國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-2026012808010202【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/01/19-2026/01/25)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026012808010202	發佈時間	2026-01-28 08:56:05
事故類型	ANA-漏洞預警	發現時間	2026-01-28 08:56:05
影響等級	低		

[主旨說明:]【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/01/19-2026/01/25)

[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-200-202601-00000024

【CVE-2026-20045】Cisco Unified Communications Products Code Injection Vulnerability (CVSS v3.1: 8.2)

【是否遭勒索軟體利用:未知】 Cisco Unified Communications Manager (Unified CM)、Cisco Unified Communications Manager Session Management Edition (Unified CM SME)、Cisco Unified Communications Manager IM Presence Service (Unified CM IM P)、Cisco Unity Connection 和 Cisco Webex Calling Dedicated Instance 中存在程式碼注入漏洞，可能使攻擊者取得底層作業系統的使用者層級存取權限，並進一步提升權限至 root。

【CVE-2025-68645】Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Synacor Zimbra Collaboration Suite（ZCS）存在 PHP 遠端檔案包含漏洞，可能允許遠端攻擊者透過向 /h/rest 端點發送特製請求，從而影響內部請求分發，包含 WebRoot 目錄中的任意檔案。

【CVE-2025-34026】Versa Concerto Improper Authentication Vulnerability (CVSS v3.1: 7.5)

【是否遭勒索軟體利用:未知】 Versa Concerto SD-WAN orchestration platform 的 Traefik 反向代理配置存在不當驗證漏洞，可能允許攻擊者存取管理端點。內部的 Actuator 端點可被利用來取得 Heap Dump 與追蹤日誌。

【CVE-2025-31125】Vite Vitejs Improper Access Control Vulnerability (CVSS v3.1: 5.3)

【是否遭勒索軟體利用:未知】 Vite Vitejs 存在不當存取控制漏洞，攻擊者可透過特定查詢參數存取未經授權檔案內容。僅將 Vite 開發伺服器對外開放（使用 --host 或 server.host 設定選項）的應用程式會受到影響。

【CVE-2025-54313】Prettier eslint-config-prettier Embedded Malicious Code Vulnerability (CVSS v3.1: 7.5)

【是否遭勒索軟體利用:未知】 Prettier eslint-config-prettier 存在嵌入式惡意程式碼漏洞。安裝受影響套件時，系統會執行 install.js 檔案，並在 Windows 系統上啟動惡意程式 node-gyp.dll。

【CVE-2024-37079】Broadcom VMware vCenter Server Out-of-bounds Write Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Broadcom VMware vCenter Server 在 DCERPC 通訊協定的實作中存在越界寫入漏洞。具備 vCenter Server 網路存取權限的惡意攻擊者，可能透過傳送特製的網路封包，進而導致遠端程式碼執行。

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-2026-20045】請參考官方所列的影響版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

【CVE-2025-68645】請參考官方所列的影響版本 https://wiki.zimbra.com/wiki/Security_Center

【CVE-2025-34026】請參考官方所列的影響版本 https://security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e

【CVE-2025-31125】請參考官方所列的影響版本 https://github.com/vitejs/vite/security/advisories/GHSA-4r4m-qw57-chr8

【CVE-2025-54313】請參考官方所列的影響版本 https://github.com/advisories/GHSA-f29h-pxvx-f335

【CVE-2024-37079】請參考官方所列的影響版本 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453

[建議措施:]

【CVE-2026-20045】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

【CVE-2025-68645】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://wiki.zimbra.com/wiki/Security_Center

【CVE-2025-34026】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e

【CVE-2025-31125】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/vitejs/vite/security/advisories/GHSA-4r4m-qw57-chr8

【CVE-2025-54313】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/advisories/GHSA-f29h-pxvx-f335

【CVE-2024-37079】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453

[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