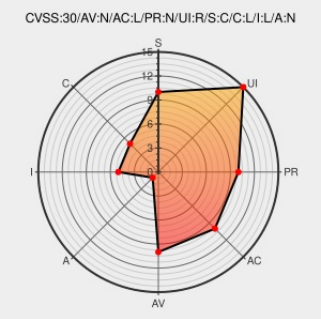
CVE-2018-19048

Published on: 05/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19048

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Simditor from Mycolorway contain the following vulnerability:

Simditor through 2.3.21 allows DOM XSS via an onload attribute within a malformed SVG element.

CVE-2018-19048 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	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
simditor_dom_xss/README.md at master · hkglue/simditor_dom_xss · GitHub	Exploit, Third Party Advisory, github.com, text/html	MISC github.com/hkglue/simditor_dom_xss/blob/master/README.md

ADD: DOMPurify for preventing xss attacks · mycolorway/simditor@ef01a64 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mycolorway/simditor/commit/ef01a643cbb7f8163535d6bfb71135f80ec6a6
GitHub - hkglue/simditor_dom_xss	Exploit Third Party Advisory github.com text/html	MISC github.com/hkglue/simditor_demo.git
Release v2.3.22 · mycolorway/simditor · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/mycolorway/simditor/releases/tag/v2.3.22

Related QID Numbers

981790 Nodejs (npm) Security Update for simditor (GHSA-8v67-x8q5-3x3g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mycolorway	Simditor	All	All	All	All

cpe:2.3:a:mycolorway:simditor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→