ADVISORY

DATE

16 FEBRUARY 2021

# Telegram rlottie 7.0.1_2065 VDasher::VDasher Type Confusion

## Summary

Telegram rlottie 7.0.1_2065 is affected by a Type Confusion in the VDasher constructor: a remote attacker might be able to access Telegram's heap memory out-of-bounds on a victim device. Note: we'll walk through the android app sources, but the issue applies to iOS and macOS Telegram apps too.

## Product Description (from vendor)

"Telegram is a cloud-based mobile and desktop messaging app with a focus on security and speed.". For more information visit https://telegram.org/

## CVE(s)

- CVE-2021-31317

## Details

### Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. The code takes for granted that, if any, there are at least two dash properties (length and gap, defined in https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vdasher.h#L40) in the animated sticker. In case there's just one dash property, the other one is read out-of-bounds. Specifically, the read access violation happens at `VDasher::updateActiveSegment` in https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vdasher.cpp#L99:

```
mCurrentLength = mDashArray[mIndex].gap;
```

where `mDashArray` points at the dash property which only has the `length` attribute coming from the sticker, while `gap` is from out-of-bounds. `Gap` is apparently a legitimate part of the object, but in reality it is "included" via the `reinterpret_cast` in https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vdasher.cpp#L30:

```
mDashArray = reinterpret_cast<const VDasher::Dash *>(dashArray);
```

which instructs the compiler to treat the `float* dashArray` (which comes from the `std::vector<float> mStroke.mDash` in https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vdrawable.cpp#L28 ) as a `VDasher::Dash*` (https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vdasher.h#L40), even though it could have only a single float (like in our case) instead of two.

### Proof of Concept

A blogpost will be published soon on our blog with a PoC walkthrough and further details.

### Impact

A remote attacker might be able to access Telegram's heap memory out-of-bounds on a victim device.

### Remediation

Upgrade to Telegram 7.1.0 (2090) or later.

## Disclosure Timeline

- 30/09/2020:
  - Telegram releases version 7.1.0 (2090) with a patch

## Credits

`polict` of Shielder

**This advisory was first published on https://www.shielder.com/advisories/telegram-rlottie-vdasher-vdasher-type-confusion/**

**INFO**

Shielder S.r.l.

P.I. 11435310013

REA TO - 1213132

Registered Capital: 81.000,00 €

Via Palestro, 1/C
10064 Pinerolo (TO) Italy

**CONTACTS**

info@shielder.com

Landline: (+39) 0121 - 39 36 42

Commercial: (+39) 345 - 30 31 983

Technical: (+39) 393 - 16 66 814