مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Axios

Tracking #:432318771

Date:13-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability (CVE-2026-40175) has been disclosed in Axios, a widely used HTTP client in Node.js and browser environments.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2026-40175) has been disclosed in Axios, a widely used HTTP client in Node.js and browser environments that enables attackers to escalate prototype pollution vulnerabilities in other dependencies into Remote Code Execution (RCE) or full cloud environment compromise.

Vulnerability Overview

- CVE ID: CVE-2026-40175
- Severity: Critical (CVSS -10.0)
- Affected Package: axios (npm)
- Type: Header Injection → Request Smuggling → SSRF escalation
- CWE: CWE-113 (Improper Neutralization of CRLF Sequences)
- Affected Component: lib/adapters/http.js (header processing logic)
- Proof of Concept: Available
- Affected Versions: All versions < 1.13.2
- Patched Version : >= 1.15.0
- Short-Term Mitigations: Apply Header Validation Patch

RECOMMENDATIONS:

Immediate Actions:

- Upgrade Axios Immediately to fixed version.

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/axios/axios/security/advisories/GHSA-fvcv-3m26-pcqx