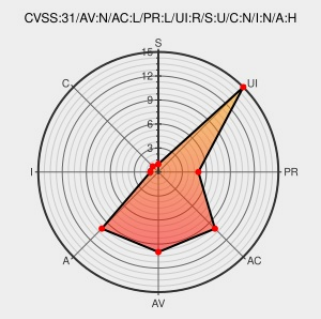
CVE-2020-26256

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-cvs 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_REGEXP` 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

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

19:06:24

← Previous ID

Next ID→