ADVISORY

DATE

16 FEBRUARY 2021

Telegram rlottie 6.1.1_1946 LOTCompLayerItem::LOTCompLayerItem Type Confusion

Summary

Telegram rlottie 6.1.1_1946 is affected by a Type Confusion in the LOTCompLayerItem::LOTCompLayerItem 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-2021-31318

Details

Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. The bug is a **type confusion** in `LOTCompLayerItem::LOTCompLayerItem` (starting at https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/lottie/lottieitem.cpp#L533): an object of an unverified type, e.g. `<LOTRepeaterData *>`, is subject to a static_cast to the type `<LOTLayerData *>`, resulting in an out-of-bounds memory access.

A static cast to `<LOTLayerData *>` is performed without any type check, e.g. against an `<LOTRepeaterData *>` which does not share the LOTGroupData "parent" and hence accessess out-of-bounds memory once it is used in https://github.com/DrKLO/Telegram/blob/release-6.1.1_1946/TMessagesProj/jni/rlottie/src/lottie/lottieitem.cpp#L813.

The classes hierarchy shows that while those objects are both children of `LOTData`, they do not share LOTGroupData:

```
LOTData
|--- LOTGroupdata
|    |--- LOTShapeGroupData
|    |--- LOTLayerData
|
|--- LOTRepeaterData
```

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-lotcomplayeritem-lotcomplayeritem-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

SITEMAP

Home

Company

Services

Advisories

Blog

Careers