# CVE Detail – CVE-2017-16021

uri-js is a module that tries to fully implement RFC 3986. One of these features is validating whether or not a supplied URL is valid or not. To do this, uri-js uses a regular expression, This regular expression is vulnerable to redos. This causes the program to hang and the CPU to idle at 100% usage while uri-js is trying to validate if the supplied URL is valid or not. To check if you're vulnerable, look for a call to `require("uri-js").parse()` where a user is able to send their own input. This affects uri-js 2.1.1 and earlier.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.44365

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1333: Inefficient Regular Expression Complexity
* CWE-400: Uncontrolled Resource Consumption

## CAPEC(s)

* CAPEC-147: XML Ping of the Death
* CAPEC-227: Sustained Client Engagement
* CAPEC-492: Regular Expression Exponential Blowup

## ATT&CK Techniques

* T1499: Endpoint Denial of Service

## Used By (Actors/Tools)

* OnionDuke (malware)
* ZxShell (malware)
* Sandworm Team (intrusion-set)

## Affected Products

* cpe:2.3:a:garycourt:uri-js:\*:\*:\*:\*:\*:node.js:\*:\*