مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Node.js

Tracking #:432317280

Date:16-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Node.js that could be exploited for denial of service, unauthorized access, or memory exhaustion on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

1. Async Crypto Operations Crash (CVE-2025-23166)
   - **Severity:** High
   - **Description:** Improper error handling in asynchronous cryptographic operations may cause Node.js to crash when processing untrusted input. This can be exploited remotely to cause a denial of service.
   - **Affected Versions:** 20.x, 22.x, 23.x, 24.x
2. HTTP Header Parsing Flaw (CVE-2025-23167)
   - **Severity:** Medium
   - **Description:** A flaw in the HTTP parser (llhttp) allows improper termination of HTTP/1 headers, enabling HTTP request smuggling attacks and bypassing proxy-based access controls.
   - **Affected Versions:** 20.x (prior to llhttp v9)
3. Memory Leak in File Reading (CVE-2025-23165)
   - **Severity:** Low
   - **Description:** A corrupted pointer in the ReadFileUtf8 binding results in an unrecoverable memory leak, leading to denial of service over time.
   - **Affected Versions:** 20.x, 22.x

Exploitation of this vulnerability can lead to:

- **Denial of Service:** Remote attackers can crash Node.js processes or exhaust system memory.
- **Unauthorized Access:** Attackers may bypass security controls via HTTP request smuggling.
- **Service Disruption:** Critical services relying on Node.js may be interrupted.

Fixed Versions:

- Node.js v20.19.2
- Node.js v22.15.1
- Node.js v23.11.1
- Node.js v24.0.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Node.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://nodejs.org/en/blog/vulnerability/may-2025-security-releases