Gianluca Buttigliero
IT consultant
g.buttigliero@gmail.com
www.buttigliero.it

Vulnerability Report

Telegram client for Android, Google Assistant

09/10/2019

SUMMARY
Telegram Secret Chat content can be saved and diffused without alert/Google assistant allow to screenshot bypassing the App auth.

VULNERABILITY TYPE
Confidential data store and diffusion/3rd part app auth forcing.

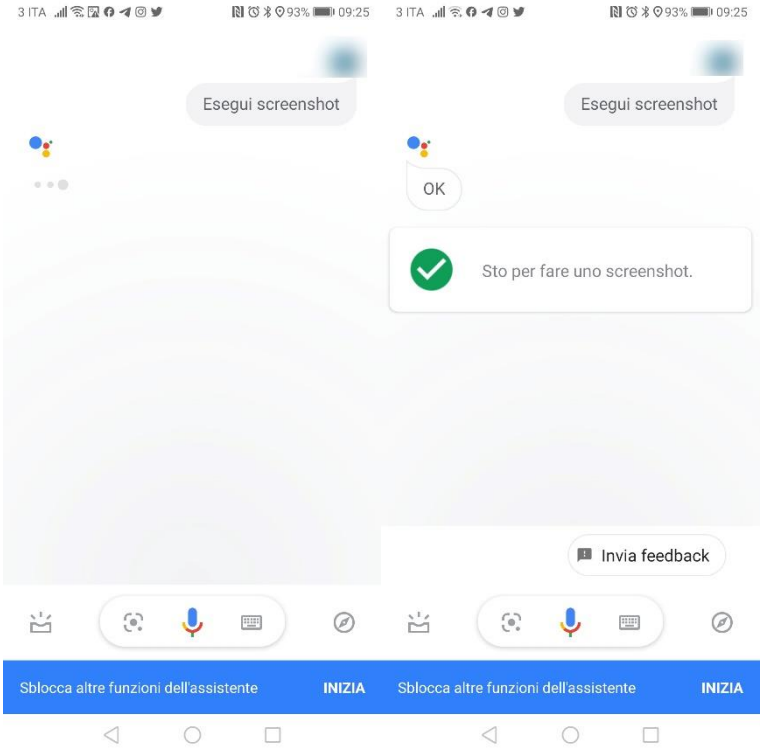
SEVERITY
LOW (extimated 2.1 on CVSS 3.1)

INTERESTED VERSION
Telegram for Android version 5.12.0(1739)arm64-v8a, Android 9 (tested on Huawei device with EMUI 9.1.0).

VULNERABILITY DESCRIPTION
The Google Vocal Assistant can bypass the block-by-app Android built-in functionality; for Telegram, in this way, the user can make screenshots of a Secret Chat without generate any alert popup on the other people client.

PROOF OF CONCEPT

1) I've made a new Secret chat with one of my contacts and set Auto-destruction time to 1 hour.
2) After opening the chat, i say to my Google Vocal Assistant "Ok Google, take a screenshot"



3) The screnshot was made and no alert popup is generated.

VARIATION
Google Assistant can bypass auth-lock from many others app, like protected documents generated by many bank app.

IOS BEHAVIOR
Siri on IOS 13.1.3 lock this possibility, but you can take screenshots from Telegram secret chat with hotkeys; nothing strange here, this thing generate an alert on target chat.

(POSSIBLE) MITIGATION
Allow Telegram to lock-out the google assistant interaction (usage-impact: high, can break-out vocal features).