TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Adobe ออกอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ระดับ Critical ในผลิตภัณฑ์ Adobe Commerce

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-34102 มีคะแนน (CVSSv3.1 : 9.8) ในผลิตภัณฑ์ Adobe Commerce โดยช่องโหว่นี้ได้ถูกนำไปใช้โจมตีแล้วในขณะนี้ ช่องโหว่ดังกล่าวเกิดจากการอ้างอิง XML external entity ที่ไม่ปลอดภัย อาจจะทำให้ผู้โจมตีสามารถเข้าควบคุมระบบเพื่อรันโค้ดอันตรายได้ด้วยการส่ง XML ที่มีการอ้างอิงไปยัง entity ภายนอก

ช่องโหว่ดังกล่าวส่งผลกระทบต่อเวอร์ชันของผลิตภัณฑ์ดังต่อไปนี้ :

- Adobe Commerce version 2.4.7 และก่อนหน้า
- Adobe Commerce version 2.4.6-p5 และก่อนหน้า
- Adobe Commerce version 2.4.5-p7 และก่อนหน้า
- Adobe Commerce version 2.4.4-p8 และก่อนหน้า
- Adobe Commerce version 2.4.3-ext-7 และก่อนหน้า
- Adobe Commerce version 2.4.2-ext-7 และก่อนหน้า
- Magento Open Source version 2.4.7 และก่อนหน้า
- Magento Open Source version 2.4.6-p5 และก่อนหน้า
- Magento Open Source version 2.4.5-p7 และก่อนหน้า
- Magento Open Source version 2.4.4-p8 และก่อนหน้า
- Adobe Commerce Webhooks Plugin version 1.2.0 - 1.4.0

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้ และผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบอัปเดตเป็นเวอร์ชันล่าสุดทันที 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://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-113
2. https://helpx.adobe.com/security/products/acrobat/apsb24-70.html

TLP:CLEAR