Cross-site Scripting (XSS) - Reflected in bustle/mobiledoc-kit

0

Valid Reported on May 5th 2021

✍️ Description

XSS using bypass of url validation

🦹 Proof of Concept

i see your code https://github.com/bustle/mobiledoc-kit uses a dependance https://github.com/bustle/mobiledoc-dom-renderer . This dependency uses for url validation to prevent xss . It filter javascript,vbscript protocol to prevent xss . But it should be bypassed using bellow payload `java script://asdad.com/%0dprompt%2812%29` With this payload your code will mark it as a safe url . Vulnerable script is https://github.com/bustle/mobiledoc-dom-renderer/blob/master/lib/utils/sanitization-utils.js Many project uses your this code to prevent xss . One of them is Ghostcms https://github.com/TryGhost/Ghost who uses this code for filtering and there i found xss because this code is failed to filter it I submitted this xss bug also to ghostcms here https://www.huntr.dev/bounties/1-other-TryGhost/Ghost/

💥 Impact

xss filter bypass

CVE
CVE-2022-2932
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Critical (9.8)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

This report was seen 856 times.

Garth Poitras 3 months ago Maintainer

The link would be invalid and not execute any javascript because of the space

ranjit-git 3 months ago Researcher

@maintainer
this payload will be executed .
The above javascript space is not normal space .
i suggest you to copy paste the payload from bellow url
see how this payload works herehttps://jsfiddle.net/63m78jdk/

Garth Poitras 3 months ago Maintainer

https://github.com/bustle/mobiledoc-dom-renderer/pull/79

ranjit-git 3 months ago Researcher

@maintainer
Can you plz Mark the report as valid

Garth Poitras validated this vulnerability 3 months ago

ranjit-git has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Garth Poitras marked this as fixed in **0.14.2** with commit **f3fdaa** 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation