

張貼日期：2026/06/24

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2026/06/15-2026/06/21)

- 主旨說明: 【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2026/06/15-2026/06/21)
- 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-200-202606-00000017
 - [CVE-2026-54420] LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability (CVSS v3.1: 8.5)
 - 【是否遭勒索軟體利用:未知】 LiteSpeed cPanel 外掛程式存在 UNIX 符號連結追蹤漏洞。在執行 CloudLinux/CageFS 的共享主機伺服器上，具 FTP 或 Web Shell 存取權限的使用者可能利用此漏洞進行未經授權操作。
 - [CVE-2026-20262] Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability (CVSS v3.1: 6.5)
 - 【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Manager 存在目錄或路徑遍歷漏洞。經身分驗證的遠端攻擊者可能利用此漏洞，在受影響系統的檔案系統中建立檔案或覆寫任意檔案。
 - [CVE-2026-48907] Widget Factory Joomla Content Editor Improper Access Control Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 Widget Factory Joomla Content Editor 存在不當存取控制漏洞，可能導致未經身份驗證的使用者透過建立新的編輯器設定檔，上傳並執行 PHP 程式碼。
 - [CVE-2026-20253] Splunk Enterprise Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 Splunk Enterprise 存在關鍵功能缺乏身分鑑別漏洞。未經驗證的使用者可透過 PostgreSQL Sidecar 服務端點建立或截斷任意檔案。
- 影響平台:
 - [CVE-2026-54420] 請參考官方所列的影響版本
<https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/>
 - [CVE-2026-20262] 請參考官方所列的影響版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ>
 - [CVE-2026-48907] 請參考官方所列的影響版本
<https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites>
 - [CVE-2026-20253] 請參考官方所列的影響版本
<https://advisory.splunk.com/advisories/SVD-2026-0603>
- 建議措施:
 - [CVE-2026-54420] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/>
 - [CVE-2026-20262] 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-arbfw-c2rZvQ>
 - [CVE-2026-48907] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites>

- [CVE-2026-20253] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://advisory.splunk.com/advisories/SVD-2026-0603>
-

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:20260624_24



Last update: **2026/06/24 16:35**