

張貼日期：2025/12/10

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/12/01-2025/12/07) (CVE-2025-48633) (CVE-2025-48572) (CVE-2021-26828) (CVE-2025-55182)

- 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(2025/12/01-2025/12/07) (CVE-2025-48633) (CVE-2025-48572) (CVE-2021-26828) (CVE-2025-55182)
- 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-200-202512-00000002
 - [CVE-2025-48633]Android Framework Information Disclosure Vulnerability (CVSS : 暫無)
 - 【是否遭勒索軟體利用:未知】Android Framework 存在未具體說明的漏洞，可能導致資訊外洩。
 - [CVE-2025-48572]Android Framework Privilege Escalation Vulnerability (CVSS : 暫無)
 - 【是否遭勒索軟體利用:未知】Android Framework 存在未具體說明的漏洞，可能導致權限提升。
 - [CVE-2021-26828]OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】OpenPLC ScadaBR 存在未受限制的危險類型檔案上傳漏洞，允許經身份驗證的遠端使用者透過 view_edit.shtm 上傳並執行任意 JSP 檔案。
 - [CVE-2025-55182]Meta React Server Components Remote Code Execution Vulnerability (CVSS v3.1: 10.0)
 - 【是否遭勒索軟體利用:未知】Meta React Server Components 存在遠端程式碼執行漏洞，攻擊者可透過利用 React 在解碼傳送至 React Server Function 端點的有效負載時的缺陷，在未經身份驗證的情況下實現遠端程式碼執行。
- 影響平台:
 - [CVE-2025-48633]請參考官方所列的影響版本
<https://source.android.com/docs/security/bulletin/2025-12-01>
 - [CVE-2025-48572]請參考官方所列的影響版本
<https://source.android.com/docs/security/bulletin/2025-12-01>
 - [CVE-2021-26828]OpenPLC ScadaBR Linux 0.9.1(含)之前的版本 OpenPLC ScadaBR Windows 1.12.4(含)之前的版本
 - [CVE-2025-55182]請參考官方所列的影響版本
<https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components>
- 建議措施:
 - [CVE-2025-48633]官方已針對漏洞釋出修復更新，請更新至相關版本
<https://source.android.com/docs/security/bulletin/2025-12-01>
 - [CVE-2025-48572]官方已針對漏洞釋出修復更新，請更新至相關版本
<https://source.android.com/docs/security/bulletin/2025-12-01>
 - [CVE-2021-26828]對應產品升級至以下版本(或更高) OpenPLC ScadaBR Linux 0.9.1(不含)之後的版本 OpenPLC ScadaBR Windows 1.12.4(不含)之後的版本
 - [CVE-2025-55182]官方已針對漏洞釋出修復更新，請更新至相關版本

<https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components>

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:20251210_02



Last update: **2025/12/10 14:58**