ADVISORY

DATE

16 FEBRUARY 2021

Telegram rlottie 7.0.1_2065 gray_split_cubic Stack Buffer Overflow

Summary

Telegram rlottie 7.0.1_2065 is affected by a Stack Based Overflow in the gray_split_cubic function: a remote attacker might be able to overwrite Telegram's stack 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-2021-31321

Details

Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. Through a Transform property it's possible to overwrite adjacent stack memory. `bez_stack` has an hardcoded size (https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/freetype/v_ft_raster.cpp#L777):

```
SW_FT_Vector   bez_stack[16 * 3 + 1];
SW_FT_Vector*  arc = bez_stack;
```

Even thought `bez_stack` has a static size, the index is not verified before accessing it in the loop starting at https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/freetype/v_ft_raster.cpp#L805:

```
for (;;)
{
    if ([...])
        goto Split;

    gray_render_line( RAS_VAR_ arc[0].x, arc[0].y );

    if ( arc == bez_stack )
        return;

    arc -= 3;
    continue;

    Split:
    gray_split_cubic( arc );
    arc += 3;
}
```

The first actual out-of-bounds write access happens in https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/freetype/v_ft_raster.cpp#L747:

```
base[6].x = base[3].x;
```

where `base` is `arc` from the previous code snippets.

By using specific values in the Transform property, it is possible to write stack memory outside of `bez_stack`'s boundaries.

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 overwrite Telegram's stack 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-gray_split_cubic-stack-buffer-overflow/

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