เอกสารการแจ้งเตือนช่องโหว่ CVE-2024-29895 ที่ส่งผลกระทบด้านความปลอดภัยของโปรแกรมตรวจสอบเครือข่าย Cacti

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับช่องโหว่ CVE-2024-29895[1] ที่ส่งผลกระทบด้านความปลอดภัยของโปรแกรมตรวจสอบเครือข่าย Cacti

Cacti เป็นเครื่องมือที่ใช้ในการตรวจสอบและจัดการระบบเครือข่าย (Network Monitoring) ซึ่งถูกออกแบบมาเพื่อเก็บข้อมูลเกี่ยวกับการใช้งานในเครือข่ายและแสดงผลข้อมูลในรูปแบบ GUI ที่สามารถวิเคราะห์ได้ง่าย

มีการพบช่องโหว่ Command injection ใน Cacti ที่ CVE-2024-29895 มีคะแนน CVSS: 10 โดยเป็นช่องโหว่ที่สามารถ command injection เพื่อช่วยให้ผู้ใช้งานที่ไม่ได้รับการรับรองความถูกต้องสามารถรันคำสั่งที่กำหนดเองบนเซิร์ฟเวอร์ได้ เมื่อตัวเลือก register_argc_argv ของ PHP เปิดอยู่

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานที่ใช้งาน Cacti ควรดำเนินการอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อป้องกันการถูกโจมตี และตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้นและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://securityonline.info/critical-security-flaws-in-cacti-command-injection-cve-2024-29895-cvss-10-and-xss-vulnerabilities//
2. https://www.csa.gov.sg/alerts-advisories/security-bulletins/2024/sb-2024-020