วันที่ 8 มกราคม 2569

ช่องโหว่ร้ายแรงใน n8n (CVSS 10.0) เปิดทางให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตนเข้าควบคุมระบบทั้งหมดได้

นักวิจัยด้านความปลอดภัยไซเบอร์ได้เปิดเผยรายละเอียดของช่องโหว่ความรุนแรงระดับสูงสุดอีกหนึ่งรายการใน n8n ซึ่งเป็นแพลตฟอร์มระบบอัตโนมัติแบบเวิร์กโฟลว์ (Workflow Automation) ที่ได้รับความนิยมอย่างมาก โดยช่องโหว่นี้เปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ไม่ต้องมีการยืนยันตัวตน สามารถเข้าควบคุมระบบที่ได้รับผลกระทบได้อย่างสมบูรณ์แบบ ช่องโหว่นี้ถูกติดตามด้วยรหัส CVE-2026-21858 และได้รับคะแนนความรุนแรง CVSS 10.0 เต็ม โดยมีชื่อรหัสว่า “Ni8mare” (ไนท์แมร์) ซึ่งตั้งโดย Cyera Research Labs โดยนักวิจัยด้านความปลอดภัยชื่อ Dor Attias เป็นผู้ค้นพบและรายงานช่องโหว่นี้ตั้งแต่วันที่ 9 พฤศจิกายน 2025

คำเตือนจาก n8n และสรุป 4 ช่องโหว่ร้ายแรงในรอบ 2 สัปดาห์

ทาง n8n ได้ระบุในประกาศแจ้งเตือนว่า “ช่องโหวใน n8n อนุญาตให้ผู้โจมตีเข้าถึงไฟล์บนเซิร์ฟเวอร์ที่อยู่เบื้องหลัง ผ่านการทำงานของเวิร์กโฟลว์บางประเภทที่ใช้แบบฟอร์ม (Form) ซึ่งอาจเปิดทางให้ผู้โจมตีจากระยะไกลที่ไม่ต้องยืนยันตัวตนเข้าถึงข้อมูลสำคัญที่เก็บอยู่ในระบบ และอาจนำไปสู่การโจมตีต่อเนื่องเพิ่มเติมได้ ขึ้นอยู่กับการตั้งค่าและการนำเวิร์กโฟลว์ไปใช้” เป็นที่น่าสังเกตว่าในช่วงเพียงสองสัปดาห์ที่ผ่านมา n8n ได้เปิดเผยช่องโหว่ระดับร้ายแรงถึง 4 รายการ ได้แก่:

- CVE-2025-68613 (CVSS 9.9): ช่องโหว่การจัดการโค้ดไดนามิกที่อาจทำให้ผู้ใช้ที่ยืนยันตัวตนแล้วรันโค้ดจากระยะไกล (RCE) ได้ (แก้ไขในเวอร์ชัน 1.120.4, 1.121.1 และ 1.122.0)
- CVE-2025-68668 หรือ N8scape (CVSS 9.9): ช่องโหว่การหลบเลี่ยง Sandbox ทำให้ผู้สร้างเวิร์กโฟลว์สั่งรันคำสั่งใดๆ บนเครื่องโฮสต์ได้ (แก้ไขในเวอร์ชัน 2.0.0)

