# CVE Detail – CVE-2021-21317

uap-core in an open-source npm package which contains the core of BrowserScope's original user agent string parser. In uap-core before version 0.11.0, some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This is fixed in version 0.11.0. Downstream packages such as uap-python, uap-ruby etc which depend upon uap-core follow different version schemes.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.80135

## CVSS Scoring

CVSS v3.1 Score: 5.3

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:uap-core\_project:uap-core:\*:\*:\*:\*:\*:node.js:\*:\*