

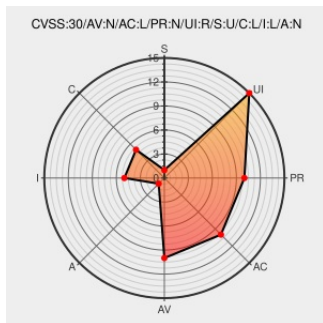


CVE-2018-1999024

Published on: 07/23/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-1999024

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

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

MathJax version prior to version 2.7.4 contains a Cross Site Scripting (XSS) vulnerability in the `\unicode{}` macro that can result in Potentially untrusted Javascript running within a web browser. This attack appear to be exploitable via The victim must view a page where untrusted content is processed using Mathjax. This vulnerability appears to have been fixed in 2.7.4 and later.

CVE-2018-1999024 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Fix parsing and output for <code>\class{}</code> and <code>\unicode{}</code> .	Patch Third Party Advisory	CONFIRM github.com/mathjax/MathJax/commit/a55da396c18cafb767a26aa9ad96f6f4199852f1

mathjax/MathJax@a55da39 · GitHub

github.com

text/html

MB blog: XSS in Google Colaboratory + CSP bypass

Exploit

Third Party Advisory

blog.bentkowski.info

text/html

MISC

blog.bentkowski.info/2018/06/xss-in-google-colaboratory-csp-bypass.html

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

981389 Nodejs (npm) Security Update for mathjax (GHSA-3c48-6pcv-88rm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mathjax	Mathjax	All	All	All	All
Application	Mathjax	Mathjax	All	All	All	All

cpe:2.3:a:mathjax:mathjax:*****:

cpe:2.3:a:mathjax:mathjax:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →