مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in React Router

Tracking #:432318231

Date:12-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in React Router and Remix server-side components, exposing affected applications to unauthorized server file system access through improper session storage handling.

TECHNICAL DETAILS:

A critical security vulnerability (CVE-2025-61686, CVSS 9.1) has been identified in React Router and Remix server-side components, exposing affected applications to unauthorized server file system access through improper session storage handling. This flaw poses a serious risk of sensitive file exposure and server-side compromise, particularly in applications using file-based session storage with unsigned cookies. In addition to the critical issue, multiple high-severity vulnerabilities have been disclosed, including several Cross-Site Scripting (XSS) flaws, open redirect weaknesses, and a CSRF vulnerability affecting server-side route actions. These issues collectively enable client-side code execution, phishing attacks, session hijacking, and unauthorized state-changing requests.

Critical Vulnerability Details

- **CVE ID**: CVE-2025-61686- Unauthorized file access when using `createFileSessionStorage()` with unsigned cookies
- **Severity**: Critical
- CVSS: 9.1
- Component: createFileSessionStorage()
- Attack Type: Path traversal / file manipulation

Affected versions:

- react-router/node (npm) >= 7.0.0, <=7.9.3
- remix-run/deno (npm) <=2.17.1
- remix-run/node (npm) <=2.17.1

Patched versions:

- react-router/node (npm)>=7.9.4
- remix-run/deno (npm) >=2.17.2
- remix-run/node (npm) >=2.17.2

High-Severity XSS Vulnerabilities

- CVE-2025-59057 (CVSS 7.6) – A Server-Side Rendering (SSR) XSS vulnerability in the Meta component allows arbitrary JavaScript execution when untrusted input is used to generate script:ld+json tags.
- ScrollRestoration XSS (CVSS 8.2) – An XSS vulnerability in the <ScrollRestoration> API enables script execution during SSR when attacker-controlled values are passed via the getKey or storageKey properties.
- CVE-2026-22029 (CVSS 8.0) – An open redirect–based XSS issue allows unsafe JavaScript execution through malicious URLs originating from SPA loaders or action-based navigation.

Medium-Severity Logic Flaws

- CVE-2026-22030 (Medium) – A Cross-Site Request Forgery (CSRF) vulnerability allows unauthorized document POST requests when using server-side route action handlers in

Framework Mode.

- CVE-2025-68470 (Medium) – An external redirect flaw allows attacker-supplied paths to force navigation to untrusted external URLs via navigate(), <Link>, or redirect().

RECOMMENDATIONS:

- Refer to the official React Router security advisory to identify all affected components, and immediately update React Router and related @remix-run packages to the appropriate fixed versions to fully remediate the identified critical and high-severity vulnerabilities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/remix-run/react-router/security/advisories/GHSA-9583-h5hc-x8cw