TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Palo Alto Networks ออกแจ้งเตือนถึงช่องโหว่ Zero-Day ใน PAN-OS

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับคุกคามทางไซเบอร์ กรณี Palo Alto Networks ออกแจ้งเตือนถึงช่องโหว่ Zero-Day ใน PAN-OS ที่ CVE-2024-3400 ความรุนแรงระดับ Criticalคะแนน CVSS 10.0 เป็นช่องโหว่ command injection ใน GlobalProtect feature ของ PAN-OS software ที่ทำให้ผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถเรียกใช้คำสั่งด้วยสิทธิ์ root บน firewall ได้และโปรแกรมไฟวอลล์ที่มีการกำหนดค่าสำหรับทั้ง GlobalProtect gateway (Network> GlobalProtect > Gateways) และ telemetry อุปกรณ์ (Device > Setup > Telemetry) ถูกเปิดใช้งาน โดยช่องโหว่ดังกล่าวส่งผลกระทบต่อ PAN-OS เวอร์ชันต่อไปนี้[1]

- PAN-OS < 11.1.2-h3
- PAN-OS < 11.0.4-h1
- PAN-OS < 10.2.9-h1

ทาง Palo Alto Networks จะออกแพตช์เพื่อแก้ไขช่องโหว่ดังกล่าวโดยเร็ว สำหรับผู้ใช้งานและผู้ดูแลเวอร์ชันที่ได้รับผลกระทบแนะนำให้อัปเดตเวอร์ชันล่าสุดทันที ในระหว่างนี้แนะนำผู้ใช้งานและผู้ดูแลที่มี Palo Alto Networks' Threat Prevention Subscription ให้เปิดใช้งาน Threat ID 95187 และเพื่อป้องกันการโจมตีจากช่องโหว่ดังกล่าว

สำหรับผู้ใช้งานและผู้ดูแลที่ไม่สามารถเปิดใช้งาน Threat ID 95187 แนะนำให้ปิดการใช้งาน telemetry ชั่วคราวจนกว่าอุปกรณ์ที่ได้รับผลกระทบจะได้รับการอัปเดตเวอร์ชัน PAN-OS การทำ telemetry ควรเปิดใช้งานบนอุปกรณ์หลังจากที่ดำเนินการอัปเดตเสร็จสมบูรณ์ โดยมีขั้นตอนดังต่อไปนี้[2]

- ไปที่ Device > Setup > Telemetry
- แก้ไข Telemetry widget
- เลือกช่องที่ Enable Telemetry
- ยกเลิกการเลือก Enable Telemetry
- คลิก OK และยืนยันการเปลี่ยนแปลง

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานที่ใช้งานผลิตภัณฑ์ควรเฝ้าระวังและตรวจสอบการทำงานของผลิตภัณฑ์ที่ใช้งานภายในหน่วยงานเพื่อตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

อ้างอิง

1. https://security.paloaltonetworks.com/CVE-2024-3400
2. https://thehackernews.com/2024/04/zero-day-alert-critical-palo-alto.html

TLP:CLEAR