Vulnerability and Severity Report

1. Node.js < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 - Multiple Vulnerabilities

Severity: Critical

CVSS v3.0 Base Score: 8.8

Details:

- Improper environment variable handling.

- HTTP/2 DoS via header parsing issues.

- File permission model bypass.

- Privilege escalation with setuid().

- Crypto library padding flaws.

2. Node.js < 18.20.1 / 20.12.1 / 21.7.2 - Multiple Vulnerabilities

Severity: High

CVSS v3.0 Base Score: 8.2

Details:

- HTTP/2 server race condition (DoS risk).

- HTTP header parsing flaws (request smuggling).

3. Node.js < 18.20.4 / 20.15.1 / 22.4.1 - Multiple Vulnerabilities

Severity: High

CVSS v3.0 Base Score: 8.1

Details:

- Remote execution via child_process.spawn.

- Permission model bypass using --allow-* flags.

- Directory traversal due to double backslashes.

4. Node.js < 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 - Multiple Vulnerabilities

Severity: High

CVSS v3.0 Base Score: 7.7

Details:

- Memory leaks during abnormal connection termination.

- Worker threads exposure.

- Drive name handling on Windows.

5. Node.js < 20.19.2 / 22.15.1 / 23.11.1 / 24.0.2 - Multiple Vulnerabilities

Severity: Medium

CVSS v3.0 Base Score: 6.2

Details:

- Memory leak via ReadFileUtf8.

- Crashes due to unsafe cryptographic operations.

- HTTP request smuggling.

6. Python Tornado < 6.5.0 - DoS

Severity: High

CVSS v3.0 Base Score: 7.5

Details:

- DoS via malformed multi-part data parsing.

- Logging subsystem is synchronous, worsening DoS.

7. SSL Certificate Cannot Be Trusted

Severity: Medium

CVSS v3.0 Base Score: 6.5

Details:

- Self-signed or untrusted certificate authority.

- Certificate expired or not valid yet.

- Invalid signature on certificate.