# CVE Detail – CVE-2018-12116

Node.js: All versions prior to Node.js 6.15.0 and 8.14.0: HTTP request splitting: If Node.js can be convinced to use unsanitized user-provided Unicode data for the `path` option of an HTTP request, then data can be provided which will trigger a second, unexpected, and user-defined HTTP request to made to the same server.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.71232

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-115: Misinterpretation of Input

## Affected Products

* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:a:nodejs:node.js:\*:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:suse:suse\_enterprise\_storage:4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux\_enterprise\_server:12:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux\_enterprise\_server:15:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_openstack\_cloud:7:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_openstack\_cloud:8:\*:\*:\*:\*:\*:\*:\*