

張貼日期：2026/10/15

【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2026/10/05-2026/10/11)

- 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(2026/10/05-2026/10/11)
- 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-200-202610-00000021
 - [CVE-2015-5477]ISC BIND Data Processing Errors Vulnerability (CVSS v3.1: 7.5)
 - 【是否遭勒索軟體利用:未知】ISC BIND存在資料處理錯誤漏洞，遠端攻擊者可能透過發送TKEY查詢，導致阻斷服務。
 - [CVE-2016-3081]Apache Struts Command Injection Vulnerability (CVSS v3.1: 8.1)
 - 【是否遭勒索軟體利用:未知】Apache Struts存在指令注入漏洞，當啟用Dynamic Method Invocation功能時，遠端攻擊者可能透過method:prefix執行任意程式碼。
 - [CVE-2023-22894]Strapi Cleartext Storage of Sensitive Information Vulnerability (CVSS v3.1: 7.2)
 - 【是否遭勒索軟體利用:未知】Strapi存在明文儲存敏感資訊漏洞，具有管理面板存取權限的攻擊者可能透過查詢篩選器查閱敏感資訊。受影響產品可能已達產品生命週期終止[EoL]或服務終止[EoS]建議使用者停止使用或轉移至受支援版本。
 - [CVE-2021-3199]ONLYOFFICE Docs Server Path Traversal Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】ONLYOFFICE Docs存在路徑遍歷漏洞，當使用JWT時，攻擊者可能透過圖片上傳參數中的/..序列觸發此漏洞，進而導致遠端程式碼執行。
 - [CVE-2015-3306]ProFTPD Improper Access Control Vulnerability (CVSS v3.1: 10.0)
 - 【是否遭勒索軟體利用:未知】ProFTPD存在不當存取控制漏洞，遠端攻擊者可能透過SITE CPTO與SITE CPTO指令，讀取及寫入任意檔案。
- 影響平台:
 - [CVE-2015-5477]請參考官方所列的影響版本 <https://kb.isc.org/docs/aa-01272>
 - [CVE-2016-3081]請參考官方所列的影響版本 <https://cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032>
 - [CVE-2023-22894]請參考官方所列的影響版本 <https://github.com/advisories/GHSA-jjqf-j4w7-92w8>
 - [CVE-2021-3199]ONLYOFFICE Document Server 5.6.3 之前的版本
 - [CVE-2015-3306]請參考所列的影響版本 <https://lists.debian.org/debian-security-announce/2015/msg00154.html>
- 建議措施:
 - [CVE-2015-5477] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://kb.isc.org/docs/aa-01272>
 - [CVE-2016-3081] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032>
 - [CVE-2023-22894] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://github.com/advisories/GHSA-jjqf-j4w7-92w8>
 - [CVE-2021-3199] 對應產品升級至以下版本(或更高) ONLYOFFICE Document Server 5.6.3
 - [CVE-2015-3306] 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://lists.debian.org/debian-security-announce/2015/msg00154.html>
- 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/announcement:20261015_31



Last update: **2026/10/15 13:23**