مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Next.js

Tracking #:432317335

Date:02-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Next.js framework. This flaw allows attackers to exploit the development server via Cross-site WebSocket Hijacking (CSWSH), potentially exposing sensitive application source code.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-48068) has been identified in the Next.js development server affecting versions 13.0.0 through 15.2.1 when the App Router feature is enabled. This flaw allows attackers to exploit Cross-site WebSocket Hijacking (CSWSH) to potentially access sensitive application source code during local development.

Vulnerability Details:

- **CVE-2025-48068**
- CVSS Score 2.3 LOW
- **Vulnerability Type:** Cross-site WebSocket Hijacking (CSWSH)
- **Attack Vector:** Local development environment only (does not affect production deployments)
- The vulnerability arises from inadequate origin verification in the WebSocket server of the Next.js development environment. When the development server is running, a malicious website can establish a WebSocket connection to the localhost and access the source code of projects using the App Router feature. This can lead to unauthorized exposure of proprietary code or sensitive logic.
- Exploitation of this vulnerability can lead to:
  - Confidentiality: Attackers may access and exfiltrate application source code.
- **Affected Software:** Next.js (npm/next)
- **Affected Versions:** 13.0.0 to 15.2.1 (with App Router enabled)
- **Fixed Version:** 15.2.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Next.js.

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://nvd.nist.gov/vuln/detail/CVE-2025-48068