TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Adobe ออกอัปเดตแก้ไขช่องโหว่ระดับ Critical ใน Acrobat Reader

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี Adobe ออกอัปเดตแก้ไขช่องโหว่ระดับ Critical ใน Adobe Acrobat Reader ที่ช่องโหว่ CVE-2024-41869 คะแนน CVSS 9.8[1] โดย Adobe ได้เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่ส่งผลกระทบต่อ Adobe Acrobat Reader ซึ่งช่องโหว่ดังกล่าวเป็นช่องโหว่"user interface"ที่สามารถถูก Remote Code Execution เมื่อเปิดเอกสาร PDF ที่ถูกออกแบบมาเป็นพิเศษ [2] โดยส่งผลกระทบต่อผลิตภัณฑ์เวอร์ชัน ดังนี้

- Acrobat Reader DC Continuous 24.003.20054 และเวอร์ชันก่อนหน้า (Windows)
- Acrobat Reader DC Continuous, 24.002.21005 และเวอร์ชันก่อนหน้า (MacOS)
- Acrobat Reader 2020 Classic 2020, 20.005.30655 และเวอร์ชันก่อนหน้า (Windows และ MacOS)

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานและผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบอัปเดตเป็นเวอร์ชันล่าสุดทันที 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