

## ANA事件單通知:TACERT-ANA-2025082609085555【漏洞預警】CISA新增2個已知遭駭客利用之漏洞至KEV目錄(2025/08/18-2025/08/24)

### 教育機構ANA通報平台

發佈編號	TACERT-ANA-2025082609085555	發佈時間	2025年8月26日 09:57:56
事故類型	ANA-漏洞預警	發現時間	2025年8月26日 09:57:56
影響等級	低		

[主旨說明:]【漏洞預警】CISA新增2個已知遭駭客利用之漏洞至KEV目錄(2025/08/18-2025/08/24)

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202508-00000013

1. 【CVE-2025-54948】趨勢科技 Apex One OS 指令注入漏洞 (CVSS v3.1: 9.4)

【是否遭勒索軟體利用:未知】 Trend Micro Apex One本地部署版本存在作業系統指令注入漏洞，未經身分鑑別之遠端攻擊者可於管理主控台上傳惡意程式碼並達成遠端執行任意程式碼。

【影響平台】請參考官方所列的影響版本

<https://success.trendmicro.com/en-US/solution/KA-0020652>

2. 【CVE-2025-43300】Apple iOS、iPadOS 和 macOS 越界寫入漏洞 (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Apple iOS、iPadOS和macOS的Image I/O架構中存在越界寫入漏洞。

【影響平台】

- iPad OS 17.7.10(不含)之前的版本
- iPad OS 18.0至18.6.2(不含)的版本
- iOS 18.6.2(不含)之前的版本
- macOS 13.0.0至13.7.8(不含)的版本
- macOS 14.0至14.7.8(不含)的版本
- macOS 15.0至15.6.1(不含)的版本

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:]

詳細內容於內容說明欄之影響平台

[建議措施:]

1. 【CVE-2025-54948】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://success.trendmicro.com/en-US/solution/KA-0020652>

2. 【CVE-2025-43300】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.apple.com/en-us/124925>

<https://support.apple.com/en-us/124926>

<https://support.apple.com/en-us/124927>

<https://support.apple.com/en-us/124928>

<https://support.apple.com/en-us/124929>

[參考資料:]

(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](mailto:service@cert.tanet.edu.tw)