張貼日期：2026/03/03

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/02/23-2026/03/01)

- 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(2026/02/23-2026/03/01)

- 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-200-202603-00000001
  - 【CVE-2026-25108】Soliton Systems K.K FileZen OS Command Injection Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Soliton Systems K.K FileZen 存在作業系統指令注入漏洞，當使用者登入受影響產品並傳送特製的 HTTP 請求，即可能觸發此漏洞。
  - 【CVE-2022-20775】Cisco SD-WAN Path Traversal Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Cisco SD-WAN CLI 存在路徑遍歷漏洞。由於應用程式 CLI 內指令存取控制不當，經驗證的本機攻擊者可能藉此提升權限。成功利用此漏洞後，攻擊者可作為 root 使用者執行任意指令。
  - 【CVE-2026-20127】Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Controller【原 SD-WAN vSmart】與 Cisco Catalyst SD-WAN Manager【原 SD-WAN vManage】存在身分驗證繞過漏洞，可能使未經驗證的遠端攻擊者繞過驗證機制，並在受影響系統上取得管理權限。
- 影響平台:
  - 【CVE-2026-25108】請參考官方所列的影響版本 https://www.soliton.co.jp/support/2026/006657.html
  - 【CVE-2022-20775】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-priv-E6e8tEdF
  - 【CVE-2026-20127】請參考官方所列的影響版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
- 建議措施:
  - 【CVE-2026-25108】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.soliton.co.jp/support/2026/006657.html
  - 【CVE-2022-20775】 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-sd-wan-priv-E6e8tEdF
  - 【CVE-2026-20127】 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-rpa-EHchtZk

---

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:20260303_25

Last update: **2026/03/03 15:48**