วันที่ 20 เมษายน 2569

พบ Zero-Day ใน Microsoft Defender 3 รายการถูกนำไปใช้โจมตีจริง

Huntress ออกมาเตือนว่ากลุ่มผู้ไม่หวังดีกำลังใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยที่เพิ่งถูกเปิดเผย 3 รายการใน Microsoft Defender เพื่อยกระดับสิทธิ์การเข้าถึงในระบบที่ถูกเจาะแล้ว

รายละเอียดช่องโหว่

การโจมตีนี้เกี่ยวข้องกับช่องโหว่ 3 รายการ ได้แก่ BlueHammer (ต้องล็อกอิน GitHub), RedSun และ UnDefend ซึ่งทั้งหมดถูกเปิดเผยในฐานะ Zero-day โดยนักวิจัยที่ใช้ชื่อว่า Chaotic Eclipse (หรือ Nightmare-Eclipse) เพื่อตอบโต้แนวทางของ Microsoft ในการจัดการกระบวนการเปิดเผยช่องโหว่

- BlueHammer และ RedSun: เป็นช่องโหว่ประเภทยกระดับสิทธิ์ในเครื่อง (Local Privilege Escalation หรือ LPE) ที่ส่งผลต่อ Microsoft Defender
- UnDefend: สามารถถูกใช้เพื่อทำให้ระบบเกิดอาการหยุดทำงาน (Denial-of-Service หรือ DoS) และทำให้ไม่สามารถอัปเดตฐานข้อมูลไวรัสได้

สถานะการแพตช์และการโจมตี

Microsoft ได้ออกแพตช์แก้ไข BlueHammer แล้วในชุดอัปเดต Patch Tuesday ที่ปล่อยออกมาเมื่อต้นสัปดาห์ที่ผ่านมา โดยถูกติดตามภายใต้รหัส CVE-2026-33825 อย่างไรก็ตาม ช่องโหว่อื่นๆ ยังไม่มีการแก้ไขในขณะนี้

ทาง Huntress ระบุว่าพบการนำช่องโหว่ทั้งสามไปใช้โจมตีจริง โดยมีลำดับเหตุการณ์ดังนี้:

- BlueHammer: ถูกนำมาใช้ตั้งแต่วันที่ 10 เมษายน 2026
- RedSun และ UnDefend: มีการใช้โค้ดตัวอย่าง (PoC) ในวันที่ 16 เมษายน

การเรียกใช้งานเหล่านี้เกิดขึ้นหลังจากมีการรันคำสั่งพื้นฐาน เช่น whoami /priv, cmdkey /list, net group และคำสั่งอื่นๆ ซึ่งบ่งชี้ว่าผู้โจมตีกำลังควบคุมเครื่องโดยตรง

การดำเนินการและความมุ่งมั่นของ Microsoft

บริษัทด้านความปลอดภัยไซเบอร์ระบุว่า ได้ดำเนินการแยกระบบขององค์กรที่ได้รับผลกระทบออกมาแล้ว เพื่อป้องกันการโจมตีเพิ่มเติมในขั้นตอนหลังจากเจาะระบบสำเร็จ

เมื่อสอบถามไปยัง **Microsoft** บริษัทได้ยืนยันการแก้ไขช่องโหว่ BlueHammer ผ่าน CVE-2026-33825 พร้อมแถลงว่า "Microsoft มีความมุ่งมั่นในการตรวจสอบปัญหาด้านความปลอดภัยที่มีการรายงานเข้ามา และจะอัปเดตอุปกรณ์ที่ได้รับผลกระทบเพื่อปกป้องผู้ใช้งานโดยเร็วที่สุด" โฆษกของ Microsoft กล่าว

ข้อมูลอ้างอิง

Apr 17, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/three-microsoft-defender-zero-days.html