Telegram Messenger - Bug report

ID	4
Discovery Date	07-06-2016
Summary	Lack of audio-file format checking
Severity	Major
Product	Telegram messenger

Description

Due to lack of format checking on audio files (sent from clients), a malicious user can send arbitrary files, which by playing would be executed on the receiver's device.

During the test, we managed to send files with '.exe' and '.bat' formats to an account in place of audio files. Expectedly, after downloading the file, by clicking on the play button, the files were executed on the device (directly by the OS - Windows).

The sender can set the duration of the audio from API and make file's name long enough (to prevent the device from showing the file format) in order to make things look normal.

Proof of concept

You can find a '.bat' file (which would reboot the receiver's computer as soon as being played!) is sent as an audio file to the following PoC channel: @test_sadghaf

Suggestions

An approach, can be to check if the file has one of the below formats. Otherwise, it can be sent as a normal file (and not as an audio one).

.3gp,.aa,.aac,.aax,.act,.aiff,.amr,.ape,.au,.awb,.dct,.dss,.dvf,.flac,.gsm,.iklax,.ivs,.m4a,.m4b,.m4p,.mmf,.mp3,.mpc,.msv,.ogg,.oga,.opus,.ra, .rm,.raw,.sln,.tta,.vox,.wav,.wma,.wv,.webm (from Wikipedia).