Severity

High

Analysis Summary

CVE-2022-25844 CVSS:5.3

Node.js Angular module is vulnerable to a denial of service, caused by a regular expression denial of service (ReDoS) flaw in posPre: ‘ ‘.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre. By sending a specially-crafted regex input, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-29078 CVSS:9.8

Node.js ejs module could allow a remote attacker to execute arbitrary code on the system, caused by a server-side template injection flaw in settings[view options][outputFunctionName]. By sending a specially-crafted HTTP request to overwrites the outputFunctionName option with an arbitrary OS command, an attacker could exploit this vulnerability to execute arbitrary code on the system.

Impact

- Denial of Service
- Code Execution

Indicators Of Compromise

CVE

- CVE-2022-25844
- CVE-2022-29078

Affected Vendors

- Node.js

Affected Products

- Node.js angular 1.8.3
- Node.js ejs 3.1.6

Remediation

Upgrade to the latest version of Node.js, available from the Node.js Website.

CVE-2022-25844 CVE-2022-29078