مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Node.js

Tracking #:432316772

Date:22-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that The Node.js project released important security updates across multiple release lines to address a one high-severity and two medium-severity issues.

TECHNICAL DETAILS:

The Node.js project released important security updates across multiple release lines to address a one high-severity and two medium-severity issues that could potentially lead to unauthorized access, data leaks, or denial-of-service conditions if exploited. Additionally, CVEs have been issued for end-of-life (EOL) Node.js versions, emphasizing the importance of using supported releases.

Vulnerability Overview:

1. **CVE-2025-23083 – Worker Permission Bypass (High Severity)**
   - Affected Versions: Node.js v20.x, v22.x, v23.x
   - Description: A high-severity flaw in the diagnostics_channel utility allows attackers to hook into events such as worker thread creation. By exploiting this vulnerability, an attacker could potentially gain unauthorized access to worker thread instances, bypassing security controls and accessing sensitive data or resources that should be restricted. This poses a significant risk in applications relying on the Permission Model to isolate worker permissions and maintain security boundaries between threads.
2. **CVE-2025-23084 – Path Traversal by Drive Name in Windows Environments (Medium Severity)**
   - Affected Versions: Node.js v18.x, v20.x, v22.x, v23.x
   - Description: This vulnerability impacts Windows users of the path.join API. On Windows, path names not starting with a file separator are treated as relative paths. This flaw could allow attackers to exploit the handling of drive names in paths, potentially enabling them to access files outside the intended directory, resulting in unauthorized file access.
3. **CVE-2025-23085 – Memory Leak in HTTP/2 Servers (Medium Severity)**
   - Affected Versions: Node.js v18.x, v20.x, v22.x, v23.x
   - Description: A memory leak vulnerability in the HTTP/2 server implementation could lead to performance degradation and potential denial-of-service (DoS) conditions. If exploited, this flaw could exhaust system resources, leading to application crashes or service outages.
4. **End-of-Life (EOL) Versions**
   - **CVE-2025-23087: Node.js v17.x or earlier (EOL)**
   - **CVE-2025-23088: Node.js v19.x (EOL)**
   - **CVE-2025-23089: Node.js v21.x (EOL)**
   - Description: Several vulnerabilities have been discovered in Node.js versions that have reached end-of-life status, including v17.x, v19.x, and v21.x. These versions no longer receive security patches, leaving users vulnerable to unaddressed risks. Users of these versions are urged to upgrade to supported releases immediately.

Fixed Versions:

- Node.js v18.20.6
- Node.js v20.18.2
- Node.js v22.13.1
- Node.js v23.6.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to ensure Node.js installations are updated to the fixed versions.

Upgrade End-of-Life Versions to a supported version, as these EOL versions no longer receive security patches.

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/january-2025-security-releases