Telegram Messenger - Bug report

ID	6
Discovery Date	20-06-2016
Summary	Improper bound checking (both size and request rate of the messages)
Severity	Major
Product	Telegram messenger

Description

A malicious user can cause application crash and unwanted data download by taking advantage of the following flaws:

- Current size limit (4096 characters) does not hold for Contact messages (messages containing contact information).
  There are three fields in those messages (Phone number, First name and Last name) and each has a a maximum limitation of 35 KB. Summing up, one can send 105KB long messages, which are completely received on the client side (See in the PoC section).
  More interestingly, using bot API, we faced with server side limitation on those 105KB messages. But adding “multipart/form-data” to the http headers, circumvented the limit and server started to accept the messages.
- Request rate bound does not hold for contact messages. Consequently, we managed to send more than 300 of those messages in 1 minute (It seems rate bounds to can be much more).

Proof of concept

- There is also a clip, attached to this report, to show the severity of the issue.
- You can find a 105KB long message, sent to the following PoC channel: @bypass_sadghaf.
- In order to reproduce the issue you can follow instructions written in the following file: poc/readme.txt.

Suggestions

An approach, can be to set proper limitations on the size and request rate of the Contact messages.