b-c-ds / **CVE-2021-27292-ua-parser-js.txt**

Created last year

☆ Star

cve-2021-27292

CVE-2021-27292-ua-parser-js.txt

```
Doyensec Vulnerability Advisory
CVE-2021-27292
======================================================================
* Regular Expression Denial of Service (REDoS) in ua-parser-js
* Affected Product: ua-parser-js >= 0.7.14, fixed in 0.7.24
* Vendor: https://github.com/faisalman
* Severity: Medium
* Vulnerability Class: Denial of Service
* Status: Fixed
* Author(s): Ben Caller (Doyensec)
======================================================================

=== SUMMARY ===

The npm package ua-parser-js uses a regular expression which is vulnerable to Regular Expression Denial of Service (REDoS).
If an attacker provides a malicious User-Agent header, ua-parser-js can get stuck processing for a long time.

=== TECHNICAL DESCRIPTION ===

The vulnerable regular expression is found in src/ua-parser.js on line 620 (version 0.7.23):

    /android.+[;\/]\s+(Barnes[&\s]+Noble\s+|BN[RT])(V?.*)\s+build/

The section (Barnes[&\s]+Noble\s+|BN[RT])(V?.*)\s+ can be simplified as

    Noble\s+(.*)\s+

showing that it contains three infinitely repeating groups which all match space character. A long string of spaces can cause catastrophic
The complexity is cubic, so doubling the length of the malicious string of spaces makes processing take 8 times as long.

When used on a server, the payload will be constrained by the server's maximum header length.

=== REPRODUCTION STEPS ===

require('ua-parser-js')('android0/ Barnes&Noble' + ' '.repeat(5432) + '!')

To attack a server, set the User-Agent header to 'android0/ Barnes&Noble            !' but with more spaces.

Doubling the length of the string of spaces will make processing take 8 times as long.

=== REMEDIATION ===

Fix the vulnerable regular expression.

A potential fix is to replace (V?.*) with (\S.*\S) or (\S(?:.*\S)?), so that a long string of spaces does not match multiple groups.

=== DISCLOSURE TIMELINE ===

2021-02-05: Vulnerability disclosed via email to maintainers
2021-02-06: Acknowlegement from maintainer
2021-02-12: Fixed in 0.7.24: https://github.com/faisalman/ua-parser-js/commit/809439e20e273ce0d25c1d04e111dcf6011eb566

======================================================================

Doyensec (www.doyensec.com) is an independent security research
and development company focused on vulnerability discovery and
remediation. We work at the intersection of software development
and offensive engineering to help companies craft secure code.

Copyright 2021 by Doyensec LLC. All rights reserved.

Permission is hereby granted for the redistribution of this
advisory, provided that it is not altered except by reformatting
it, and that due credit is given. Permission is explicitly given
for insertion in vulnerability databases and similar, provided
that due credit is given. The information in the advisory is
believed to be accurate at the time of publishing based on
currently available information, and it is provided as-is,
as a free service to the community by Doyensec LLC. There are
no warranties with regard to this information, and Doyensec LLC
does not accept any liability for any direct, indirect, or
consequential loss or damage arising from use of, or reliance
on, this information.
```