เอกสารการแจ้งเตือนกรณีช่องโหว่หลายรายการในผลิตภัณฑ์ Common UNIX Printing System (CUPS)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีช่องโหว่ใน Common UNIX Printing System (CUPS) ของระบบปฏิบัติการ UNIX และ LINUX มี 4 รายการ ดังนี้

- ช่องโหว่หมายเลข CVE-2024-47076 มีคะแนน (CVSSv3 : 8.6) ความรุนแรงระดับ High เป็นช่องโหว่ที่เกิดจากการตรวจสอบข้อมูลที่ไม่ถูกต้องใน libcupsfilters ที่ทำให้ผู้โจมตีสามารถส่งข้อมูลที่เป็นอันตรายไปยังระบบ CUPS[1]

- ช่องโหว่หมายเลข CVE-2024-47175 มีคะแนน (CVSSv3 : 8.6) ความรุนแรงระดับ High เป็นช่องโหว่ที่เกิดจากการตรวจสอบข้อมูลที่ไม่ถูกต้องในไลบารี libppd โดยข้อมูล IPP ที่ไม่ผ่านการรับรองความถูกต้องทำให้ผู้โจมตีสามารถแทรกข้อมูลที่เป็นอันตรายในไฟล์ PPD ได้[2]

- ช่องโหว่หมายเลข CVE-2024-47176 มีคะแนน (CVSSv3 : 8.3) ความรุนแรงระดับ High เป็นช่องโหว่ที่เกี่ยวกับบริการ cups-browsed จะเชื่อมต่อกับ INAPPR_ANY ผ่านพอร์ต UPP 631 ทำให้ผู้โจมตีที่ไม่ได้รับการยืนยันตัวตนสามารถส่งแพ็กเก็จพิเศษไปยัง URL ที่ควบคุมได้ และทำให้สามารถ Execute Arbitrary Commands ได้[3]

- ช่องโหว่หมายเลข CVE-2024-47177 มีคะแนน (CVSSv3 : 9.0) ความรุนแรงระดับ Critical เป็นช่องโหว่ Command Injection ในไลบารี Cups-filters ซึ่งทำให้ผู้โจมตีสามารถเข้าถึงและรันโค้ดจากระยะไกลได้ ผ่านพารามิเตอร์ Podomatic RlpcommadLine PPD[4]

ช่องโหว่เหล่านี้ส่งผลกระทบต่อผลิตภัณฑ์ดังต่อไปนี้:

- cups-browsed เวอร์ชัน 2.0.1 และเก่ากว่า
- libcupsfilters เวอร์ชัน 2.1b1 และเก่ากว่า
- libppd เวอร์ชัน 2.1b1 และเก่ากว่า
- cups-filters เวอร์ชัน 2.0.1 และเก่ากว่า

สำหรับวิธีแก้ปัญหาทาง Ubantu, Debian, Red Hat และบริษัทพัฒนาผู้จัดจำหน่ายอื่น ๆ ได้ออกคำแนะนำเกี่ยวกับวิธีการแก้ไขปัญหาเบื้องต้น ซึ่งแนะนำให้ผู้ใช้งานที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบใช้มาตรการที่เกี่ยวข้องเพื่อป้องกันช่องโหว่ดังกล่าวโดยเร็วที่สุด[5]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที 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://nvd.nist.gov/vuln/detail/CVE-2024-47076
2. https://nvd.nist.gov/vuln/detail/CVE-2024-47175
3. https://nvd.nist.gov/vuln/detail/CVE-2024-47176
4. https://nvd.nist.gov/vuln/detail/CVE-2024-47177
5. https://nsfocusglobal.com/remote-code-execution-vulnerability-alert-of-unix-cups-print-service-cve-2024-47076-cve-2024-47175-cve-2024-47177