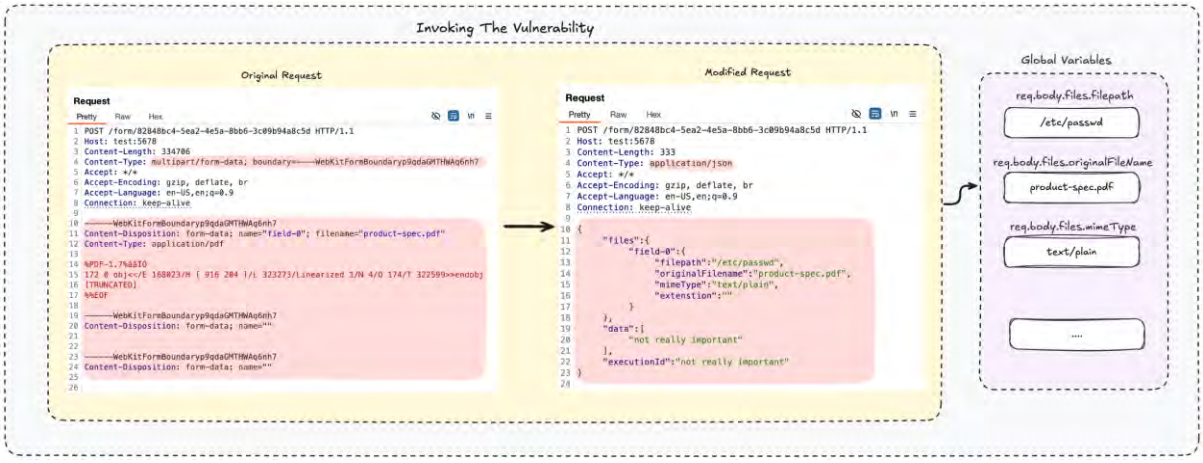
- CVE-2026-21877 (CVSS 10.0): ช่องโหว่การอัปโหลดไฟล์อันตรายโดยไม่มีการจำกัด นำไปสู่การยึดครองระบบทั้งหมด (แก้ไขในเวอร์ชัน 1.121.3)
- CVE-2026-21858 (Ni8mare): ช่องโหว่ล่าสุดที่มีความแตกต่างเพราะไม่ต้องใช้ข้อมูลเข้าสู่ระบบใด ๆ และใช้ค่าของ “Content-Type” เพื่อดึงข้อมูลลับและรันคำสั่งบนเซิร์ฟเวอร์

เจาะลึกรายละเอียดเชิงเทคนิค: กลไกการจัดการ Webhook ที่ผิดพลาด

Cyera ได้เปิดเผยข้อมูลกับ The Hacker News ว่าปัญหาหลักเกิดจากกลไกการทำงานของ Webhook และการจัดการไฟล์ใน n8n โดยปกติ Webhook จะเรียกใช้งานฟังก์ชันชื่อ parseRequestBody() เพื่อประมวลผลคำขอที่เข้ามา ซึ่งฟังก์ชันนี้จะอ่านค่า “Content-Type” จาก HTTP header เพื่อเลือกวิธีประมวลผลดังนี้:

1. ใช้ parseFormData() (file upload parser): เมื่อ Content-Type เป็น multipart/form-data โดยจะใช้ฟังก์ชัน parse() จากไลบรารี formidable ของ Node.js และนำผลลัพธ์ไปเก็บไว้ในตัวแปร req.body.files
2. ใช้ parseBody() (regular body parser): สำหรับ Content-Type ประเภทอื่นทั้งหมด และเก็บข้อมูลไว้ในตัวแปร req.body

ต้นตอของช่องโหว่: CVE-2026-21858 เกิดขึ้นเพราะฟังก์ชันที่จัดการการส่งแบบฟอร์ม (formWebhook()) เรียกใช้ฟังก์ชันจัดการไฟล์ที่ชื่อว่า copyBinaryFile() โดยดึงข้อมูลมาจาก req.body.files โดยไม่ได้ตรวจสอบก่อนว่า Content-Type เป็น multipart/form-data หรือไม่ คุณ Attias อธิบายว่า: “ปัญหาคือฟังก์ชันนี้ถูกเรียกใช้งานโดยไม่มีการตรวจสอบ ทำให้เราควบคุมค่า req.body.files ได้ทั้งหมดรวมถึงพารามิเตอร์ filepath ด้วย ดังนั้นแทนที่จะคัดลอกไฟล์ที่ผู้ใช้อัปโหลด เรากลับสามารถคัดลอกไฟล์ใดก็ได้จากระบบ ส่งผลให้โหนดใดๆ ที่ทำงานต่อจาก Form node จะได้รับเนื้อหาของไฟล์ในเครื่องแทนที่จะเป็นไฟล์ที่ผู้ใช้ส่งเข้ามา”



