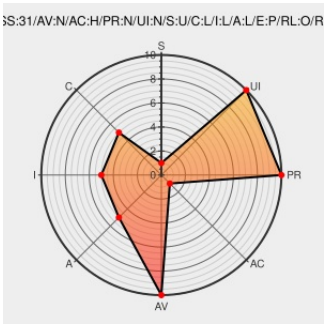
CVE-2021-23438

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 | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-MPATH-1577289

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 Snyk 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→