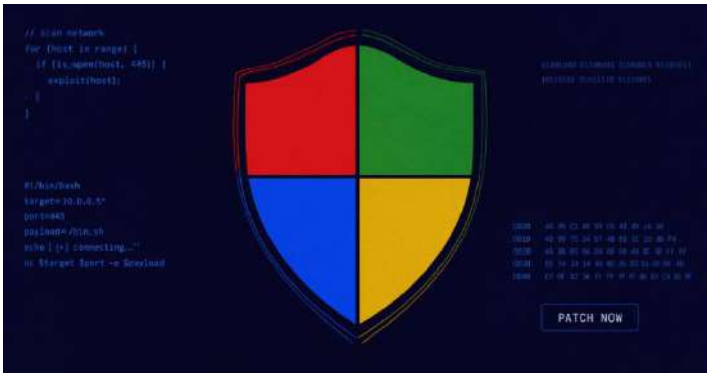
วันที่ 10 กรกฎาคม 2569

Microsoft ออกแพตช์อุดช่องโหว่ RoguePlanet ใน Defender ที่อาจถูกใช้ยกระดับสิทธิ์เป็น SYSTEM ได้



Microsoft ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ใน Microsoft Defender ที่มีชื่อว่า RoguePlanet หลังจากรายละเอียดของช่องโหว่ถูกเปิดเผยสู่สาธารณะเกือบหนึ่งเดือน ช่องโหว่นี้ถูกติดตามในรหัส CVE-2026-50656 (คะแนน CVSS: 7.8) เป็นช่องโหว่ประเภท Privilege Escalation ที่อยู่ใน Microsoft Malware Protection Engine (mpengine.dll) ซึ่งเป็นส่วนสำคัญที่ทำหน้าที่สแกน ตรวจจับ และกำจัดมัลแวร์สำหรับซอฟต์แวร์ป้องกันไวรัสและสปายแวร์ของ Microsoft

Microsoft ได้แก้ไขปัญหาดังกล่าวใน Microsoft Malware Protection Engine เวอร์ชัน 1.1.26060.3008 พร้อมทั้งเพิ่มการปรับปรุงด้านความปลอดภัย (Defense-in-Depth) เพื่อเสริมความแข็งแกร่งให้กับฟังก์ชันด้านความปลอดภัยบางส่วน แม้ว่าจะไม่ได้เปิดเผยรายละเอียดเพิ่มเติม

ช่องโหว่ RoguePlanet ถูกเปิดเผยครั้งแรกโดยนักวิจัยด้านความปลอดภัยที่ใช้ชื่อว่า Chaotic Eclipse (หรือ Nightmare-Eclipse) โดยระบุว่าเป็นช่องโหว่ประเภท Race Condition ที่สามารถถูกนำไปใช้เพื่อเปิดเชลล์ (Shell) ด้วยสิทธิ์ระดับ SYSTEM ได้

เมื่อผู้โจมตีได้รับสิทธิ์ระดับ SYSTEM แล้ว ก็จะสามารถรันโค้ดใดก็ได้ หรือดำเนินการต่างๆ บนเครื่องโดยไม่ได้รับอนุญาต นักวิจัยยังระบุเพิ่มเติมว่า การโจมตีนี้สามารถใช้งานได้แม้ระบบจะติดตั้งอัปเดต Patch Tuesday ประจำเดือนมิถุนายน 2026 แล้ว และยังสามารถใช้ได้ทั้งในกรณีที่เปิดหรือปิด Real-time Protection ของ Microsoft Defender

อย่างไรก็ตาม Microsoft ยังไม่ได้ให้เครดิต Chaotic Eclipse ในฐานะผู้ค้นพบช่องโหว่นี้อย่างเป็นทางการ RoguePlanet ถือเป็นช่องโหว่ตัวที่ 4 ใน Microsoft Defender ที่ Chaotic Eclipse เปิดเผย ต่อจาก BlueHammer (CVE-2026-33825), UnDefend (CVE-2026-45498) และ RedSun (CVE-2026-41091) ซึ่งทั้งหมดได้รับการแก้ไขจาก Microsoft ไปแล้ว

Microsoft ระบุว่า ผู้ใช้งานไม่จำเป็นต้องดำเนินการใดๆ เพื่อรับการอัปเดตสำหรับ CVE-2026-50656 เนื่องจาก Microsoft Malware Protection Engine จะได้รับการอัปเดตโดยอัตโนมัติเป็นประจำ เพื่อให้สามารถป้องกันภัยคุกคามรูปแบบใหม่ๆ ได้อย่างต่อเนื่อง

Microsoft ระบุเพิ่มเติมว่า ทั้งในองค์กรและผู้ใช้งานทั่วไป การตั้งค่าเริ่มต้นของซอฟต์แวร์ป้องกันมัลแวร์ของ Microsoft จะช่วยให้ฐานข้อมูลมัลแวร์ (Malware Definitions) และ Microsoft Malware Protection Engine ได้รับการอัปเดตโดยอัตโนมัติ

นอกจากนี้ Microsoft ยังอธิบายว่า ขึ้นอยู่กับซอฟต์แวร์ป้องกันมัลแวร์ที่ใช้งานและการตั้งค่าของแต่ละระบบ โปรแกรมอาจตรวจสอบการอัปเดตของตัว Engine และฐานข้อมูลมัลแวร์ทุกวัน หรือหลายครั้งต่อวันเมื่อเชื่อมต่ออินเทอร์เน็ต และผู้ใช้งานยังสามารถตรวจสอบการอัปเดตด้วยตนเองได้ทุกเมื่อ

ข้อมูลอ้างอิง

Jul 9, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/microsoft-patches-rogueplanet-defender.html