

2 Persistent CSS injection with 'marked' markdown parser in Rocket.Chat

Share:



SUMMARY BY ROCKET.CHAT



Summary: Rocket.Chat offers two different markdown parsers out of the box: the 'original' one and the 'marked' one. Both markdown parsers offer a different set of features with different restrictions. Due to more loose restrictions in the 'marked' parser, a persistent CSS injection in the web interface of Rocket.Chat is possible.

Description: Due to style injection in the complete chat window, an adversary is able to manipulate not only the style of it, but will also be able to block functionality as well as hijacking the content of targeted users. Hence the payloads are stored in messages, it is a persistent attack vector, which will trigger as soon as the message gets viewed.

Releases Affected:

- 4.1.0 with 'marked' parser

Steps To Reproduce (from initial installation to vulnerability):

(Add details for how we can reproduce the issue)

1. Setup a new installation of Rocket.Chat
2. Enable the 'marked' parser in the admin settings under 'Message' > 'Markdown' > 'Markdown Parser'
3. Create a second user account with username `usertest` and a channel containing both accounts
4. Send some messages between both accounts
4. Send

Code 129 Bytes

```
1 <div style="position: fixed; top: 6px; right: 0px; height: 50px; width: 400px; back
```



This should block the top right channel settings with a red box.

6. Send

```

3  [data-username="usertest"] div div p{
4      background: rgba(255, 0, 0, 0.2);
5      font-size: 0;
6  }
7  [data-username="usertest"] div div p::after{ font-size: initial;
8      content: "hacked";
9  }
10 </style>

```

as admin user and observe, that the messages of 'usertest' are overwritten with the content 'hacked'. (It can be done vice versa when replacing 'usertest' in the payload with the admins username).

Supporting Material/References:

Root Cause

The implementation of the 'marked' render removes html encoding of the message right before rendering it in `app/markdown/lib/parser/marked/marked.js` line 98.

Code 307 Bytes

```

1  message.html = _marked(unescapeHTML(message.html), {
2      gfm,
3      tables,
4      breaks,
5      pedantic,
6      smartLists,
7      smartypants,
8      renderer,
9      highlight,
10 });
11
12 const window = getGlobalWindow();
13 const DomPurify = createDOMPurify(window);
14 message.html = DomPurify.sanitize(message.html, { ADD_ATTR: ['target'] });

```

Due to the unscape, the user will be able to inject custom HTML elements. Since `DomPurify.sanitize` will only sanitize XSS relevant elements and properties, the malicious

To avoid the style injection, but still allow the usage of custom tags, `DomPurify.sanitize` could be configured to also remove style elements and attributes. Another way to mitigate the issue would be to not unescape the html before rendering it with 'marked' to therefore prohibit the user to use custom HTML in their messages.


Impact

An attacker can block the user from certain functionalities as well as render the chat window unusable (e.g. with a rotation of the complete html body) after the user enters a channel. Another impact of the issue is the authenticity and integrity of messages. Since an adversary will be able to manipulate or hide arbitrary user messages, the authenticity and integrity is not given anymore. These attack vectors are stored in messages, which will make them available for every new user entering the channel.


Fix

Fixed in 5.0>


TIMELINE

- 


danieljpp submitted a report to [Rocket.Chat](#).

Nov 16th (about 1 year ago)
- 


danieljpp posted a comment.

Updated Dec 1st (12 months ago)
- 


mrrorschach Rocket.Chat staff updated the severity from Medium (6.5) to High.

Dec 8th (12 months ago)
- 


mrrorschach Rocket.Chat staff changed the status to ● **Triaged**.

Dec 8th (12 months ago)
- 


danieljpp posted a comment.

Dec 10th (12 months ago)
- 


danieljpp posted a comment.

Feb 9th (10 months ago)
- 

mrrorschach Rocket.Chat staff posted a comment.

Feb 9th (10 months ago)
- 

mrrorschach Rocket.Chat staff closed the report and changed the status to ● **Resolved**.

Aug 2nd (4 months ago)
- 

mrrorschach Rocket.Chat staff requested to disclose this report.

Sep 22nd (2 months ago)

