ADVISORY

DATE

16 FEBRUARY 2021

Telegram rlottie 6.1.1_1946 VGradientCache::generateGradientColorTable Heap Buffer Overflow

Summary

Telegram rlottie 6.1.1_1946 is affected by a Heap Buffer Overflow in the VGradientCache::generateGradientColorTable function: a remote attacker might be able to overwrite 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-2021-31320

Details

Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. The bug is an **heap-based buffer overflow** in `VGradientCache::generateGradientColorTable` (starting at https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/vector/vdrawhelper.cpp#L136): an out-of-bounds write access is caused by inaccurate boundary checks.

The `while` loop starting on line https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/vector/vdrawhelper.cpp#L158 does not limit `pos` size, which with a great enough input can become larger than `size` (which is the `colorTable` array size), leading to writing out-of-bounds 4 bytes.

Specifically, while `fpos` and `incr` are static, curr->first comes directly from the animated sticker. `colorTable` is an uint32_t array of size 1024, hence it is possible to overwrite an arbitrary amount memory after it by carefully using a specific float number as `curr->first` in the animated sticker file.

The written values are controlled via the sticker file too, but not 100% arbitrary because of ARGB codes constraints readable in premulARGB() https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/vector/vglobal.h#L292 and getColorReplacement() https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/lottie/lottiemodel.h#L99.

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 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-vgradientcache-generategradientcolortable-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