Telegram Messenger - Bug report

ID	3
Discovery Date	07-06-2016
Summary	Lack of input checking on the Telegram URI scheme that leads to semi-permanent device crash
Severity	Critical
Product	Telegram messenger

Description

Due to improper input checking, a malicious user can take advantage of the Telegram URI scheme to cause a semi-permanent crash on devices.

Using "**tg://msg?text= aaa**" or "**tg://msg_url?text=aaa**", with big inputs would cause device crash on the victim side.

During the study, we managed to produce the following attack vector:

1-Send a link to the victim with the following content (PHP):

```
<?PHP header("tg://msg_url?url=&text= ".str_repeat("a",250000));?>
```

2-By opening the link on the victim side, the device showed two different reactions with the same result.

- After clicking on the link, by tapping on any user the application freezes (See the first link in the PoC channel).
- The application would be closed. After reopening the app, by tapping on any user the app freezes (See the second link in the PoC channel).

*** The problem continues happening (See the clip in the PoC folder) till the user remove the conversation which was clicked on. The bug caused us to reboot the device two times to make it working properly.

Proof of concept

- Open the links in the following telegram channel: @crash_sadghaf
- There is a small clip showing the problem in the POC directory (3.mp4).
- The PHP file is in the POC directory (3.php).

Suggestions

An approach can be, to check the URI schema more accurately before processing the link.