วันที่ 8 กันยายน 2568

ช่องโหว่ร้ายแรงใน SAP S/4HANA CVE-2025-42957 ถูกโจมตี

มีการค้นพบช่องโหว่ด้านความปลอดภัยที่ร้ายแรงซึ่งส่งผลกระทบต่อ SAP S/4HANA ซอฟต์แวร์ระบบ ERP (Enterprise Resource Planning) โดยล่าสุดมีการยืนยันแล้วว่า ถูกนำไปโจมตีใช้งานจริงแล้วในโลกออนไลน์

ช่องโหว่นี้คือ CVE-2025-42957 ได้รับคะแนนความรุนแรงสูงถึง 9.9 จากคะแนนเต็ม 10.0 ซึ่งจัดว่าเป็นภัยคุกคามในระดับวิกฤต โดยเป็นช่องโหว่ประเภท command injection ที่ได้รับการแก้ไขโดย SAP ในชุดอัปเดตรายเดือนเมื่อเดือนที่แล้ว

“SAP S/4HANA เปิดโอกาสให้ผู้โจมตีที่มีสิทธิ์ผู้ใช้งาน สามารถใช้ประโยชน์จากช่องโหว่ในฟังก์ชันโมดูลที่ถูกเปิดใช้งานผ่าน RFC” ตามที่ระบุไว้ในคำอธิบายของช่องโหว่ในฐานข้อมูล NIST (NVD) “ช่องโหว่นี้ทำให้สามารถใส่โค้ด ABAP ที่เป็นอันตรายเข้าสู่ระบบ โดยข้ามการตรวจสอบสิทธิ์ที่สำคัญได้”

ผลกระทบจากการโจมตีและสถานการณ์ปัจจุบัน

การโจมตีที่สำเร็จสามารถนำไปสู่การยึดระบบ SAP ได้ทั้งหมด ส่งผลกระทบต่อความลับ ความถูกต้อง และความพร้อมใช้งานของระบบ ผู้โจมตีสามารถแก้ไขฐานข้อมูล, สร้างบัญชีผู้ใช้ระดับสูงที่มีสิทธิ์ SAP_ALL, ดาวน์โหลดรหัสผ่านที่เข้ารหัสไว้ และเปลี่ยนแปลงกระบวนการทางธุรกิจได้ตามต้องการ

SecurityBridge Threat Research Labs ยืนยันว่าได้พบการโจมตีจริงที่ใช้ประโยชน์จากช่องโหว่นี้ โดยมีผลกระทบทั้งเวอร์ชันที่ติดตั้งในองค์กร (on-premise) และเวอร์ชัน Private Cloud

“การโจมตีต้องการเพียงสิทธิ์ผู้ใช้ที่มีสิทธิต่ำเท่านั้น ก็สามารถยึดระบบ SAP ได้ทั้งหมด” บริษัทกล่าว “เป็นการยึดระบบที่ทำได้ง่ายมาก และหากสำเร็จ อาจนำไปสู่การฉ้อโกง, การขโมยข้อมูล, การสอดแนม, หรือแม้แต่การติดตั้งแรนซัมแวร์ได้”

แม้ว่าการโจมตีในวงกว้างยังไม่ถูกตรวจพบ แต่ผู้ไม่หวังดีมีความรู้ในการนำไปใช้งานแล้ว และการย้อนวิเคราะห์แพตช์เพื่อสร้างเครื่องมือโจมตีนั้น “ทำได้ค่อนข้างง่าย”

แนวทางป้องกันและคำแนะนำด่วน

องค์กรต่างๆ จึงถูกแนะนำให้รีบดำเนินการโดยด่วนเพื่อลดความเสี่ยง:

1. ติดตั้งแพตช์ทันที: รีบติดตั้งแพตช์จาก SAP ที่ออกในชุดอัปเดตเดือนที่แล้ว
2. เฝ้าระวัง Logs: เฝ้าระวังบันทึกการใช้งาน (logs) สำหรับการเรียกใช้ RFC ที่น่าสงสัยหรือการสร้างผู้ดูแลระบบใหม่
3. ตรวจสอบความปลอดภัย: ตรวจสอบให้แน่ใจว่ามีการแบ่งส่วนระบบ (segmentation) และการสำรองข้อมูลที่เหมาะสม

นอกจากนี้ ยังมีคำแนะนำเพิ่มเติมว่าควรพิจารณาเปิดใช้ SAP UCON เพื่อจำกัดการใช้งาน RFC และตรวจสอบรวมถึงจำกัดสิทธิ์การเข้าถึงวัตถุอนุญาต S_DMIS activity 02 เพื่อเพิ่มความปลอดภัยอีกชั้นหนึ่ง

อัปเดต: ผู้ให้บริการด้านความปลอดภัยไซเบอร์ Pathlock ยังเปิดเผยด้วยว่า “ตรวจพบกิจกรรมผิดปกติที่สอดคล้องกับการพยายามโจมตี CVE-2025-42957” พร้อมเตือนว่า “องค์กรใดก็ตามที่ยังไม่ได้ติดตั้งโน้ตความปลอดภัยประจำเดือนสิงหาคม 2025 ของ SAP กำลังตกอยู่ในความเสี่ยง”

ข้อมูลอ้างอิง

Sep 5, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/sap-s4hana-critical-vulnerability-cve.html