ADVISORY

DATE

16 FEBRUARY 2021

Telegram rlottie 7.0.1_2065 LOTGradient::populate Integer Overflow

Summary

Telegram rlottie 7.0.1_2065 is affected by a Integer 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-2021-31319

Details

Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. The vulnerability is a **signed integer overflow** in `LOTGradient::populate` (starting at https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.cpp#L198): an *out-of-bounds read access* is performed because the checks in place for malicious inputs are bypassable.

The integer `mColorPoints` comes directly from the animated sticker. Before using it to access the colorPoints in memory, the following check is performed at https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.cpp#L204:

```
1 if (colorPoints < 0 || colorPoints * 4 > size) {
2     colorPoints = size / 4;
3 }
```

In particular `colorPoints * 4` might overflow and wraparound to INT_MIN. Shortly later it is used to calculate the pointer to the actual colorPoints in memory at https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.cpp#L211, which could point out-of-bounds:

```
1 float *opacityPtr = ptr + (colorPoints * 4);
2 [...]
3 for (int i = 0; i < colorPoints; i++) {
4     float       colorStop = ptr[0];
5     LottieColor color = LottieColor(ptr[3], ptr[2], ptr[1], nullptr);
```

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-lotgradient-populate-integer-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