

張貼日期: 2026/10/08

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄 (2026/09/28-2026/10/04)

- 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 (2026/09/28-2026/10/04)
- 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-200-202610-00000002
 - CVE-2026-86950□Apple Multiple Products Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用: 未知】Apple iOS□macOS和iPadOS在CoreGraphics中存在越界寫入漏洞, 可能導致任意程式碼執行。
 - CVE-2026-76504□Cisco Catalyst SD-WAN Manager Hex Encoding Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用: 未知】Cisco Catalyst SD-WAN Manager存在十六進位編碼漏洞。由於對HTTP請求中的URI編碼處理不當, 未經驗證的遠端攻擊者可能利用此漏洞, 以管理員權限存取受影響的系統。
 - CVE-2026-104286□Fortinet FortiMail Path Traversal Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用: 未知】Fortinet FortiMail存在路徑遍歷漏洞, 可能導致未經驗證的攻擊者透過特製的HTTP或HTTPS請求, 在底層系統上寫入任意檔案。
 - CVE-2026-102490□Zammad GmbH Zammad Improper Privilege Management Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用: 未知】Zammad GmbH Zammad存在權限管理不當漏洞, 可能導致本機zammad使用者將權限提升至root□
 - CVE-2026-102489□Zammad GmbH Zammad Session Fixation Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用: 未知】Zammad GmbH Zammad存在Session Fixation漏洞, 可能導致攻擊者以zammad使用者身分遠端執行任意程式碼。
 - CVE-2026-88779□Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVSS v4.0: 8.7)
 - 【是否遭勒索軟體利用: 未知】Citrix NetScaler ADC及Citrix NetScaler Gateway存在記憶體緩衝區內操作限制不當漏洞, 可能導致阻斷服務。
- 影響平台:
 - CVE-2026-86950□請參考官方所列的影響版本 <https://support.apple.com/en-us/100100>
 - CVE-2026-76504□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-webauth-xr8beuuU>
 - CVE-2026-104286□請參考官方所列的影響版本 <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>
 - CVE-2026-102490□請參考官方所列的影響版本 <https://csirt.divd.nl/cves/CVE-2026-102490/>
 - CVE-2026-102489□請參考官方所列的影響版本 <https://csirt.divd.nl/cves/CVE-2026-102489/>
 - CVE-2026-88779□請參考官方所列的影響版本 <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174>
- 建議措施:

- [CVE-2026-86950] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://support.apple.com/en-us/100100>
 - [CVE-2026-76504] 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-webauth-xr8beuuU>
 - [CVE-2026-104286] 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-26-175>
 - [CVE-2026-102490] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://community.zammad.org/t/take-care-local-privilege-escalation-cve-2026-102490-is-reported-as-being-actively-exploited/21297/2>
 - [CVE-2026-102489] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://community.zammad.org/t/take-care-local-privilege-escalation-cve-2026-102490-is-reported-as-being-actively-exploited/21297/2>
 - [CVE-2026-88779] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174>
- 參考資料：

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:20261008_21

Last update: **2026/10/08 08:34**

