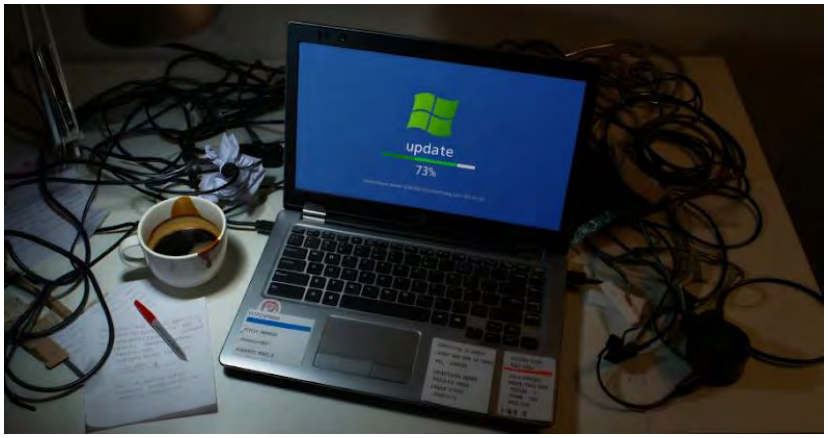
วันที่ 4 ธันวาคม 2568

ไมโครซอฟท์อุดช่องโหว่ไฟล์ลัด Windows แบบเงียบๆ หลังถูกใช้โจมตีต่อเนื่องมาหลายปี



ไมโครซอฟท์ได้ทำการแก้ไขช่องโหว่ความปลอดภัยที่ถูกผู้โจมตีใช้ประโยชน์มานานกว่า 8 ปีอย่างเงียบ ๆ ในการอัปเดต Patch Tuesday เดือนพฤศจิกายน 2025 ที่ผ่านมา โดยช่องโหว่นี้มีรหัสว่า CVE-2025-9491 (คะแนนความรุนแรง 7.8/7.0)

ช่องโหว่นี้ถูกจัดเป็นปัญหาการตีความข้อมูลผิดพลาดในหน้าต่างแสดงผลของไฟล์ลัด Windows (ไฟล์ .LNK) ซึ่งอาจนำไปสู่การรันโค้ดจากระยะไกล (Remote Code Execution) ในสิทธิ์ของผู้ใช้ปัจจุบันได้

กลไกทางเทคนิค: การซ่อนคำสั่งอันตรายด้วยความยาวไฟล์

ช่องโหว่นี้ไม่ได้เกิดจากความผิดพลาดในการจัดการโค้ด แต่เกิดจากความไม่สมบูรณ์ของการแสดงผล:

- ปัญหาคืออะไร: ข้อบกพร่องเกิดขึ้นในกระบวนการจัดการไฟล์ .LNK โดยเฉพาะในช่อง Target ที่ใช้เก็บคำสั่งที่ไฟล์ลัดจะรัน
- ความยาวที่ซ่อน: ไฟล์ลัดถูกสร้างขึ้นให้ซ่อนคำสั่งอันตรายเวลาเปิดดูใน Properties โดยใช้ตัวอักษร “ช่องว่าง” หลายแบบเพื่อหลอกให้คิดว่าปลอดภัย โครงสร้างไฟล์สามารถรองรับความยาวได้ถึงประมาณ 32,000 ตัวอักษร แต่หน้าต่าง Properties ที่ Windows แสดงผลจะแสดงเพียงแค่ 260 ตัวอักษรแรกเท่านั้น
- วิธีการโจมตี: ผู้โจมตีมักปลอมไฟล์ให้ดูเหมือนเอกสารทั่วไปเพื่อหลอกให้กดเปิด เมื่อผู้ใช้เห็นเพียงช่วงต้นของคำสั่งที่ไม่เป็นอันตราย ส่วนที่เหลือของโค้ดก็จะถูกรันโดยที่ผู้ใช้ไม่รู้ตัว

ช่องโหว่ที่ถูกใช้โดยรัฐบาลมานานกว่า 8 ปี

รายละเอียดของช่องโหว่นี้ถูกเปิดเผยครั้งแรกโดย Trend Micro ZDI ในเดือนมีนาคม 2025 (รหัสติดตาม ZDI-CAN-25373) โดยพบข้อมูลที่น่าตกใจ:

