แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงของซอฟต์แวร์ Common UNIX Printing System (CUPS) ในระบบปฏิบัติการ UNIX และ LINUX 4 รายการ (CVE-2024-47076, CVE-2024-47175, CVE-2024-47176 และ CVE-2024-47177)

วันที่แจ้งเตือน 7 ตุลาคม 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เผยแพร่รายงานช่องโหว่ของซอฟต์แวร์ Common UNIX Printing System (CUPS) ซึ่งเป็นซอฟต์แวร์ Open-source ที่ใช้ในการสั่งพิมพ์งานบนระบบปฏิบัติการ UNIX และ LINUX ส่งผลให้ผู้ไม่หวังดีสามารถเรียกใช้คำสั่งที่เป็นอันตรายจากระยะไกล (Remote Code Execution (RCE)) บนระบบ Linux ได้ โดยมีช่องโหว่ที่เกี่ยวข้องจำนวน 4 รายการ ดังนี้

หมายเลขช่องโหว่	Impact	Affected
CVE-2024-47076 (HIGH)	ช่องโหว่ที่เกิดจาก Invalid Input Validate ที่ไม่ถูกต้องในไลบรารี “libcupsfilters” ทำให้ผู้โจมตีสามารถส่งข้อมูลที่เป็นอันตรายและควบคุม CUPS ได้	libcupsfilters <= 2.1b1
CVE-2024-47175 (HIGH)	ช่องโหว่ที่เกิดจาก Input Verification ที่ไม่ถูกต้องในไลบารี “libppd” โดยข้อมูล Internet Printing Protocol (IPP) ที่ใช้สื่อสารระหว่างเครื่องผู้ใช้งานกับ Printer ที่ไม่ผ่านการรับรองความถูกต้องทำให้ผู้โจมตีสามารถแทรกข้อมูลที่เป็นอันตรายในไฟล์ PostScript Printer Description (PPD) ซึ่งเป็นไฟล์ที่ Printer Driver ใช้สำหรับทำความเข้าใจคุณสมบัติของ Printer แต่ละรุ่นได้	libppd <= 2.1b1
CVE-2024-47176 (HIGH)	ช่องโหว่ที่เกี่ยวกับบริการ cups-browsed ซึ่งทำหน้าที่ในการค้นหาเครื่องพิมพ์บนเครือข่าย, ทั้งนี้ช่องโหว่นี้เกิดจากการผูกพารามิเตอร์ INAPPR_ANYaddress เข้ากับพอร์ต UDP 631 ทำให้บริการดังกล่าวยอมรับการเชื่อมต่อจากแหล่งต้นทางใดๆ (trust from any source) ทำให้ผู้โจมตีที่ไม่ได้รับการยืนยันตัวตนสามารถส่งแพ็กเกจพิเศษไปยัง URL ที่ควบคุมได้ และทำให้สามารถรันคำสั่งที่ไม่เหมาะสม (Arbitrary Commands) ได้	cups-browsed <= 2.0.1
CVE-2024-47177 (CRITICAL)	ช่องโหว่ Command Injection ในไลบารี “cups-filters” ซึ่งทำให้ผู้โจมตีสามารถเข้าถึงและรันโค้ดจากระยะไกลได้ ผ่านพารามิเตอร์ FoomaticRIPCommadLine PPD ได้	cups-filters <= 2.0.1

สำหรับวิธีแก้ปัญหาทาง Ubuntu, Debian, RedHat และ บริษัทอื่น ๆ ได้ออกคำแนะนำเกี่ยวกับวิธีการแก้ไขปัญหาเบื้องต้น ซึ่งแนะนำให้ผู้ใช้งานที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบใช้มาตรการที่เกี่ยวข้องเพื่อป้องกันช่องโหว่ดังกล่าวโดยเร็วที่สุด **(อ้างอิง2)**

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 4 ต.ค. 2567
2) https://nsfocusglobal.com/remote-code-execution-vulnerability-alert-of-unix-cups-print-service-cve-2024-47076-cve-2024-47175-cve-2024-47177/