

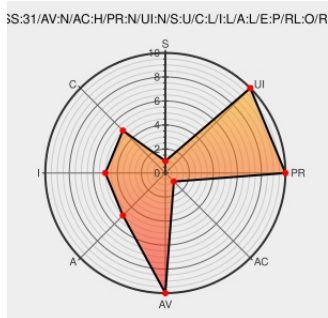


CVE-2021-23438

Published on: 09/01/2021 12:00:00 AM UTC

Last Modified on: 09/10/2021 03:23:00 PM UTC

CVE-2021-23438

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

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

This affects the package mpath before 0.8.4. A type confusion vulnerability can lead to a bypass of CVE-2018-16490. In particular, the condition `ignoreProperties.indexOf(parts[i]) !== -1` returns -1 if `parts[i]` is `['__proto__']`. This is because the method that has been called if the input is an array is `Array.prototype.indexOf()` and not `String.prototype.indexOf()`. They behave differently depending on the type of the input.

CVE-2021-23438 has been assigned by [report@snyk.io](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Prototype Pollution in org.webjars.npm:mpath Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1579548

fix: throw error if `parts` contains an element that isn't a string o... · aheckmann/mpath@89402d2 · GitHub

[github.com](#)
[text/html](#)

 MISC
github.com/aheckmann/mpath/commit/89402d2880d4ea3518480a8c9847c541f2d824fc

Prototype Pollution in mpath | Snky

[snyk.io](#)
[text/html](#)

 MISC snyk.io/vuln/SNYK-JS-MPATH-1577289

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

981063 Nodejs (npm) Security Update for mpath (GHSA-p92x-r36w-9395)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mpath Project	Mpath	All	All	All	All
cpe:2.3:a:mpath_project:mpath:*:*:*:*:node.js:*:*:						

Discovery Credit

Alessio Della Libera of Snky Research Team

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23438 : This affects the package mpath before 0.8.4. A type confusion vulnerability can lead to a bypass... twitter.com/i/web/status/1...	2021-09-01 18:24:04

[← 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](#)