國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-2026042704040909【漏洞預警】CISA新增14個已知遭駭客利用之漏洞至KEV目錄(2026/04/20-2026/04/26)(下)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026042704040909	發佈時間	2026-04-27 16:57:10
事故類型	ANA-漏洞預警	發現時間	2026-04-27 16:57:10
影響等級	低		

[主旨說明:]【漏洞預警】CISA新增14個已知遭駭客利用之漏洞至KEV目錄(2026/04/20-2026/04/26)(下)

[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-200-202604-00000028

【CVE-2024-27199】JetBrains TeamCity Relative Path Traversal Vulnerability (CVSS v3.1: 7.3)

【是否遭勒索軟體利用:已知】 JetBrains TeamCity 存在相對路徑遍歷漏洞，可能導致能夠執行有限的管理員操作。

【CVE-2026-33825】Microsoft Defender Insufficient Granularity of Access Control Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Microsoft Defender 存在存取控制粒度不足漏洞，可能使已授權的攻擊者在本機進行權限提升。

【CVE-2026-39987】Marimo Remote Code Execution Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Marimo 存在預驗證遠端程式碼執行漏洞，允許未經驗證的攻擊者取得 shell 存取權限並執行任意系統指令。

【CVE-2025-29635】D-Link DIR-823X Command Injection Vulnerability (CVSS v3.1: 7.2)

【是否遭勒索軟體利用:未知】 D-Link DIR-823X 存在指令注入漏洞，允許經授權的攻擊者透過對 /goform/set_prohibiting 發送 POST 請求，在遠端裝置上執行任意指令。受影響產品可能已達生命週期終止（EoL）或服務終止（EoS）階段。建議使用者停止使用該產品。

【CVE-2024-7399】Samsung MagicINFO 9 Server Path Traversal Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Samsung MagicINFO 9 Server 存在路徑遍歷漏洞，可能使攻擊者以系統權限寫入任意檔案。

【CVE-2024-57728】SimpleHelp Path Traversal Vulnerability (CVSS v3.1: 7.2)

【是否遭勒索軟體利用:未知】 SimpleHelp 存在路徑遍歷漏洞，允許管理員使用者透過上傳特製的 ZIP 檔案將任意檔案上傳至檔案系統的任何位置。此漏洞可被利用，使攻擊者以 SimpleHelp 伺服器使用者的身分在主機上執行任意程式碼。

【CVE-2024-57726】SimpleHelp Missing Authorization Vulnerability (CVSS v3.1: 9.9)

【是否遭勒索軟體利用:未知】 SimpleHelp 存在授權缺失漏洞，可能使低權限技術人員建立具有過高權限的 API 金鑰。這些 API 金鑰可被用來將權限提升至伺服器管理員角色。

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-2024-27199】請參考官方所列的影響版本 https://www.jetbrains.com/privacy-security/issues-fixed/

【CVE-2026-33825】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825

【CVE-2026-39987】請參考官方所列的影響版本 https://github.com/marimo-team/marimo/security/advisories/GHSA-2679-6mx9-h9xc

【CVE-2025-29635】 D-Link DIR-823X 240126、D-Link DIR-823X 240802

【CVE-2024-7399】請參考官方所列的影響版本 https://security.samsungtv.com/securityUpdates

【CVE-2024-57728】請參考官方所列的影響版本 https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

【CVE-2024-57726】請參考官方所列的影響版本 https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

[建議措施:]

【CVE-2024-27199】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.jetbrains.com/privacy-security/issues-fixed/

【CVE-2026-33825】 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-2026-33825

【CVE-2026-39987】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/marimo-team/marimo/security/advisories/GHSA-2679-6mx9-h9xc

【CVE-2025-29635】 受影響產品可能已達生命週期終止(EoL)或服務終止(EoS)階段，建議使用者停止使用該產品。

【CVE-2024-7399】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://security.samsungtv.com/securityUpdates

【CVE-2024-57728】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

【CVE-2024-57726】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

[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