- 11 กลุ่มแฮ็กเกอร์: ช่องโหว่นี้ถูกกลุ่มที่รัฐสนับสนุนจาก จีน, อิหร่าน, เกาหลีเหนือ และรัสเซีย รวม 11 กลุ่ม นำไปใช้ปฏิบัติการจารกรรม ขโมยข้อมูล และโจมตีเพื่อหวังผลทางการเงิน
- โจมตีตั้งแต่ปี 2017: พบหลักฐานว่าช่องโหว่นี้ถูกใช้โจมตีในโลกจริงมาตั้งแต่ ปี 2017 แล้ว

การโจมตีจริงที่เกิดขึ้นหลังการเปิดเผย

แม้ไมโครซอฟท์จะทราบปัญหา แต่ก็เคยให้เหตุผลว่าช่องโหว่นี้ยังไม่ถึงระดับที่ต้องแก้ไขทันที และชี้ว่าไฟล์ .LNK ถูกบล็อกในแอปพลิเคชัน Office อยู่แล้ว (Outlook, Word, Excel, PowerPoint, OneNote) อย่างไรก็ตาม การโจมตีก็ยังคงเกิดขึ้น:

1. XDSpy: กลุ่มจารกรรมไซเบอร์ชื่อ XDSpy ได้ใช้ช่องโหว่นี้ในการโจมตีหน่วยงานรัฐบาลในยุโรปตะวันออก เพื่อกระจายมัลแวร์ชื่อ XDigo ที่เขียนด้วยภาษา Go ซึ่งเกิดขึ้นในเดือนเดียวกับที่มีการเปิดเผยช่องโหว่นี้สู่สาธารณะ
2. PlugX: ในปลายเดือนตุลาคม 2025 ช่องโหว่นี้ก็ถูกนำกลับมาใช้เป็นครั้งที่สาม เมื่อ Arctic Wolf ตรวจพบการโจมตีที่กลุ่มผู้ไม่หวังดีที่เชื่อมโยงกับ จีน ใช้ช่องโหว่นี้เล่นงานหน่วยงานรัฐบาลและการทูตในยุโรป พร้อมแพร่กระจายมัลแวร์ PlugX

การแก้ไขที่มาแบบเงียบ ๆ (Patch Tuesday)

หลังจากที่ไมโครซอฟท์เคยออกคำแนะนำอย่างเป็นทางการเกี่ยวกับ CVE-2025-9491 แต่ยืนยันว่าตัดสินใจไม่แพตช์ช่องโหว่นี้ ก็ถูกแก้ไขอย่างเงียบ ๆ ในที่สุดใน Patch Tuesday เดือนพฤศจิกายน 2025:

- วิธีการแก้ไขของ Microsoft: แพตช์นี้แก้ไขปัญหาโดยให้หน้าต่าง Properties แสดงคำสั่งทั้งหมดในช่อง Target ไม่ว่าจะยาวเท่าใดก็ตาม ซึ่งทำให้คำสั่งอันตรายที่ถูกซ่อนไว้ทั้งหมดถูกเปิดเผยออกมา อย่างไรก็ตามวิธีนี้จะทำงานได้ต่อเมื่อมีไฟล์ลัดที่มีคำสั่งยาวเกิน 260 ตัวอักษรอยู่จริง

ทางเลือกอื่นจาก 0patch

ในขณะที่รอการแก้ไขจากไมโครซอฟท์ ทางบริษัท 0patch ได้ออกไมโครแพตช์เพื่อแก้ปัญหาแตกต่างไป:

- วิธีการแก้ไขของ 0patch: แพตช์ของ 0patch จะแสดงคำเตือน เมื่อผู้ใช้พยายามเปิดไฟล์ลัดที่มีความยาวเกิน 260 ตัวอักษร โดยมองว่าการทำให้การโจมตีที่พบจริงใช้งานไม่ได้ จะช่วยป้องกันเหยื่อได้มาก

The Hacker News ระบุว่าได้ติดต่อไมโครซอฟท์เพื่อขอความคิดเห็นเพิ่มเติม และจะอัปเดตข้อมูลหากได้รับการตอบกลับจากบริษัท

ข้อมูลอ้างอิง

Dec 3, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/12/microsoft-silently-patches-windows-lnk.html