مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Next.js

Tracking #:432316311

Date:20-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Next.js, a popular web development framework. This vulnerability can lead to cache poisoning attacks, potentially compromising the integrity of web applications.

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2024-46982
- **CVSS Score:** 7.5 **Severity:** High
- A cache poisoning vulnerability exists in Next.js that allows an attacker to manipulate the cache of non-dynamic server-side rendered routes. By sending a specially crafted HTTP request, an attacker can coerce Next.js to cache a route that should not be cached. This can result in sensitive or unexpected data being exposed to unauthorized users.
- Successful exploitation of this vulnerability can lead to data exposure, where sensitive or unauthorized data may be exposed to attackers, or denial of service, where the vulnerability could lead to a denial of service (DoS) attack.

Affected Versions:

- Next.js versions between 13.5.1 and 14.2.9

Affected Configurations:

- Router: Using the pages router
- Routes: Using non-dynamic server-side rendered routes e.g. pages/dashboard.tsx not pages/blog/[slug].tsx

Fixed Versions:

- Next.js version 13.5.7, 14.2.10, or later

The following configurations are not affected:

- Deployments using only the app router
- Deployments on Vercel

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-46982