مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Authorization Bypass Vulnerability in Next.js Middleware

Tracking #:432317005

Date:24-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability in Next.js middleware allows attackers to bypass authorization logic, granting unauthorized access to protected application routes and resources.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-29927) has been identified in Next.js middleware, allowing attackers to bypass authorization logic and gain unauthorized access to protected areas of applications. This flaw impacts a core security feature used by developers to enforce access control, session validation, and authentication. With Next.js being downloaded nearly 10 million times weekly, this vulnerability poses a significant risk to organizations across critical sectors, including banking, healthcare, and blockchain.

Vulnerability Details:

- CVE ID: CVE-2025-29927
- CVSS Score: 9.1 (Critical)
- Affected Versions:
  - 11.1.4 <=13.5.6
  - 14.0 <14.2.25
  - 15.0 <15.2.3
- Patched Versions: 14.2.25 and 15.2.3
- Impact: Authorization bypass leading to unauthorized access to protected resources.
- Exploit Complexity: Low (no authentication or user interaction required).
- Indicators of Compromise (IOCs):
  - Suspicious requests containing the x-middleware-subrequest header.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to immediately upgrade Next.js Middleware to the 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-f82v-jwr5-mffw