เอกสารการแจ้งเตือนกรณีช่องโหว่ในปลั๊กอิน GiveWP ของ WordPress

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-8353 มีคะแนน (CVSSv3 : 10.0) ในปลั๊กอิน GiveWP ใช้บนเว็บไซต์ WordPress สำหรับระบบบริจาคและระดมทุนออนไลน์ ช่องโหว่นี้เกิดจากการจัดการข้อมูลที่ไม่ปลอดภัยในกระบวนการแปลงข้อมูล (deserialization) โดยเฉพาะพารามิเตอร์อย่าง give_title และ card_address ทำให้ผู้โจมตีที่ไม่ได้รับการยืนยันตัวตนสามารถใช้ประโยชน์จากช่องโหว่ PHP Object Injection เพื่อรันโค้ดระยะไกล (Remote Code Execution - RCE) [1]

ช่องโหว่ส่งผลกระทบต่อ GiveWP ทุกเวอร์ชันก่อน 3.16.2 โดยเฉพาะเวอร์ชัน 3.16.1 ที่มีการแก้ไขบางส่วน ทำให้ต้องอัปเดตเป็นเวอร์ชัน 3.16.2 เพื่อแก้ไขปัญหานี้ [2]

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-2024-8353
2. https://vulmon.com/vulnerabilitydetails?qid=CVE-2024-8353