Message ID Enumeration with Regular Expression in getReadReceipts Meteor method

Share:

Summary

The `getReadReceipts` Meteor server method does not properly filter user inputs that are passed to MongoDB queries, allowing `$regex` queries to enumerate arbitrary Message IDs.

Description

Authenticated users are able to query the `getReadReceipts` Meteor server method to enumerate existing Message IDs:

Code 101 Bytes

```
1  Meteor.call("getReadReceipts", {
2    messageId: { $regex: ".*" }
3  }, (...args) => console.log(...args));
```

When guessing individual characters of a message in the $regex MongoDB query of the messageId parameter, the server will respond with an error in case a message does not exist and return an (empty) list in case it does.

Releases Affected:

- 3.18.2
- 4.0.3

Steps To Reproduce (from initial installation to vulnerability):

(Add details for how we can reproduce the issue)

1. Login to Rocket.Chat as any authenticated user
2. Query `getReadReceipts` with $regex

- imports/message-read-receipt/server/api/methods/getReadReceipts.js

Suggested mitigation

- Filter messageId parameter of the Meteor method

Impact

An Adversary can enumerate existing Message IDs on the server with Regular Expression pattern matching.

Fix

Fixed in versions 4.7.5, 4.8.2 and 5.0.0

TIMELINE

gronke submitted a report to **Rocket.Chat**.	Oct 21st (about 1 year ago)
lucas_magno (Rocket.Chat staff) posted a comment.	Feb 2nd (10 months ago)
mrrorschach (Rocket.Chat staff) changed the status to ○ **Triaged**.	Mar 19th (8 months ago)
mrrorschach (Rocket.Chat staff) closed the report and changed the status to ○ **Resolved**.	Jul 25th (4 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)