov/vuln/detail/cve-2024-9466
5. https://nvd.nist.gov/vuln/detail/cve-2024-9467
6. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-137