เอกสารการแจ้งเตือนกรณีช่องโหว่ CVE-2025-1240 ใน WinZip เสี่ยงถูกใช้ในการโจมตี

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีช่องโหว่ CVE-2025-1240 ใน WinZip เสี่ยงถูกใช้ในการโจมตี

ช่องโหว่ความปลอดภัยในซอฟต์แวร์ WinZip ที่หมายเลข CVE-2025-1240 (มีคะแนน CVSS 7.8) เป็นช่องโหว่ที่เปิดโอกาสให้ผู้โจมตี สามารถรันโค้ดที่เป็นอันตรายบนอุปกรณ์ของเหยื่อได้ ซึ่งช่องโหว่นี้เกิดจากการที่ WinZip ประมวลผลไฟล์ 7Z โดยไม่มีการตรวจสอบข้อมูล ทำให้เกิดการเขียนข้อมูลเกินขอบเขตของบัฟเฟอร์ (Buffer Overflow) ผู้โจมตีสามารถใช้ช่องโหว่นี้โดยหลอกให้เหยื่อเปิดไฟล์ 7Z ที่ถูกสร้างขึ้นมาเป็นพิเศษ หรือเข้าไปยังเว็บไซต์ที่มีเนื้อหาประสงค์ร้าย ซึ่งอาจนำไปสู่การควบคุมระบบและการขโมยข้อมูล WinZip ได้ออกอัปเดตเวอร์ชัน 29.0 เพื่อแก้ไขปัญหาดังกล่าว ผู้ใช้ควรอัปเดตซอฟต์แวร์โดยเร็วและหลีกเลี่ยงการเปิดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ[1]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://vulnera.com/newswire/critical-remote-code-execution-vulnerability-identified-in-winzip-cve-2025-1240/