เอกสารการแจ้งเตือนกรณี Palo Alto Networks ออกอัปเดตเพื่อแก้ไขช่องโหว่ Zero day จำนวน 2 รายการ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี Palo Alto Networks ออกอัปเดตเพื่อแก้ไขช่องโหว่ Zero day จำนวน 2 รายการ ที่หมายเลขช่องโหว่ CVE-2024-0012 และ CVE-2024-9474 ที่ส่งผลกระทบต่อ Palo Alto Networks PAN-OS โดยมีรายละเอียดของช่องโหว่ดังต่อไปนี้

- CVE-2024-0012: เป็นช่องโหว่ใน Palo Alto Networks PAN-OS ที่ทำให้ผู้โจมตีที่เข้าถึง Management Web Interface สามารถ Authentication bypass และทำให้ได้สิทธิ์ผู้ดูแลระบบได้โดยไม่ได้รับอนุญาต และผู้โจมตีสามารถปรับเปลี่ยนการตั้งค่าระบบ หรือใช้ช่องโหว่อื่น เช่น CVE-2024-9474 เพื่อโจมตีเพิ่มเติม ช่องโหว่นี้มีผลกระทบต่อ PAN-OS เวอร์ชัน 10.2, 11.0, 11.1 และ 11.2 แต่ไม่ส่งผลต่อ Cloud NGFW หรือ Prisma Access

- CVE-2024-9474: เป็นช่องโหว่ privilege escalation ใน Palo Alto Networks ที่อนุญาตให้ผู้ดูแลระบบ PAN-OS เข้าถึง Management Web Interface ซึ่งสามารถดำเนินการด้วยสิทธิ์ root บนไฟร์วอลล์ได้

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้ และผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบอัปเดตเป็นเวอร์ชันล่าสุดทันที 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://securityaffairs.com/171168/security/u-s-cisa-progress-kemp-loadmaster-palo-alto-networks-pan-os-and-expedition-bugs-known-exploited-vulnerabilities-catalog.html
2. https://www.bleepingcomputer.com/news/security/palo-alto-networks-patches-two-firewall-zero-days-used-in-attacks/