教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025063008061313	發佈時間	2025-06-30 08:55:13
事故類型	ANA-漏洞預警	發現時間	2025-06-30 08:55:13
影響等級	低		

[主旨說明:]【漏洞預警】CISA 新增 3 個已知遭駭客利用之漏洞至 KEV 目錄 (2025/06/16-2025/06/22)

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202506-00000020

1.【CVE-2023-33538】TP-Link Multiple Routers Command Injection Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 TP-Link TL-WR940N V2/V4、TL-WR841N V8/V10，以及 TL-WR740N V1/V2 存在透過 /userRpm/WlanNetworkRpm 元件進行指令注入的漏洞。

【影響平台】 TP-Link TL-WR940N V2/V4 TP-Link TL-WR841N V8/V10 TP-Link TL-WR740N V1/V2

2.【CVE-2025-43200】Apple Multiple Products Unspecified Vulnerability (CVSS v3.1: 4.8)

【是否遭勒索軟體利用:未知】 Apple iOS、iPadOS、macOS、watchOS 及 visionOS 在處理透過 iCloud 連結分享的惡意製作照片或影片時，存在安全性漏洞。

【影響平台】請參考官方所列的影響版本 https://support.apple.com/en-us/100100

3.【CVE-2023-0386】Linux Kernel Improper Ownership Management Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Linux 核心存在權限管理不當漏洞，該漏洞出現在 OverlayFS 子系統中，允許已取得一般權限之本機攻擊者在特定條件下執行原本應受限制的 setuid 檔案，從而提升至管理者權限。

【影響平台】 Linux kernel 6.2-rc6

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:]

【CVE-2023-33538】 受影響的產品可能已經達到產品生命週期終點（EoL）和/或終止服務（EoS）。建議使用者停止使用這些產品。

【CVE-2025-43200】 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/122346

https://support.apple.com/en-us/122901

https://support.apple.com/en-us/122900

https://support.apple.com/en-us/122173

https://support.apple.com/en-us/122903

https://support.apple.com/en-us/122345

https://support.apple.com/en-us/122902

https://support.apple.com/en-us/122174

https://support.apple.com/en-us/122904

【CVE-2023-0386】 官方已針對漏洞釋出修復更新，請更新至相關版本

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a