สถานการณ์จำลองการโจมตี: จากการอ่านไฟล์สู่การรันโค้ด (RCE)

หากเว็บไซต์มีระบบแชตที่ใช้ไฟล์สเปกสินค้าผ่านเวิร์กโฟลว์แบบฟอร์ม ผู้โจมตีสามารถใช้ช่องโหว่นี้เพื่อยึดครองระบบตามขั้นตอนดังนี้:

1. อ่านฐานข้อมูล: เข้าถึงไฟล์ฐานข้อมูลที่ /home/node/.n8n/database.sqlite แล้วโหลดเข้าไปในฐานความรู้ของระบบแชต
2. ดึงข้อมูลแอดมิน: ดึงค่า user ID, อีเมล และรหัสผ่านที่ถูกแฮชของผู้ดูแลระบบผ่านระบบแชตนั้น
3. ขโมย Secret Key: ใช้การอ่านไฟล์อีกครั้งเพื่อเข้าถึงไฟล์คอนฟิกที่ /home/node/.n8n/config เพื่อดึงค่า secret key สำหรับการเข้ารหัส
4. ปลอมตัวเป็นแอดมิน: ใช้ข้อมูลที่ได้มาสร้าง session cookie ปลอม เพื่อข้ามการยืนยันตัวตนและเข้าสู่ระบบในฐานะผู้ดูแล
5. ยึดระบบโดยสมบูรณ์: สร้างเวิร์กโฟลว์ใหม่ที่มีโหนด “Execute Command” เพื่อรันคำสั่งใดๆ บนเครื่อง (RCE)

ผลกระทบมหาศาล: Cyera ระบุว่าการถูกเจาะ n8n เท่ากับมอบกุญแจเข้าถึงทุกอย่าง ทั้ง API credentials, OAuth tokens, การเชื่อมต่อฐานข้อมูล หรือคลาวด์สตอเรจทั้งหมดที่ถูกรวมศูนย์ไว้ n8n จึงกลายเป็นจุดล้มเหลวเพียงจุดเดียว (Single Point of Failure) ที่มีค่ามหาศาลสำหรับผู้ไม่หวังดี

เวอร์ชันที่ได้รับผลกระทบและแนวทางแก้ไข

- เวอร์ชันที่ได้รับผลกระทบ: n8n ทุกเวอร์ชันตั้งแต่เริ่มต้นจนถึงเวอร์ชัน 1.65.0
- เวอร์ชันที่แก้ไขแล้ว: เวอร์ชัน 1.121.0 (ปล่อยเมื่อ 18 พ.ย. 2025)
- เวอร์ชันล่าสุดปัจจุบัน: 1.123.10, 2.1.5, 2.2.4 และ 2.3.0

ข้อแนะนำในการป้องกัน:

1. **อัปเกรดทันที:** ผู้ใช้งานควรรีบอัปเกรดเป็นเวอร์ชันล่าสุดโดยเร็วที่สุด
2. **จำกัดการเข้าถึง:** หลีกเลี่ยงการเปิด n8n ให้เข้าถึงจากอินเทอร์เน็ตโดยตรง และกำหนดให้ทุก Form ต้องมีการยืนยันตัวตน
3. **มาตรการชั่วคราว:** แนะนำให้จำกัดหรือปิดการเข้าถึง webhook และ form endpoint ที่เปิดให้สาธารณะ จนกว่าจะอัปเดตระบบเสร็จสิ้น

ข้อมูลอ้างอิง

Jan 7, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/critical-n8n-vulnerability-cvss-100.html