12 Invitation Email is resent as a Reminder after invalidating pending email invites

Share:

TIMELINE

r_anksec submitted a report to Mattermost. Feb 20th (9 months ago)

Hello Team , I have found an issue through which unwanted users can be added to victim's workspace inside *.cloud.mattermost.com .

So I have created an workspace with my email id , let's say email1 and invited email2 to my workspace . Email2 is not having an account at mattermost , So email2 will be a fresh account. But I noticed that there is no option present to cancel the invite . This will lead to the issue . Let's see this in detail -

Real life case - Suppose a victim has invited someone to the workspace by putting email id but later on victim decided to withdraw the email id but there is no such option present due to which attacker can now join the workspace which leads to info disclosure . Also victim can mistype the email while inviting but victim now can't withdraw that email invite.

Mitigation - There should be an option present to cancel the invite sent to any email.

Steps to reproduce -
1) create account at mattermost and then create a workspace for yourself inside - *.cloud.mattermost.com
2) now invite email2 (email2 is not having account at mattermost) by invite option
3) now you will notice that there is no way present to cancel the invite
4) now email2 can easily join the workspace

Impact

Unwanted users can join the workspace leading to information disclosure.

rohitesh_mattermost Mattermost staff changed the status to ○ **Needs more info**. Feb 21st (9 months ago)

Thanks for your report. Please note that as mentioned in our documentation page

Please feel free to self close this report as N/A to avoid any reputation damages.

Best regards and happy hunting!

mr_anksec changed the status to ○ **New**. Feb 22nd (9 months ago)

Thanks for the info , I am closing this .

mr_anksec closed the report and changed the status to ○ **Not Applicable**. Feb 22nd (9 months ago)

mr_anksec posted a comment. Feb 22nd (9 months ago)

Hello @rohitesh_mattermost I think this attack I explained above is working . So I invited my second email let's say email2 to the team and then I went to system console and invalidated all the invite links , So now that invite link stops working. But after sometime (maybe after 1-2 days) you will again receive a reminder email in email2 inbox which contains the link to join the team and that link is working .

Which means if victim by mistake invites someone but then invalidate all invite links then also attacker can join the team by using the link he/she gets on reminder email.

Steps to reproduce -
1) invite email2 to the workspace
2) now after sometime invalidate all the invite link
3) after sometime you will again receive a reminder email in your inbox which contains a link to join the team
4) open that link and you will be able to join the team

mr_anksec posted a comment. Feb 22nd (9 months ago)

If you now believe that this is valid then please reopen the report .

rohitesh_mattermost Mattermost staff **reopened** this report. Feb 23rd (9 months ago)

Thanks @mr_anksec for adding further information. I am reopening this report for further investigation. Please stay tuned for further updates.

Feb 23rd (9 months ago)

rohitesh_mattermost Mattermost staff changed the report title from **Logical issue causing adding of unwanted users to workspace** to **Invitation Email is resent as a Reminder after invalidating pending email invites**.

rohitesh_mattermost Mattermost staff changed the status to ○ **Triaged**. Feb 23rd (9 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 mr_anksec with a **$150** bounty. Feb 23rd (9 months ago)

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

Best regards and happy hunting!

mr_anksec posted a comment. Feb 23rd (9 months ago)

Thanks for the bounty !!

Mar 16th (9 months ago)

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

Thanks again for reporting this issue. We've prepared a fix and it should be available in server version 6.5

rohitesh_mattermost Mattermost staff updated CVE reference to **CVE-2022-1385**. Apr 19th (7 months ago)

rohitesh_mattermost Mattermost staff requested to disclose this report. Apr 19th (7 months ago)

mr_anksec agreed to disclose this report. Apr 19th (7 months ago)

This report has been disclosed. Apr 19th (7 months ago)