2 Bypass local authentication (PIN code)

Share:

SUMMARY BY ROCKET.CHAT

Summary: An attacker with physical access to a mobile device can bypass local authentication (PIN code).

Description: When you set the PIN code to enter the application, the blocking occurs after the time set in the settings after the activity is closed. System time is used as a starting point. It is possible to bypass PIN by setting the system time back to a value when the application has not yet been blocked.

Releases Affected:

- 4.14.1.22788 iOS/Android

Steps To Reproduce (from initial installation to vulnerability):

1. Enable Screen Lock and set lock time (e.g. 1 min)
2. Close chat activity, mark the current time (e.g. 00:02), wait for blocking.
3. Open the app and make sure it is blocked, close the app.
4. Change the system time to a value when the lock has not yet been triggered (e.g. 00:01 or 00:02)
5. Start the app, it should be unblocked.

Suggested mitigation

- Use a separate timer to count down time to lock instead of the system time

Impact

Full access to user account with his privilegies.

Fixed in

We have fix this issue in the latest version of mobile app. You can download it in apple store or play store

markus-rocketchat changed the status to ○ **Triaged**. Mar 15th (2 years ago)

mrrorschach Rocket.Chat staff closed the report and changed the status to ○ **Resolved**. May 19th (6 months ago)

dago_669 posted a comment. May 28th (6 months ago)

mrrorschach Rocket.Chat staff requested to disclose this report. Sep 22nd (2 months ago)

mrrorschach Rocket.Chat staff disclosed this report. Sep 22nd (2 months ago)