مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Denial-of-Service Vulnerability in Next.js

Tracking #:432316706

Date:06-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Next.js that could be exploited to execute Denial of Service (DoS) attacks on affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2024-56332**
- CVSS Base Score: 5.3 MEDIUM
- A security vulnerability exists in Next.js, affecting the Server Actions feature. This vulnerability allows attackers to execute Denial of Service (DoS) attacks against applications using Server Actions.
- The vulnerability enables attackers to craft requests that cause Server Actions to hang indefinitely until the hosting provider terminates the function execution. While the Next.js server remains idle during these attacks, keeping connections open with low CPU and memory usage, it can lead to service disruption and potential excessive billing for deployments lacking protection against long-running Server Action invocations
- Successful exploitation of this vulnerability can result in:
    - **Denial of Service:** Legitimate users may be prevented from accessing the application.
    - **Resource Exhaustion:** Server resources may be tied up, affecting overall application performance.
    - **Potential Financial Impact:** Deployments without proper safeguards may face excessive billing due to prolonged function executions.

Affected Versions:

- Next.js versions >= 13.0.0 < 14.2.21
- Next.js versions >= 15.0.0 < 15.1.1

Fixed Versions:

- Next.js 15.1.2
- Next.js 14.2.21
- Next.js 13.5.8

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2024-56332