國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-2026022404022222【漏洞預警】CISA新增11個已知遭駭客利用之漏洞至KEV目錄(2026/02/09-2026/02/15)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026022404022222	發佈時間	2026-02-24 16:38:23
事故類型	ANA-漏洞預警	發現時間	2026-02-24 16:38:23
影響等級	低		

[主旨說明:]【漏洞預警】CISA新增11個已知遭駭客利用之漏洞至KEV目錄(2026/02/09-2026/02/15)

[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-200-202602-00000009

【CVE-2026-21513】Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Microsoft MSHTML Framework 存在保護機制失效漏洞，可能允許未經授權的攻擊者透過網路繞過安全功能。

【CVE-2026-21525】Microsoft Windows NULL Pointer Dereference Vulnerability (CVSS v3.1: 6.2)

【是否遭勒索軟體利用:未知】 Microsoft Windows Remote Access Connection Manager 存在空指標解引用漏洞，可能允許未經授權的攻擊者在本機造成服務阻斷。

【CVE-2026-21510】Microsoft Windows Shell Protection Mechanism Failure Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Microsoft Windows Shell 存在保護機制失效漏洞，可能允許未經授權的攻擊者透過網路繞過安全功能。

【CVE-2026-21533】Microsoft Windows Improper Privilege Management Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Microsoft Windows Remote Desktop Services 存在不當權限管理漏洞，可能允許已授權的攻擊者在本機提升權限。

【CVE-2026-21519】Microsoft Windows Type Confusion Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Microsoft Desktop Windows Manager 存在類型混淆漏洞，可能允許已授權的攻擊者在本機提升權限。

【CVE-2026-21514】Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Microsoft Office Word 在安全決策中依賴不受信任的輸入，可能允許已授權的攻擊者在本機提升權限。

【CVE-2026-20700】Apple Multiple Buffer Overflow Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Apple iOS、macOS、tvOS、watchOS 及 visionOS 存在緩衝區溢位漏洞，可能允許具備記憶體寫入權限的攻擊者執行任意程式碼。

【CVE-2024-43468】Microsoft Configuration Manager SQL Injection Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Microsoft Configuration Manager 存在SQL 注入漏洞。未經驗證的攻擊者可透過向目標環境發送特製請求，於伺服器及／或底層資料庫上執行指令。

【CVE-2025-15556】Notepad++ Download of Code Without Integrity Check Vulnerability (CVSS v3.1: 7.5)

【是否遭勒索軟體利用:未知】 Notepad++ 在使用 WinGUp 更新程式時，存在未經完整性檢查的程式碼下載漏洞，可能允許攻擊者攔截或重新導向更新流量，進而下載並執行攻擊者控制的安裝程式。

此漏洞可能導致攻擊者以使用者權限執行任意程式碼。

【CVE-2025-40536】SolarWinds Web Help Desk Security Control Bypass Vulnerability (CVSS v3.1: 8.1)

【是否遭勒索軟體利用:未知】 SolarWinds Web Help Desk 存在安全控制繞過漏洞，可能允許未經驗證的攻擊者存取部分受限功能。

【CVE-2026-1731】BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:是】 BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) 存在作業系統指令注入漏洞。

該漏洞可能允許未經驗證的遠端攻擊者以網站使用者的身份執行作業系統指令。

此漏洞無需驗證或使用者互動即可利用，可能導致系統遭入侵，包括未經授權存取、資料外洩及服務中斷。

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:]

【CVE-2026-21513】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513

【CVE-2026-21525】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21525

【CVE-2026-21510】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21510

【CVE-2026-21533】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533

【CVE-2026-21519】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21519

【CVE-2026-21514】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21514

【CVE-2026-20700】請參考官方所列的影響版本 https://support.apple.com/en-us/100100

【CVE-2024-43468】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468

【CVE-2025-15556】請參考官方所列的影響版本 https://notepad-plus-plus.org//news//clarification-security-incident/

【CVE-2025-40536】請參考官方所列的影響版本 https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40536

【CVE-2026-1731】請參考官方所列的影響版本 https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

[建議措施:]

【CVE-2026-21513】 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-2026-21513

【CVE-2026-21525】 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-2026-21525

【CVE-2026-21510】 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-2026-21510

【CVE-2026-21533】 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-2026-21533

【CVE-2026-21519】 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-2026-21519

【CVE-2026-21514】 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-2026-21514

【CVE-2026-20700】 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/100100

【CVE-2024-43468】 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-2024-43468

【CVE-2025-15556】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://notepad-plus-plus.org//news//clarification-security-incident/

【CVE-2025-40536】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40536

【CVE-2026-1731】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

[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