

張貼日期：2025/04/28

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/04/14-2025/04/20)

- 主旨說明：【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/04/14-2025/04/20)

- 內容說明：

- 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202504-00000008

1. CVE-2021-20035 SonicWall SMA100 Appliances OS Command Injection Vulnerability (CVSS v3.1: 6.5)

【是否遭勒索軟體利用：未知】SonicWall SMA100裝置的管理介面存在作業系統指令注入漏洞，該漏洞允許遠端已驗證的攻擊者以nobody使用者身份注入任意指令，導致任意程式碼執行。

【影響平台】請參考官方所列的影響版本

<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0022>

2. CVE-2025-24054 Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability (CVSS v3.1: 5.4)

【是否遭勒索軟體利用：未知】Microsoft Windows NTLM存在檔案名稱或路徑的外部控制漏洞，該漏洞允許未經授權的攻擊者透過網路進行偽冒。

【影響平台】請參考官方所列的影響版本

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054>

3. CVE-2025-31201 Apple Multiple Products Arbitrary Read and Write Vulnerability (CVSS v3.1: 6.8)

【是否遭勒索軟體利用：未知】Apple iOS iPadOS macOS及其他產品中存在任意讀寫漏洞，該漏洞允許攻擊者繞過指標驗證。

【影響平台】

- iOS 18.4.1
- iPadOS 18.4.1
- macOS Sequoia 15.4.1
- tvOS 18.4.1
- visionOS 2.4.1

4. CVE-2025-31200 Apple Multiple Products Memory Corruption Vulnerability (CVSS v3.1: 7.5)

【是否遭勒索軟體利用：未知】Apple iOS iPadOS macOS及其他產品中存在記憶體損毀漏洞，當處理惡意製作的媒體檔案中的音訊串流時，允許執行任意程式碼。

【影響平台】

- iOS 18.4.1
- iPadOS 18.4.1
- macOS Sequoia 15.4.1
- tvOS 18.4.1
- visionOS 2.4.1

- 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-2021-20035 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0022>

2. CVE-2025-24054 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054>

3. CVE-2025-31201 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/122282>

- <https://support.apple.com/en-us/122400>

- <https://support.apple.com/en-us/122401>
 - <https://support.apple.com/en-us/122402>
4. [CVE-2025-31200] 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/122282>
 - <https://support.apple.com/en-us/122400>
 - <https://support.apple.com/en-us/122401>
 - <https://support.apple.com/en-us/122402>
-

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/announcement:20250428_01



Last update: **2025/04/28 09:54**