10 html injection via invite members can be leads account takeover

Share:

TIMELINE

ynexxx submitted a report to Mattermost. Jan 7th (11 months ago)

Hi team,

I have found an vulnerability on your website .

step to reproduce :

1.navigate to : yourworkspace.cloud.mattermost.com

2.create new channel Screenshot_from_2022-01-07_23-10-23.png (F1571445)

3.there you will find a functionality invite members Screenshot_from_2022-01-07_23-15-57.png (F1571448)

4.click on invite members

5 input your email address

6.scroll down & click on invite as guest Screenshot_from_2022-01-07_23-10-40.png (F1571456)

7. on Add to channels input your channel name

8.click on set a custom message , input this html payloads : `<a href=evil.com>` click `</a>` `<input type=x>`

9. invite

10.open inbox of email that you have invited

as you can see html injected & there's an input field & click button

follow my video poc for better understanding & if you need any info let me know .

thanks for reading my report .God bless you

Impact

As HTML injection worked in email an attacker can trick victim to click on such hyperlinks to redirect him to any malicious site and also can host a XSS page. All this will surely cause some damage to victim. This could lead to users being tricked into giving logins away to malicious attackers.

F1571456: Screenshot_from_2022-01-07_23-10-40.png

F1571459: cloud.mattermost.com_html_injection.mkv

rohitesh_mattermost Mattermost staff posted a comment. Jan 10th (11 months ago)

Thank you for your report. We will investigate the issue as soon as possible and shall let you know if we need any more information. Once validated, we will let you know and triage the issue.

Best regards and happy hunting!

rohitesh_mattermost Mattermost staff updated the severity from Medium to Low (2.0). Jan 10th (11 months ago)

rohitesh_mattermost Mattermost staff changed the status to ○ **Triaged**. Jan 10th (11 months ago)

Thanks for reporting this vulnerability. We have reviewed your report and after internally assessing the finding, we have determined that it is a valid issue. We would like to thank you for bringing this to our attention. Your report will be rewarded soon once we have discussed this further. Please stay tuned.

Best regards and happy hunting!

Mattermost rewarded rynexxx with a **$150** bounty. Jan 11th (11 months ago)

Thank you for reporting this vulnerability. After internally reviewing your finding, we have determined that it is a valid issue. We appreciate you bringing this to our attention. Congratulations!! We look forward to more additional reports from you.

Best regards and happy hunting!

rynexxx posted a comment. Jan 11th (11 months ago)

@Mattermost

thks for the bounty

kesavkesav filed a duplicate (#1446852) and was invited to participate in this report. Jan 11th (11 months ago)

yash__hackz filed a duplicate (#1449935) and was invited to participate in this report. Jan 16th (10 months ago)

Feb 18th (9 months ago)

rohitesh_mattermost Mattermost staff closed the report and changed the status to ○ **Resolved**.

 rynexxx posted a comment. Feb 28th (9 months ago)

Hi @rohitesh_mattermost

is this issue eligible for retesting?

rohitesh_mattermost Mattermost staff updated CVE reference to CVE-2022-1002. Mar 17th (8 months ago)

rohitesh_mattermost Mattermost staff requested to disclose this report. Mar 22nd (8 months ago)

rynexxx agreed to disclose this report. Mar 22nd (8 months ago)

This report has been disclosed. Mar 22nd (8 months ago)

 rynexxx posted a comment. Mar 22nd (8 months ago)

Hi @rohitesh_mattermost

is this issue eligible for retesting

 rohitesh_mattermost Mattermost staff posted a comment. Mar 22nd (8 months ago)

Hi @rynexxx

If you find any issues or bypasses with the fix, please feel free to report it as a separate new issue.

Thanks