วันที่ 5 มกราคม 2569

เตือนผู้ใช้ n8n พบช่องโหว่ร้ายแรงระดับ CVSS 9.9 อินสแตนซ์ทั่วโลกเสี่ยงถูกโจมตี

ตรวจพบช่องโหว่ด้านความปลอดภัยระดับร้ายแรงในแพลตฟอร์มระบบอัตโนมัติแบบเวิร์กโฟลว์ n8n ซึ่งหากถูกโจมตีสำเร็จ ผู้ไม่หวังดีอาจสามารถ สั่งรันโค้ดใด ๆ บนระบบได้โดยตรง ส่งผลให้ระบบตกอยู่ในความเสี่ยงสูง ช่องโหว่นี้ถูกระบุด้วยรหัส CVE-2025-68613 และคะแนนความรุนแรง CVSS สูงถึง 9.9 จาก 10 คะแนน ซึ่งถือว่าอยู่ในระดับวิกฤต โดย n8n เป็นแพ็กเกจที่มีการดาวน์โหลดจาก npm ประมาณ 57,000 ครั้งต่อสัปดาห์ ทำให้มีผู้ใช้งานจำนวนมากที่อาจได้รับผลกระทบ

ผู้ดูแลแพ็กเกจบน npm ระบุว่า “ภายใต้เงื่อนไขคำสั่งบางอย่าง นิพจน์ (expressions) ที่ผู้ใช้ซึ่งล็อกอินแล้วใส่เข้าไปตอนตั้งค่าเวิร์กโฟลว์ อาจถูกนำไปประมวลผลในระบบที่ ไม่ได้แยกออกจากตัวระบบหลักอย่างปลอดภัย ช่องโหว่นี้ทำให้ผู้โจมตีที่มีบัญชีผู้ใช้ สามารถใช้ช่องโหว่เพื่อรันคำสั่งหรือโค้ดใด ๆ ได้ด้วยสิทธิ์เดียวกับระบบ n8n ซึ่งหากถูกโจมตีสำเร็จ อาจนำไปสู่การยึดระบบเครื่องทั้งหมด ไม่ว่าจะเป็นการเข้าถึงข้อมูลสำคัญ แก้ไขเวิร์กโฟลว์ หรือสั่งงานในระดับระบบปฏิบัติการได้

ช่องโหว่นี้ส่งผลกระทบต่อ n8n ทุกเวอร์ชันตั้งแต่ 0.211.0 ขึ้นไปจนถึงเวอร์ชันก่อน 1.120.4 โดยปัจจุบันได้มีการแก้ไขแล้วในเวอร์ชัน 1.120.4, 1.121.1 และ 1.122.0

จากข้อมูลของแพลตฟอร์ม Censys พบว่า ณ วันที่ 22 ธันวาคม 2025 มีอินสแตนซ์ที่อาจได้รับผลกระทบมากถึง 103,476 แห่งทั่วโลก โดยส่วนใหญ่อยู่ในสหรัฐอเมริกา เยอรมนี ฝรั่งเศส บราซิล และสิงคโปร์

คำแนะนำเร่งด่วน

- อัปเดตเป็นเวอร์ชันล่าสุดทันที เวอร์ชัน 1.120.4, 1.121.1 และ 1.122.0
- หากยังไม่สามารถอัปเดตได้ ให้จำกัดสิทธิ์การสร้าง และแก้ไขเวิร์กโฟลว์เฉพาะผู้ใช้ที่เชื่อถือได้
- ลดสิทธิ์ของระบบปฏิบัติการที่ใช้รันบริการ และจำกัดการเข้าถึงเครือข่ายและพอร์ตที่ไม่จำเป็น
- ตรวจสอบการตั้งค่าความปลอดภัยของระบบโดยรวม เพื่อลดความเสี่ยงจากการถูกโจมตี

ข้อมูลอ้างอิง

Dec 23, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/12/critical-n8n-flaw-cvss-99-enables.html