ADVISORY

DATE

16 FEBRUARY 2021

Telegram rlottie 6.1.1_1946 LOTGradient::populate Heap Buffer Overflow

Summary

Telegram rlottie 6.1.1_1946 is affected by a Heap Buffer Overflow in the LOTGradient::populate function: a remote attacker might be able to access 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-2021-31322

Details

Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. The bug is an **heap-based buffer overflow** in `LOTGradient::populate` (starting at https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.cpp#L198) an *out-of-bounds read access* is performed because the actual number of color points in the animated sticker is not verified before accessing heap memory.

The number of color points is read from the animated sticker and it is used as end value for the loop on line https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.cpp#L211, triggering an out-of-bounds read access if it is higher than the actual number of color points in the animated sticker. Specifically, the read access violation happens at https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.cpp#L213 :

```
1 LottieColor color = LottieColor(ptr[3], ptr[2], ptr[1], nullptr);
```

where `ptr` points to the beginning of the color points data in heap memory:

```
1 float *       ptr = gradData.mGradient.data();
```

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 6.2.0 (1984) or later.

Disclosure Timeline

- 4/06/2020:
  - Telegram releases version 6.2.0 (1984) with a patch

Credits

`polict` of Shielder

This advisory was first published on https://www.shielder.com/advisories/telegram-rlottie-lotgradient-populate-heap-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