แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนพบช่องโหว่ที่ส่งผลกระทบด้านความปลอดภัย ของโปรแกรมตรวจสอบเครือข่าย Cacti

วันที่แจ้งเตือน 24 พฤษภาคม 2567

ThaiCERT สกมช. ได้เผยแพร่การพบช่องโหว่ Command injection ใน Cacti (open-source network monitoring software) สำหรับเวอร์ชัน 1.3.X DEV Branch **(CVE-2024-29895 มีคะแนน CVSS: 10 [Critical])** โดยเป็นช่องโหว่ที่ผู้ไม่ประสงค์ดีทำ command injection เพื่อรันคำสั่งที่กำหนดเอง บน Server ของผู้ที่เปิดใช้งาน register_argc_argv ของ PHP ให้มีสถานะเป็น On

Cacti เป็นเครื่องมือที่ถูกออกแบบมาเพื่อเก็บข้อมูลเกี่ยวกับการใช้งานในเครือข่ายและแสดงผลข้อมูลในรูปแบบ GUI ที่สามารถวิเคราะห์ได้ง่าย

ทั้งนี้ ผู้ประกอบธุรกิจที่ใช้งาน Cacti เวอร์ชันดังกล่าว ควรดำเนินการอัปเดตเวอร์ชัน/Patch เพื่อป้องกันความเสี่ยงและความเสียหายที่อาจเกิดขึ้น เช่น การถูก Attacker บุกรุก Server ผ่านช่องโหว่ command injection และรันคำสั่งใด ๆ บน Server ได้ และอาจทำให้ Attacker สามารถเข้าถึงและขโมยข้อมูลสำคัญต่าง ๆ

ผลกระทบจากการถูกโจรกรรมตัวตนของผู้ใช้งาน ผ่านช่องโหว่ดังกล่าว ทำให้ผู้ไม่ประสงค์ดีสามารถขโมย session cookie ของผู้ใช้งานหรือผู้ดูแลระบบ Cacti ได้ และเข้าถึงระบบในนามของ Account นั้นทำให้เกิดความเสียหาย เช่น เปลี่ยนการตั้งค่าเครือข่าย ลบข้อมูล สร้างผู้ใช้ใหม่ และขโมยข้อมูล เป็นต้น ทั้งนี้ ช่องโหว่ดังกล่าวถูกจัดอยู่ในระดับ Critical หากเพิกเฉยหรือไม่ดำเนินการป้องกัน อาจจะสร้างความเสี่ยงด้าน compliance ได้ ดังนั้น ผู้ประกอบธุรกิจจึงควรตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 15 พ.ค. 2567
2) https://securityonline.info/critical-security-flaws-in-cacti-command-injection-cve-2024-29895-cvss-10-and-xss-vulnerabilities//
3) https://www.csa.gov.sg/alerts-advisories/security-bulletins/2024/sb-2024-020
4) https://nvd.nist.gov/vuln/detail/CVE-2024-29895