مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Denial of Service (DoS) Vulnerability in React Server Components

Tracking #:432318757

Date:09-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity Denial of Service (DoS) vulnerability has been identified in React Server Components, tracked as CVE-2026-23869.

TECHNICAL DETAILS:

A high-severity Denial of Service (DoS) vulnerability has been identified in React Server Components, tracked as CVE-2026-23869. The flaw allows attackers to trigger excessive CPU utilization on the server via crafted HTTP requests targeting Server Function endpoints.

Vulnerability Details:

- CVE ID: CVE-2026-23869
- Type: Denial of Service (DoS)
- CVSS Score: 7.5 (High)
- Affected Component: React Server Components (Server Functions)
- Attack Vector: Remote (via HTTP requests)
- Impact: CPU exhaustion → service degradation or outage

Affected versions

- Next.js >=13.0.0 < 15.5.15, >= 16.0 < 16.2.3

Applications are vulnerable if they use any of the following:

- react-server-dom-webpack
- react-server-dom-parcel
- react-server-dom-turbopack
  - 19.0.0 → 19.0.4
  - 19.1.0 → 19.1.5
  - 19.2.0 → 19.2.4

Patched versions

- Next.js 15.5.15, 16.2.3
- React Server
  - 19.0.5
  - 19.1.6
  - 19.2.5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade React packages immediately to patched versions.

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/vercel/next.js/security/advisories/GHSA-q4gf-8mx6-v5v3
- https://github.com/facebook/react/security/advisories/GHSA-479c-33wc-g2pg