# CVE Detail – CVE-2020-8287

Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request (for example, two Transfer-Encoding header fields). In this case, Node.js identifies the first header field and ignores the second. This can lead to HTTP Request Smuggling.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.92257

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

## CAPEC(s)

* CAPEC-273: HTTP Response Smuggling
* CAPEC-33: HTTP Request Smuggling

## Affected Products

* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:33:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:graalvm:19.3.4:\*:\*:\*:enterprise:\*:\*:\*
* cpe:2.3:a:oracle:graalvm:20.3.0:\*:\*:\*:enterprise:\*:\*:\*
* cpe:2.3:a:siemens:sinec\_infrastructure\_network\_services:\*:\*:\*:\*:\*:\*:\*:\*