ADVISORY

DATE

16 FEBRUARY 2021

Telegram rlottie 7.0.1_2065 blit Stack Buffer Overflow

Summary

Telegram rlottie 7.0.1_2065 is affected by a Stack Based Overflow in the blit function: a remote attacker might be able to access 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-2021-31315

Details

Root Cause Analysis

Telegram uses a custom fork of rlottie to render animated stickers. A malicious animated sticker with multiple "maskProperties" might bypass the protection in place against out-of-bounds access during the rendering process. The bound checks in place are not sufficient against a negative index: the resulting offset might point to memory before the target region `buffer` in https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vrle.cpp#L562.

```
int    x = spans->x + offsetX;
int    l = spans->len;
if (x + l > len) {
    return;
}
```

In case `spans->x` is negative, an out-of-bounds read access is triggered. The read access violation happens shortly later inside the `std::max` call at https://github.com/DrKLO/Telegram/blob/release-7.0.1_2065/TMessagesProj/jni/rlottie/src/vector/vrle.cpp#L569:

```
*ptr = std::max(spans->coverage, *ptr);
```

where the address of `ptr` is calculated using the negative `span->x`:

```
uchar *ptr = buffer + x;
```

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 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-blit-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