

ประจำวันพุธที่ 24 สิงหาคม 2565

CISA เตือนถึงการใช้ประโยชน์จากช่องโหว่ PAN-OS ของ Palo Alto Networks

Cybersecurity and Infrastructure Security Agency (CISA) ได้เพิ่มข้อบกพร่องด้านความปลอดภัยที่ส่งผลกระทบต่อ PAN-OS ของ Palo Alto Networks ใน Known Exploited Vulnerabilities Catalog เมื่อวันที่จันทร์ที่ผ่านมา โดยช่องโหว่นี้มีความรุนแรงสูง โดยหมายเลข CVE-2022-0028 (คะแนน CVSS : 8.6) เป็นการกำหนดค่านโยบายการกรอง URL ที่ไม่ถูกต้อง ซึ่งอาจเปิดโอกาสให้ผู้โจมตีระยะไกลที่ไม่ผ่านการตรวจสอบสิทธิ์ทำการโจมตี TCP denial-of-service (DoS)

Palo Alto Networks กล่าวในการแจ้งเตือนว่า “หากถูก exploit ปัญหานี้จะไม่ส่งผลกระทบต่อการรักษาความปลอดภัย ความสมบูรณ์ หรือความพร้อมของผลิตภัณฑ์ของเรา” อย่างไรก็ตาม ผลของการการโจมตีแบบปฏิเสธการให้บริการ (DoS) อาจทำให้การระบุตัวตนของผู้โจมตีมีความคลุมเครือและโยงว่าการโจมตีมาจากไฟร์วอลล์ โดยช่องโหว่ส่งผลกระทบต่อรุ่นผลิตภัณฑ์ต่อไปนี้และได้รับการแก้ไขแล้ว โดยเป็นส่วนหนึ่งของการอัปเดตที่ออกมาในเดือนนี้ ได้แก่

- PAN-OS 10.2 (เวอร์ชัน <10.2.2-h2)
- PAN-OS 10.1 (เวอร์ชัน <10.1.6-h6)
- PAN-OS 10.0 (เวอร์ชัน <10.0.11-h1)
- PAN-OS 9.1 (เวอร์ชัน < 9.1.14-h4)
- PAN-OS 9.0 (เวอร์ชัน < 9.0.16-h3) และ
- PAN-OS 8.1 (เวอร์ชัน <8.1.23-h1)