

張貼日期：2025/03/25

# 【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/03/17-2025/03/23)

- 主旨說明: 【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/03/17-2025/03/23)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202503-00000011
  - [CVE-2025-30066] tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability (CVSS v3.1: 8.6)  
【是否遭勒索軟體利用:未知】 tj-actions/changed-files GitHub Action存在嵌入式惡意程式碼漏洞，遠端攻擊者可藉由讀取GitHub Actions工作流程日誌發現機密。這些機密可能包括但不限於有效的AWS存取金鑰、GitHub個人存取權限(PATs)、npm權限和RSA私鑰。  
【影響平台】tj-actions changed-files 46之前的版本
  - [CVE-2025-24472] Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability (CVSS v3.1: 9.8)  
【是否遭勒索軟體利用:是】 Fortinet FortiOS和FortiProxy存在身份驗證繞過漏洞，遠端攻擊者可通過製作的CSF代理請求獲得超級管理員權限。  
【影響平台】請參考官方所列的影響版本：<https://fortiguard.fortinet.com/psirt/FG-IR-24-535>
  - [CVE-2017-12637] SAP NetWeaver Directory Traversal Vulnerability (CVSS v3.1: 7.5)  
【是否遭勒索軟體利用:未知】 SAP NetWeaver應用伺服器Java在scheduler/ui/js/ffffffbca41eb4/UIUtilJavaScriptJS中存在目錄遍歷漏洞，遠端攻擊者可透過查詢字串中使用 .. 來讀取任意檔案。  
【影響平台】請參考官方所列的影響版本：<https://userapps.support.sap.com/sap/support/knowledge/en/3476549>
  - [CVE-2024-48248] NAKIVO Backup and Replication Absolute Path Traversal Vulnerability (CVSS v3.1: 8.6)  
【是否遭勒索軟體利用:未知】 NAKIVO Backup and Replication 存在絕對路徑遍歷漏洞，攻擊者能夠讀取任意檔案。  
【影響平台】請參考官方所列的影響版本：<https://helpcenter.nakivo.com/Knowledge-Base/Content/Security-Advisory/CVE-2024-48248.htm>
  - [CVE-2025-1316] Edimax IC-7100 IP Camera OS Command Injection Vulnerability (CVSS v3.1: 9.3)  
【是否遭勒索軟體利用:未知】 Edimax IC-7100 IP攝影機存在作業系統指令注入漏洞，攻擊者可透過特殊的請求檔執行遠端程式碼。  
【影響平台】請參考官方所列的影響版本：[https://www.edimax.com/edimax/post/post/data/edimax/global/press\\_releases/4801/](https://www.edimax.com/edimax/post/post/data/edimax/global/press_releases/4801/)
- 影響平台: 詳細內容於內容說明欄之影響平台
- 建議措施:
  - [CVE-2025-30066] 對應產品升級至以下版本(或更高) tj-actions changed-files 46.0.1
  - [CVE-2025-24472] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://fortiguard.fortinet.com/psirt/FG-IR-24-535>
  - [CVE-2017-12637] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://userapps.support.sap.com/sap/support/knowledge/en/3476549>
  - [CVE-2024-48248] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://helpcenter.nakivo.com/Knowledge-Base/Content/Security-Advisory/CVE-2024-48248.htm>
  - [CVE-2025-1316] 官方已針對漏洞釋出緩解措施

[https://www.edimax.com/edimax/post/post/data/edimax/global/press\\_releases/4801/](https://www.edimax.com/edimax/post/post/data/edimax/global/press_releases/4801/)

---

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/announcement:20250325\\_01](https://net.nthu.edu.tw/netsys/announcement:20250325_01)



Last update: **2025/03/26 11:07**