เอกสารการแจ้งเตือนกรณีพบช่องโหว่ในปลั๊กอิน Really Simple Security WordPress

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-10924 มีคะแนน CVSSv3 9.8 ในปลั๊กอิน Really Simple Security ที่ใช้งานบนเว็บไซต์ WordPress โดยช่องโหว่ดังกล่าวเกิดจากข้อผิดพลาดในการจัดการระบบ Two-Factor Authentication (2FA) ผ่าน REST API ของปลั๊กอิน ทำให้ผู้ไม่หวังดีสามารถหลีกเลี่ยงการยืนยันตัวตนและเข้าถึงบัญชีผู้ใช้ ซึ่งรวมถึงบัญชีผู้ดูแลระบบได้สำเร็จ[1]

ช่องโหว่ส่งผลกระทบต่อปลั๊กอิน Really Simple Security ในเวอร์ชัน 9.0.0 ถึง 9.1.1.1 และได้ออกอัปเดตเป็นเวอร์ชัน 9.1.2 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-2024-10924
2. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-140