



CVE-2022-24434

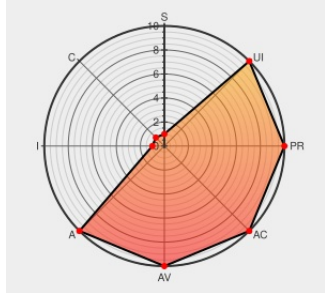
Published on: Not Yet Published

Last Modified on: 06/07/2022 02:04:00 AM UTC

CVE-2022-24434

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

JS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/R



Certain versions of [Dicer](#) from [Dicer Project](#) contain the following vulnerability:

This affects all versions of package dicer. A malicious attacker can send a modified form to server, and crash the nodejs service. An attacker could sent the payload again and again so that the service continuously crashes.

CVE-2022-24434 has been assigned by [report@snyk.io](#) to track the vulnerability - currently rated as **HIGH** severity.

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Denial of Service (DoS) in dicer CVE-2022-24434 Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-DICER-2311764
Removed a bug which could cause a crash in HeaderParser,	github.com text/html	MISC github.com/mscdex/dicer/pull/22/commits/b7fca2e93e8e9d4439d8acc5c02f5e54a0112dac

and as consequence could potentially crash a web server based on it by RolandHeinze · Pull Request #22 · mscdex/dicer · GitHub

Denial of Service (DoS) in org.webjars.npm:dicer | CVE-2022-24434 | Snyk

snyk.io

text/html

MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2838865

Security alert: Busboy can crash on manipulated multipart/form-data header names · Issue #250 · mscdex/busboy · GitHub

github.com

text/html

MISC github.com/mscdex/busboy/issues/250

Removed a bug which could cause a crash in HeaderParser, and as consequence could potentially crash a web server based on it by RolandHeinze · Pull Request #22 · mscdex/dicer · GitHub

github.com

text/html

MISC github.com/mscdex/dicer/pull/22

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	Dicer Project	Dicer	All	All	All	All

cpe:2.3:a:dicer_project:dicer:*:*:*:*:node.js:*:*:

Discovery Credit

Aras Abbasi

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-24434 : This affects all versions of package dicer. A malicious attacker can send a modified form to serv... twitter.com/i/web/status/1...	2022-05-20 20:06:47
 @Hamed_0X096	CVE-2022-24434 This affects all versions of package dicer. A malicious attacker can send a modified form to server,... twitter.com/i/web/status/1...	2022-05-20 22:37:48
 /r/netcve	CVE-2022-24434	2022-05-20 21:38:14
 /r/npm	error when install netbeans_cli with npm	2023-06-29 15:37:23

← 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](#)