วันที่ 13 มีนาคม 2569

Microsoft แก้ไขช่องโหว่ 84 รายการในเดือนมีนาคม รวมถึง Zero-Day ที่ถูกเปิดเผยต่อสาธารณะ 2 รายการ

เมื่อวันอังคารที่ผ่านมา Microsoft ได้ปล่อยอัปเดตความปลอดภัยประจำเดือน เพื่อแก้ไขช่องโหว่รวมทั้งหมด 84 รายการ ที่ส่งผลกระทบต่อซอฟต์แวร์หลายส่วนในระบบ โดยในจำนวนนี้มี 2 ช่องโหว่ที่ถูกเปิดเผยต่อสาธารณะไปก่อนหน้าแล้ว

สรุปภาพรวมของช่องโหว่ในเดือนนี้

จากรายการทั้งหมด พบว่าเป็นช่องโหว่ระดับ Critical (วิกฤต) 8 รายการ และระดับ Important (สำคัญ) 76 รายการ โดยสามารถจำแนกประเภทได้ดังนี้:

- 46 รายการ เป็นช่องโหว่การยกระดับสิทธิ์ (Privilege Escalation)
- 18 รายการ เป็นช่องโหว่ที่อาจนำไปสู่การรันโค้ดจากระยะไกล (Remote Code Execution)
- 10 รายการ เป็นการเปิดเผยข้อมูล (Information Disclosure)
- 4 รายการ เป็นการปลอมแปลงตัวตน (Spoofing)
- 4 รายการ เป็นการโจมตีแบบปฏิเสธการให้บริการ (Denial-of-Service)
- และ 2 รายการ เป็นช่องโหว่ที่ใช้ข้ามกลไกด้านความปลอดภัย (Security Feature Bypass)

นอกจากนี้ การอัปเดตยังครอบคลุมช่องโหว่อีก 10 รายการในเบราว์เซอร์ Microsoft Edge (Chromium) ซึ่งเคยได้รับการแก้ไขไปแล้วตั้งแต่ช่วงกุมภาพันธ์ 2026 ที่ผ่านมา

เจาะลึกช่องโหว่ Zero-Day ที่น่ากังวล

มีการตรวจพบช่องโหว่ที่ถูกเปิดเผยต่อสาธารณะ (Zero-Day) 2 รายการ ซึ่งรายงานผ่านระบบค้นหาช่องโหว่อัตโนมัติด้วย AI ที่ชื่อว่า XBOW

1. CVE-2026-26127 (CVSS 7.5): ช่องโหว่ Denial-of-Service ใน .NET
2. CVE-2026-21262 (CVSS 8.8): ช่องโหว่ยกระดับสิทธิ์ใน Microsoft SQL Server

ทาง Microsoft ยืนยันว่าปัญหาเหล่านี้ได้รับการลดความเสี่ยงเบื้องต้นแล้ว และผู้ใช้ทั่วไปไม่จำเป็นต้องดำเนินการใดๆ เพิ่มเติมนอกเหนือจากการอัปเดตแพตช์

วิเคราะห์ความเสี่ยง: เน้นหนักที่การ "ยกระดับสิทธิ์"

Satnam Narang จาก Tenable ระบุว่า กว่า 55% ของช่องโหว่ในเดือนนี้เป็นการยกระดับสิทธิ์ (Privilege Escalation) ซึ่งมี 6 รายการที่มีโอกาสถูกนำไปใช้โจมตีสูงมาก โดยพบในส่วนประกอบสำคัญของ Windows เช่น Windows Graphics Component, Windows Accessibility Infrastructure, Windows Kernel, Windows SMB Server และ Winlogon

ช่องโหว่เด่นที่ต้องเฝ้าระวัง

- CVE-2026-25187 (CVSS 7.8) ใน Winlogon: ค้นพบโดย James Forshaw จาก Google Project Zero เป็นช่องโหว่ที่ยอมให้ผู้โจมตีที่มีสิทธิ์ระดับต่ำ สามารถยกระดับตัวเองขึ้นเป็น SYSTEM ได้ผ่านการจัดการลิงก์ที่ผิดพลาด โดยไม่ต้องอาศัยการโต้ตอบจากผู้ใช้ (Zero-click) และมีความซับซ้อนในการโจมตีต่ำมาก
- CVE-2026-26118 (CVSS 8.8) ใน Azure MCP Server: เป็นช่องโหว่แบบ Server-Side Request Forgery (SSRF) โดยผู้โจมตีสามารถส่ง URL อันตรายเพื่อหลอกให้ Server ส่ง managed identity token ออกมา ทำให้สามารถขโมยสิทธิ์เข้าถึงทรัพยากรต่างๆ ขององค์กรได้โดยไม่จำเป็นต้องมีสิทธิ์เป็นแอดมิน

ความเสี่ยงใหม่ ข้อมูลรั่วไหลผ่าน AI ใน Excel

ในกลุ่มระดับ Critical ยังพบช่องโหว่ CVE-2026-26144 (CVSS 7.5) ใน Microsoft Excel ซึ่งเป็นช่องโหว่ Cross-Site Scripting (XSS) หากถูกโจมตีสำเร็จ อาจทำให้ Copilot Agent ส่งข้อมูลสำคัญออกจากระบบโดยอัตโนมัติในรูปแบบ zero-click

Alex Vovk ซีอีโอจาก Action1 เตือนว่า ช่องโหว่นี้อันตรายมากสำหรับองค์กร เพราะไฟล์ Excel มักเก็บข้อมูลความลับ เช่น งบการเงินหรือทรัพย์สินทางปัญญา และการทำงานร่วมกับ AI อาจกลายเป็นช่องทางให้ข้อมูลรั่วไหลออกไปโดยไม่ตั้งใจ

ก้าวใหม่ของ Windows Autopatch: อัปเดตไว ไม่ต้องรีสตาร์ท

Microsoft ได้ประกาศเปลี่ยนพฤติกรรมของ Windows Autopatch โดยจะเริ่มเปิดใช้การอัปเดตแบบ Hotpatch เป็นค่าเริ่มต้นตั้งแต่เดือนพฤษภาคม 2026 สำหรับอุปกรณ์ที่มีสิทธิ์ทั้งหมดใน Microsoft Intune รวมถึงอุปกรณ์ที่เข้าถึงบริการผ่าน Microsoft Graph API

ข้อดีของการใช้ Hotpatch

- ติดตั้งแพตช์ได้โดย ไม่ต้องรีสตาร์ทเครื่อง
- ช่วยให้อุปกรณ์ 90% ได้รับการอัปเดตเร็วขึ้นกว่าเดิมเท่าตัว
- ผู้ดูแลระบบยังคงสามารถควบคุมและจัดการการอัปเดตได้ตามปกติ

ข้อมูลอ้างอิง

Mar 11, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/microsoft-patches-84-flaws-in-march.html