Telegram – Incorrect ACL

- Telegram privacy fails again!

TL; DR

This is not a security vulnerability it's a privacy issue.

As I understand Telegram a messaging app focuses on privacy which has over 10,00,00,000+ downloads in Playstore. In this case, we are abusing a well-known feature of deleting messages, which allows users to delete messages sent by mistake or genuinely to any recipient. It was observed that once the message (image) is sent to the recipient, it still remains in the internal storage of the user which is located at `/Telegram/Telegram Images/`path.

I found this bug when I was researching about Telegram and MTProto protocol. To demonstrate this bug let's assume two people here, Bob and Alice.

Assume a scenario where Bob sends a message which is a confidential image and was mistakenly sent to Alice, Bob proceeds to utilize a feature of Telegram known as "**Also delete for Alice**" which would essentially delete the message for Alice. Apparently, this feature does not work as intended, as Alice would still be able to see the image stored under `**/Telegram/Telegram Images/**` folder, concluding that the feature only deletes the image from the chat window.
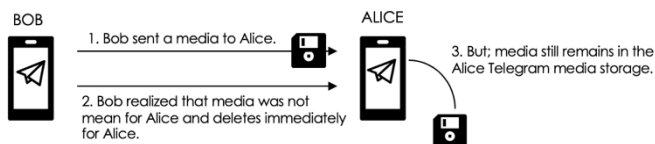
The highlighted issue is valid when we talk about Telegram "supergroups" as well, assume a case wherein you're a part of a group with 2,000,00 members and you accidentally share a media file not meant to be shared in that particular group and proceed to delete, by checking "delete for all members" present in the group.
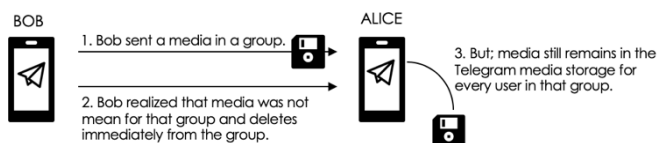
You're relying on a functionality that is broken since your file would still be present in storage for all users. Aside from this, I found that since Telegram takes `read/write/modify` permission of the USB storage which technically means the confidential photo should have been deleted from Alice's device or storage.

A compete, app for Telegram which is WhatsApp also has the same feature to "**Delete for everyone**". If you perform the following steps mentioned above in WhatsApp it deletes the confidential photo from Alice's `**/Whatsapp/Whatsapp Media/Whatsapp Images/**` folder and maintains the privacy however Telegram fails. WhatsApp takes the same permission when it comes to storage which is `read/write/modify`.

This issue could have a bigger impact and I am not sure how far this was in place; the word privacy of Telegram fails here again, and users trust against the Telegram is at risk.

I have tried this with the latest stable version (5.10.0 (1684)) of Telegram for Android. I haven't tried this with Telegram for iOS and Telegram for Windows but assuming this issue **would** exist on other these platforms.

I submitted this to Telegram sec-team via security[at]telegram[dot]org and a fix was pushed for same also €2,500 was awarded by Telegram.

The alternative solution would be to utilize the feature of "**New Secret Chat**" in Telegram where no such traces are left.

Twitter: @RandomDhiraj
Video PoC: https://youtu.be/_S64ApkqH1Y
Blog: https://www.inputzero.io/2019/09/telegram-privacy-fails-again.html