**POSTING DATE: 2025/12/10**

# [VULNERABILITY ALERT] CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/12/01-2025/12/07) (CVE-2025-48633) (CVE-2025-48572) (CVE-2021-26828) (CVE-2025-55182)

- Subject: [VULNERABILITY ALERT] CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/12/01-2025/12/07) (CVE-2025-48633) (CVE-2025-48572) (CVE-2021-26828) (CVE-2025-55182)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202512-00000002
  - [CVE-2025-48633] Android Framework Information Disclosure Vulnerability (CVSS : None)
  - [Exploited by Ransomware: Unknown] Android Framework contains an unspecified vulnerability that may lead to information disclosure.
  - [CVE-2025-48572] Android Framework Privilege Escalation Vulnerability (CVSS : None)
  - [Exploited by Ransomware: Unknown] Android Framework contains an unspecified vulnerability that may lead to privilege escalation.
  - [CVE-2021-26828] OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 8.8)
  - [Exploited by Ransomware: Unknown] OpenPLC ScadaBR contains an Unrestricted Upload of File with Dangerous Type vulnerability, allowing an authenticated remote user to upload and execute arbitrary JSP files via view_edit.shtm.
  - [CVE-2025-55182] Meta React Server Components Remote Code Execution Vulnerability (CVSS v3.1: 10.0)
  - [Exploited by Ransomware: Unknown] Meta React Server Components contains a Remote Code Execution vulnerability, allowing an unauthenticated attacker to achieve remote code execution by exploiting a flaw in React's decoding of payloads sent to a React Server Function endpoint.
- Affected Platforms:
  - [CVE-2025-48633] Please refer to the affected versions listed officially https://source.android.com/docs/security/bulletin/2025-12-01
  - [CVE-2025-48572] Please refer to the affected versions listed officially https://source.android.com/docs/security/bulletin/2025-12-01
  - [CVE-2021-26828] OpenPLC ScadaBR Linux versions prior to and including 0.9.1, OpenPLC ScadaBR Windows versions prior to and including 1.12.4
  - [CVE-2025-55182] Please refer to the affected versions listed officially https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
- Recommended Actions:

  - [CVE-2025-48633] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://source.android.com/docs/security/bulletin/2025-12-01
  - [CVE-2025-48572] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://source.android.com/docs/security/bulletin/2025-12-01
  - [CVE-2021-26828] Update the corresponding product to the following versions (or later): OpenPLC ScadaBR Linux versions later than 0.9.1 (exclusive), OpenPLC ScadaBR Windows versions later than 1.12.4 (exclusive)
  - [CVE-2025-55182] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

---

Computer and Communication Center
Network Systems Division, Respectfully

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
**https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251210_02**

Last update: **2025/12/10 15:05**