วันที่ 15 เมษายน 2569

Adobe ออกแพตช์ฉุกเฉินแก้ช่องโหว่ Acrobat Reader ที่ถูกโจมตีจริง CVE-2026-34621

Adobe เพิ่งปล่อยอัปเดตด้านความปลอดภัยแบบฉุกเฉิน หลังพบว่าช่องโหว่ร้ายแรงใน Acrobat Reader กำลังถูกแฮกเกอร์นำไปใช้โจมตีผู้ใช้งานจริงอยู่ในขณะนี้

ช่องโหว่นี้อันตรายแค่ไหน

ช่องโหว่ที่ถูกค้นพบมีรหัสว่า CVE-2026-34621 และได้รับคะแนนความรุนแรง 8.6 จาก 10 ตามมาตรฐาน CVSS โดยหากถูกโจมตีสำเร็จ ผู้ไม่หวังดีอาจสามารถรันโค้ดอันตรายบนเครื่องของผู้ใช้ได้ ปัญหานี้ถูกอธิบายว่าเป็นช่องโหว่ประเภท prototype pollution ซึ่งเป็นช่องโหว่ใน JavaScript ที่เปิดโอกาสให้ผู้โจมตีสามารถแก้ไขโครงสร้างของวัตถุและค่าภายในโปรแกรมได้

ซอฟต์แวร์รุ่นไหนได้รับผลกระทบบ้าง

ช่องโหว่นี้ส่งผลกระทบต่อผลิตภัณฑ์และเวอร์ชันต่อไปนี้ ทั้งบน Windows และ macOS

- Acrobat DC เวอร์ชัน 26.001.21367 และก่อนหน้า (แก้ไขแล้วในเวอร์ชัน 26.001.21411)
- Acrobat Reader DC เวอร์ชัน 26.001.21367 และก่อนหน้า (แก้ไขแล้วในเวอร์ชัน 26.001.21411)
- Acrobat 2024 เวอร์ชัน 24.001.30356 และก่อนหน้า (แก้ไขแล้วในเวอร์ชัน 24.001.30362 สำหรับ Windows และ 24.001.30360 สำหรับ macOS)

ถูกโจมตีมาตั้งแต่เมื่อไหร่

Adobe ยืนยันอย่างเป็นทางการแล้วว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริงในโลกออนไลน์ และมีหลักฐานชี้ว่าการโจมตีอาจเริ่มต้นมาตั้งแต่ เดือนธันวาคม 2025 แล้ว ผู้ที่เป็นคนแรกที่เปิดเผยรายละเอียดของช่องโหว่นี้คือ Haifei Li นักวิจัยด้านความปลอดภัยและผู้ก่อตั้งบริษัท EXPMON โดยเขาพบว่าเพียงแค่เปิดไฟล์ PDF ที่ถูกดักแปลง ก็สามารถทำให้ JavaScript อันตรายทำงานได้ทันที

นอกจากนี้ Adobe ยังยืนยันด้วยว่าผลกระทบของช่องโหว่นี้ร้ายแรงกว่าที่คาด ไม่ใช่แค่ทำให้ข้อมูลรั่วไหล แต่สามารถนำไปสู่การ ควบคุมเครื่องของเหยื่อได้เลย ซึ่งสอดคล้องกับผลการวิเคราะห์จากนักวิจัยด้านความปลอดภัยหลายรายในช่วงไม่กี่วันที่ผ่านมา ตามที่ EXPMON ระบุผ่านโพสต์บน X

ข้อมูลอ้างอิง

Apr 12, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/adobe-patches-actively-exploited.html