مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Next.js

Tracking #:432316655
Date:20-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Next.js, a widely-used React framework for web application development. This vulnerability could potentially be exploited to gain unauthorized access to affected system.

TECHNICAL DETAILS:

Vulnerabilities Details:

- CVE-2024-51479
- CVSS Score: 7.5 High
- The vulnerability allows unauthorized access to pages directly under the root directory of a Next.js application when authorization is performed in middleware based on pathname. This bypass could potentially expose sensitive application data to attackers.
- Attackers could gain unauthorized access to root-level pages in vulnerable Next.js applications, even if these pages were intended to be protected by authorization checks

Affected Versions:

- Next.js versions 9.5.5 through 14.2.14.

Fixed Versions:

- Next.js version 14.2.15 or later

For applications hosted on Vercel, the vulnerability has been automatically mitigated regardless of the Next.js version

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-2024-51479