



CVE-2020-7644

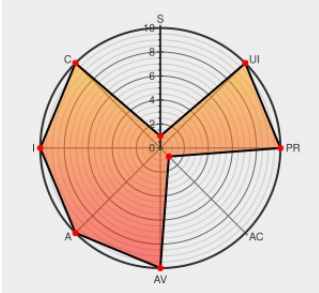
Published on: 04/28/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:26:00 AM UTC

CVE-2020-7644

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Fun-map](#) from [Fun-map Project](#) contain the following vulnerability:

fun-map through 3.3.1 is vulnerable to Prototype Pollution. The function `assocInM` could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload.

CVE-2020-7644 has been assigned by report@snyk.io to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Prototype Pollution in fun-map Snyk	Exploit Mitigation Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-FUNMAP-564436

fun-map/index.js at master · nathan7/fun-map · GitHub

Exploit
Third Party Advisory
github.com
text/html

MISC github.com/nathan7/fun-map/blob/master/index.js#L137,

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	Fun-map Project	Fun-map	All	All	All	All
cpe:2.3:a:fun-map_project:fun-map:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID →		