

hacker

343

Opportunities

TIMELINE · EXPORT

Dashbo

Inbox

Hacktivity

Leaderboard

Directory

#1888915

Reset password link sent over unsecured http protocol

Share:

Reported February 28, 2023, 10:37am UTC

uchihaluckycs

Participants

Report Id

#1888915

Resolved

Reported to

Mattermost

Disclosed

May 10, 2023, 8:53am UTC

Severity

High (7.3)

Weakness

Improper Access Control - Generic

Bounty

\$750

Time spent

None

CVE ID

None

Account de...

None

uchihaluckycs submitted a report to Mattermost.

Summary:

After creating the workspace, if victim clicks on forgot password then reset password link has been generated and sent over mail and that p  
link is unsecured http protocol.

Steps To Reproduce:

1. Signup to a workspace

2. Navigate to https://h1-\*your-own-instance\*.cloud.mattermost.com/reset\_password and enter signup email

3. Check email, you will get reset password link.

Image F2201387: chrome\_iQDUTN9H1J.png

11.91 KiB

Zoom in Zoom out Copy Download

4. Copy that link paste in notepad and observe the protocol.

Image F2201388: sublime\_text\_opnUofVDz2.png

23.38 KiB

Zoom in Zoom out Copy Download

Mitigation:

Generate reset password link with secured https protocol.

Impact

If the victim opens the reset password link and forgot to update the password, anyone from intermediate computers through network or sni  
reset the password.

2 attachments:

F2201387: chrome\_iQDUTN9H1J.png

F2201388: sublime\_text\_opnUofVDz2.png

uchihaluckycs

updated the severity to Medium.

osku\_mattermost

Mattermost staff

posted a comment.

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 v  
we will let you know and triage the issue.

Best regards and happy hunting!

osku\_mattermost

Mattermost staff

changed the status to Triaged.

Thanks for reporting this vulnerability. We have reviewed your report and after internally assessing the finding, we have determined that it i  
issue. We would like to thank you for bringing this to our attention. Please stay tuned.

Best regards and happy hunting!

osku\_mattermost

Mattermost staff

updated the severity from Medium to High (7.3).

AVA Attacker needs to be able to capture network traffic to sniff the reset link being accessed over http

ACL sniffing is easy given the conditions exist. No AITM required

PR:N no privileges required on target system prior to attack

UI:R Targeted user is required to access the reset link

CH, IH With the reset link, the attacker completely owns the targeted user

AN No specific availability impact

Mattermost

rewarded uchihaluckycs with a \$750 bounty.

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

Best regards and happy hunting!

uchihaluckycs

posted a comment.

Thanks for the bounty


hackbot


closed the report and changed the status to Resolved.


Thanks for reporting!

uchihaluckycs


requested to disclose this report.

 **eva\_sarafianou** Mattermost staff  
agreed to disclose this report.


 This report has been disclosed.

 **uchihaluckys**  
posted a comment.  
Am I eligible for the swag?

Septi

 **Mattermost**  
rewarded **uchihaluckys** with swag.  
Yep you are!

Septi

 **uchihaluckys**  
posted a comment.  
Thanks for the swag

Septi

 **Notifications**

0

 **Profile**

>