

張貼日期：2026/03/03

【漏洞預警】n8n存在4個重大資安漏洞

- 主旨說明: 【漏洞預警】n8n存在4個重大資安漏洞
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202602-00000016
 - n8n是一款開源工作流程自動化工具，透過視覺化拖拉介面串接多種應用程式，無需程式碼即可自動化重複性任務，近日n8n發布重大資安公告。
 - [CVE-2026-27495][CVSS]9.4 此漏洞允許經身分驗證且擁有或修改工作流程權限的攻擊者，可利用JavaScript任務執行沙箱中的漏洞，在邊界之外執行任意程式碼。
 - [CVE-2026-27493][CVSS]9.5 此為二階段表達式注入漏洞，未經身分驗證的攻擊者，可透過精心設計的表單資料注入並執行任意n8n表達式，若與表達式的沙箱逃逸機制結合使用，可能導致在n8n主機上執行遠端程式碼。
 - [CVE-2026-27577][CVSS]9.4 此漏洞允許經身分驗證且擁有建立或修改工作流程權限的攻擊者，可利用特製的工作流程參數表達式，在執行n8n主機上觸發未經授權的系統指令。
 - [CVE-2026-27498][CVSS]9.0 此漏洞允許經身分驗證且擁有建立或修改工作流程權限的攻擊者，利用git操作連結「從磁碟讀取/寫入檔案」節點，導致攻擊者可遠端程式碼執行。
- 影響平台:
 - [CVE-2026-27495][CVE-2026-27493][CVE-2026-27577] n8n 1.123.22(不含)之前版本 [n8n 2.0.0至2.9.3(不含)之前版本 [n8n 2.10.0至2.10.1(不含)之前版本
 - [CVE-2026-27498] n8n 1.123.8(不含)之前版本 [n8n 2.2.0(不含)之前版本
- 建議措施:
 - [CVE-2026-27495][CVE-2026-27493][CVE-2026-27577] 請更新至以下版本 [n8n 1.123.22(含)之後版本 [n8n 2.9.3(含)之後版本 [n8n 2.10.1(含)之後版本
 - [CVE-2026-27498] 請更新至以下版本 [n8n 1.123.8(含)之後版本 [n8n 2.2.0(含)之後版本
- 參考資料:
 1. <https://www.twcert.org.tw/tw/cp-169-10739-e7e58-1.html>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailling:announcement:20260303_24

Last update: **2026/03/03 15:29**