Telegram Messenger - Bug report

ID	2
Discovery Date	07-05-2016
Summary	Lack of input checking on the Telegram URI scheme that leads to unwanted message sending
Severity	Major+
Product	Telegram messenger

Description

Due to improper input checking, a malicious user can take advantage of the Telegram URI scheme to send unwanted messages from other users to specified contacts and with arbitrary content.

If "Send by enter" is active on the device (Android, IOS, Windows phone), Injecting an enter character "%0a" to **"tg://msg_url?text=An_unwanted_message%0a"** or **"tg://msg?text=An_unwanted_message%0a"** forces receivers to send the message to whom the attacker intends.

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

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

```
<?PHP header("Location: tg://msg_url?url=&text=An_unwanted_message%0a "); ?>
```

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

- Device would send the message. (See the first link in the PoC channel)
- The application would be exited (without any ...). After opening the app, by clicking on any user the message would be sent to him. The interesting part is that, as long as user tap on the contact account (in the contact list) the message would kept being sent.(See the second link in the PoC channel)

Proof of concept

- Open the links from a device in which the "Send by enter" is active. @unwanted_sadghaf
- There is a small clip showing the problem in the PpC directory (2.mp4)..
- The PHP file is in the PoC directory (2.php).

Suggestions

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