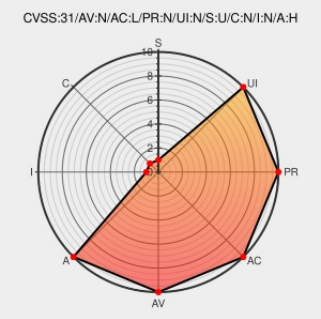
CVE-2023-34104

Published on: Not Yet Published

Last Modified on: 06/13/2023 04:26:00 PM UTC

CVE-2023-34104 - advisory for GHSA-6w63-h3fj-q4vw

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fast-xml-parser from Fast-xml-parser Project contain the following vulnerability:

fast-xml-parser is an open source, pure javascript xml parser. fast-xml-parser allows special characters in entity names, which are not escaped or sanitized. Since the entity name is used for creating a regex for searching and replacing entities in the XML body, an attacker can abuse it for denial of service (DoS) attacks. By crafting an entity name that results in an intentionally bad performing regex and utilizing it in the entity replacement step of the parser, this can cause the parser to stall for an indefinite amount of time. This problem has been resolved in v4.2.4. Users are advised to upgrade. Users unable to upgrade should avoid using DOCTYPE parsing by setting the `processEntities: false` option.

CVE-2023-34104 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **NaturalIntelligence** - **fast-xml-parser** version **= < 4.2.4**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Regex Injection via Doctype Entities · Advisory · NaturalIntelligence/fast-xml-parser · GitHub	github.com text/html	MISC github.com/NaturalIntelligence/fast-xml-parser/security/advisories/GHSA-6w63-h3fj-q4vw
fix security bug · NaturalIntelligence/fast-xml-parser@39b0e05 · GitHub	github.com text/html	MISC github.com/NaturalIntelligence/fast-xml-parser/commit/39b0e050bb909e8499478657f84a3076e39ce76c

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fast-xml-parser Project	Fast-xml-parser	All	All	All	All

cpe:2.3:a:fast-xml-parser_project:fast-xml-parser:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@_wassy555_	しかも今回のはfast-xml-parserが脆弱性報告（CVE-2023-34104）されていて、他のライブラリにも依存性があってめんどくさいパターンなのです。 放置したいのだけど、脆弱性放置するとリリース判定が通らないよ…	2023-06-27 01:41:33

← 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 registred 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