

ANA事件單通知:TACERT-ANA-2026011501012222【漏洞預警】n8n存在4個重大資安漏洞(CVE-2025-68613)(CVE-2025-68668)(CVE-2026-21877)(CVE-2026-21858)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026011501012222	發佈時間	2026-01-15 13:44:25
事故類型	ANA-漏洞預警	發現時間	2026-01-15 13:44:25
影響等級	低		

[主旨說明:]【漏洞預警】n8n存在4個重大資安漏洞(CVE-2025-68613)(CVE-2025-68668)(CVE-2026-21877)(CVE-2026-21858)

[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-200-202601-00000014

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。近期n8n發布多個重大資安漏洞公告。

【CVE-2025-68613，CVSS：9.9】 此為遠端程式碼執行漏洞，在特定條件下，允許經身分驗證的攻擊者以n8n行程的權限執行任意程式碼。

【CVE-2025-68668，CVSS：9.9】 由於n8n使用Pydide的Python程式碼節點存在沙箱繞過漏洞，經身分驗證且具有建立或修改工作流程權限的攻擊者，以n8n行程相同權限在n8n伺服器上執行任意命令。

【CVE-2026-21877，CVSS：10.0】 此漏洞允許經過身分驗證的攻擊者，可利用n8n服務執行惡意程式碼，導致系統完全被破壞。

【CVE-2026-21858，CVSS：10.0】 此漏洞允許未經身分驗證的攻擊者，可透過執行某些基於表單工作流程，存取底層伺服器的檔案，導致儲存在系統中的敏感資料外洩。

情資分享等級：WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

n8n 0.211.0至1.120.4(不含)之前版本

n8n 1.121.0版本

n8n 1.0.0至2.0.0(不含)之前版本

n8n 0.121.2 (含)之前版本

n8n 1.65.0至1.121.0(不含)之前版本

[建議措施:]

【CVE-2025-68613】 請更新至以下版本： n8n 1.120.4版本、1.121.1版本、1.122.0版本

【CVE-2025-68668】 請更新至以下版本： n8n 2.0.0版本

【CVE-2026-21877】 請更新至以下版本： n8n 1.121.3版本

【CVE-2026-21858】 請更新至以下版本： n8n 1.121.0版本

[參考資料:]

1. <https://www.twcert.org.tw/tw/cp-169-10636-1fa36-1.html>

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw