

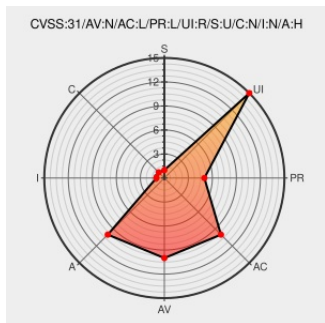


CVE-2020-26256

Published on: 12/08/2020 12:00:00 AM UTC

Last Modified on: 10/07/2021 05:08:00 PM UTC

CVE-2020-26256 - advisory for GHSA-8cv5-p934-3hwp

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Fast-csv](#) from [C2fo](#) contain the following vulnerability:

Fast-csv is an npm package for parsing and formatting CSVs or any other delimited value file in node. In fast-csv before version 4.3.6 there is a possible ReDoS vulnerability (Regular Expression Denial of Service) when using ignoreEmpty option when parsing. This has been patched in `v4.3.6` You will only be affected by this if you use the

`ignoreEmpty` parsing option. If you do use this option it is recommended that you upgrade to the latest version `v4.3.6` This vulnerability was found using a CodeQL query which identified `EMPTY\_ROW\_REGEX` regular expression as vulnerable.

CVE-2020-26256 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **C2FO** - **fast-csv** version < 4.3.6

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Security Issue: Request for contact · Issue #540 · C2FO/fast-csv · GitHub	Third Party Advisory github.com text/html	MISC github.com/C2FO/fast-csv/issues/540
fix: Simplify empty row check by removing complex regex · C2FO/fast-csv@4bbd39f · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/C2FO/fast-csv/commit/4bbd39f26a8cd7382151ab4f5fb102234b2f829e
fast-csv	Product Third Party Advisory www.npmjs.com text/html	MISC www.npmjs.com/package/fast-csv
@fast-csv/parse - npm	Product Third Party Advisory www.npmjs.com text/html	MISC www.npmjs.com/package/@fast-csv/parse
Problem loading page	Exploit Third Party Advisory lgtm.com text/html	MISC lgtm.com/query/8609731774537641779/
ReDoS vulnerability when parsing with ignoreEmpty option · Advisory · C2FO/fast-csv · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/C2FO/fast-csv/security/advisories/GHSA-8cv5-p934-3hwp

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

980483 Nodejs (npm) Security Update for @fast-csv/parse (GHSA-8cv5-p934-3hwp)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C2fo	Fast-csv	All	All	All	All
Application	C2fo	Fast-csv	All	All	All	All

cpe:2.3:a:c2fo:fast-csv:*:*:*:*:node.js:*:*:

cpe:2.3:a:c2fo:fast-csv:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @LinInfoSec	Npm - CVE-2020-26256: github.com/C2FO/fast-csv/...	2021-10-07

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)