POSTING DATE: 2025/12/17

[VULNERABILITY ALERT] Critical Security Vulnerability in Meta's React Server Components (CVE-2025-55182)

- Subject: [VULNERABILITY ALERT] Critical Security Vulnerability in Meta's React Server Components (CVE-2025-55182)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000006
  - React is an open-source JavaScript library developed by Meta for building user interfaces.
  - Recently, Meta released a critical security vulnerability advisory (CVE-2025-55182, CVSS: 10.0), stating that a Remote Code Execution (RCE) vulnerability exists in React Server Components. Due to a security weakness in how React parses data sent to React Server Function endpoints, an unauthenticated attacker could potentially trigger arbitrary code execution via a specially crafted payload.
- Affected Platforms:
  - react-server-dom-webpack versions 19.0, 19.1.0, 19.1.1, 19.2.0
  - react-server-dom-parcel versions 19.0, 19.1.0, 19.1.1, 19.2.0
  - react-server-dom-turbopack versions 19.0, 19.1.0, 19.1.1, 19.2.0
  - Affected React frameworks and bundlers include: next, react-router, waku, @parcel/rsc, @vitejs/plugin-rsc, and rwsdk.
- Recommended Actions:
  - Apply patches according to the solutions released on the official website: 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:20251217_03

Last update: **2025/12/17 13:50**