วันที่ 23 กรกฎาคม 2569

ช่องโหว่ร้ายแรง SharePoint RCE หมายเลข CVE-2026-50522 ถูกนำไปใช้โจมตีจริง หลังมีการเผยแพร่ PoC สู่สาธารณะ

ช่องโหว่ตัวที่สามของ Microsoft SharePoint Server ที่ Microsoft แก้ไขในชุดอัปเดต Patch Tuesday ประจำเดือนกรกฎาคม 2026 กำลังถูกผู้ไม่หวังดีนำไปใช้โจมตีจริงแล้ว ตามรายงานจาก watchtower ช่องโหว่ดังกล่าวคือ CVE-2026-50522 (คะแนน CVSS 9.8) ซึ่งเป็นช่องโหว่ระดับ Critical ที่เกิดจากการจัดการข้อมูลที่ไม่เชื่อถือ (Deserialization of Untrusted Data) ภายใน Microsoft Office SharePoint โดยอาจเปิดโอกาสให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถรันโค้ดผ่านเครือข่ายได้ Microsoft ระบุว่า ผู้ค้นพบและรายงานช่องโหว่นี้คือ splitline นักวิจัยด้านความปลอดภัยจาก DEVCORE

Microsoft อธิบายในประกาศด้านความปลอดภัยเมื่อสัปดาห์ที่ผ่านมาว่า ในการโจมตีผ่านเครือข่าย ผู้โจมตีที่มีสิทธิ์อย่างน้อยในระดับ Site Owner สามารถเขียนโค้ดตามต้องการ เพื่อแทรกและรันโค้ดจากระยะไกลบน SharePoint Server ได้ นอกจากนี้ Microsoft ยังอธิบายเพิ่มเติมว่า ช่องโหว่นี้มีรูปแบบการโจมตีผ่านเครือข่าย (Attack Vector: Network หรือ AV:N) เนื่องจากสามารถถูกโจมตีจากระยะไกลผ่านอินเทอร์เน็ตได้ และมีความซับซ้อนในการโจมตีต่ำ (Attack Complexity: Low หรือ AC:L) เพราะผู้โจมตีไม่จำเป็นต้องมีความรู้เกี่ยวกับระบบมากนัก และสามารถใช้ชุดคำสั่งโจมตีเดิมซ้ำได้กับระบบที่มีช่องโหว่ Microsoft ยังประเมินระดับความเสี่ยงของ CVE-2026-50522 ไว้ว่าอยู่ในกลุ่ม Exploitation More Likely หรือมีแนวโน้มสูงที่จะถูกนำไปใช้โจมตีจริง

ด้าน watchTowr เปิดเผยผ่าน LinkedIn ว่า หลังจากมีการเผยแพร่ Proof-of-Concept (PoC) ของช่องโหว่นี้สู่สาธารณะ ก็ตรวจพบการโจมตีจริงต่อระบบ Microsoft SharePoint Server แบบติดตั้งภายในองค์กร (On-Premises) โดยผู้โจมตีสามารถขโมย Machine Key ของ SharePoint เพื่อนำไปใช้รักษาสิทธิ์การเข้าถึงระบบในระยะยาว

บริษัทด้านความปลอดภัยระบุว่า ผู้โจมตีสามารถดึง SharePoint Machine Key ได้ด้วยคำขอ (Request) เพียงครั้งเดียว การติดตั้งแพตช์เพียงอย่างเดียวไม่เพียงพอ ผู้ดูแลระบบควรเปลี่ยนข้อมูลรับรอง (Credentials) ของระบบที่อาจได้รับ

ผลกระทบทันที ขณะเดียวกัน Defused Cyber เปิดเผยเพิ่มเติมว่า กลุ่มผู้โจมตีมีแนวโน้มกำลังใช้ CVE-2026-50522 เพื่อส่งเพย์โหลดแบบ .NET Deserialization ไปยังหน้าเข้าสู่ระบบ (Sign-in Endpoint) ของ SharePoint

บริษัทระบุว่า คำขอที่ตรวจจับได้ไม่มีข้อมูลยืนยันตัวตน (Authentication) แนบมาด้วย ซึ่งสอดคล้องกับลักษณะของ CVE-2026-50522 ที่สามารถถูกโจมตีได้โดยไม่ต้องผ่านการยืนยันตัวตน CVE-2026-50522 ถือเป็นช่องโหว่ตัวที่สามของ SharePoint Server ที่ถูกนำไปใช้โจมตีจริง ต่อจาก CVE-2026-56164 (คะแนน CVSS 5.3) และ CVE-2026-58644 (คะแนน CVSS 9.8) ซึ่งทั้งสองช่องโหว่นี้เคยถูกใช้เป็น Zero-Day ก่อนที่ Microsoft จะออกแพตช์แก้ไขในเดือนกรกฎาคม 2026

ด้าน สำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้ออกคำเตือนว่า ปัจจุบันผู้โจมตีกำลังใช้ช่องโหว่หลายรายการของ SharePoint Server เพื่อเข้าถึงระบบที่ติดตั้งภายในองค์กรโดยไม่ได้รับอนุญาต ซึ่งประกอบด้วย

- CVE-2026-32201
- CVE-2026-45659
- CVE-2026-56164
- CVE-2026-58644

CISA ระบุว่า ช่องโหว่เหล่านี้ส่งผลกระทบต่อ SharePoint Server แบบติดตั้งภายในองค์กร (On-Premises) ทุกเวอร์ชันที่ยังได้รับการสนับสนุน ได้แก่ Subscription Edition, SharePoint Server 2019 และ SharePoint Server 2016 โดยผู้โจมตีสามารถใช้ช่องโหว่เพื่อรันโค้ดจากระยะไกล (Remote Code Execution: RCE) และดำเนินกิจกรรมหลังจากเจาะระบบได้สำเร็จ เช่น การขโมย Internet Information Services (IIS) Machine Key และใช้เทคนิค Deserialization เพื่อคงการเข้าถึงระบบ (Persistence) รวมถึงติดตั้งมัลแวร์เพิ่มเติมในภายหลัง

ข้อมูลอ้างอิง

Jul 21, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/critical-sharepoint-rce-cve-2026-50522.html