

張貼日期：2026/05/13

【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)(上)

- 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)(上)
- 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-200-202604-00000027
 - [CVE-2026-20122] Cisco Catalyst SD-WAN Manager Incorrect Use of Privileged APIs Vulnerability (CVSS v3.1: 5.4)
 - 【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Manager 存在特權 API錯誤使用漏洞。攻擊者可透過在本機檔案系統上上傳惡意檔案來利用此漏洞。成功利用後，攻擊者能覆寫受影響系統上的任意檔案，並取得 vmanage 使用者權限。
 - [CVE-2026-20133] Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability (CVSS v3.1: 6.5)
 - 【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Manager 存在將敏感資訊暴露給未授權對象的漏洞，可能使遠端攻擊者得以檢視受影響系統上的敏感資訊。
 - [CVE-2025-2749] Kentico Xperience Path Traversal Vulnerability (CVSS v3.1: 7.2)
 - 【是否遭勒索軟體利用:未知】 Kentico Xperience 存在路徑遍歷漏洞，可能使已驗證使用者的 Staging Sync Server 將任意資料上傳至相對路徑位置。
 - [CVE-2023-27351] PaperCut NG/MF Improper Authentication Vulnerability (CVSS v3.1: 8.2)
 - 【是否遭勒索軟體利用:已知】 PaperCut NG/MF 存在不當驗證漏洞，可能使遠端攻擊者透過 SecurityRequestFilter 類別繞過受影響安裝的身分驗證。
 - [CVE-2025-48700] Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability (CVSS v3.1: 6.1)
 - 【是否遭勒索軟體利用:未知】 Synacor Zimbra Collaboration Suite (ZCS) 存在跨網站指令碼漏洞，可能使攻擊者在使用者工作階段中執行任意 JavaScript 進而導致未經授權存取敏感資訊。
 - [CVE-2026-20128] Cisco Catalyst SD-WAN Manager Storing Passwords in a Recoverable Format Vulnerability (CVSS v3.1: 7.5)
 - 【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Manager 存在將密碼以可還原格式儲存的漏洞，允許已驗證的本機攻擊者以低權限使用者身分存取檔案系統中 DCA 使用者的憑證檔案，進而取得 DCA 使用者權限。
 - [CVE-2025-32975] Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability (CVSS v3.1: 10.0)
 - 【是否遭勒索軟體利用:未知】 Quest KACE Systems Management Appliance [SMA] 存在不當驗證漏洞，可能使攻擊者在沒有有效憑證的情況下冒充合法使用者。
- 影響平台:
 - [CVE-2026-20122] 請參考官方所列的影響版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-authbp-qwCX8D4v>
 - [CVE-2026-20133] 請參考官方所列的影響版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-authbp-qwCX8D4v>
 - [CVE-2025-2749] Kentico Xperience 13.0.178(含)之前的版本
 - [CVE-2023-27351] 請參考官方所列的影響版本

- <https://www.papercut.com/kb/Main/PO-1216-and-PO-1219>
- [CVE-2025-48700] 請參考官方所列的影響版本
https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
- [CVE-2026-20128] 請參考官方所列的影響版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v>
- [CVE-2025-32975] 請參考官方所列的影響版本
<https://support.quest.com/kb/4379499/quest-response-to-kace-sma-vulnerabilities-cve-2025-32975-cve-2025-32976-cve-2025-32977-cve-2025-32978>
- 建議措施:
 - [CVE-2026-20122] 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-sdwan-authbp-qwCX8D4v>
 - [CVE-2026-20133] 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-sdwan-authbp-qwCX8D4v>
 - [CVE-2025-2749] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://devnet.kentico.com/download/hotfixes>
 - [CVE-2023-27351] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.papercut.com/kb/Main/PO-1216-and-PO-1219>
 - [CVE-2025-48700] 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/Zimbra_Security_Advisories
 - [CVE-2026-20128] 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-sdwan-authbp-qwCX8D4v>
 - [CVE-2025-32975] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://support.quest.com/kb/4379499/quest-response-to-kace-sma-vulnerabilities-cve-2025-32975-cve-2025-32976-cve-2025-32977-cve-2025-32978>

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/mailing:announcement:20260513_28

Last update: **2026/05/13 14:40**

