1

getRoomRoles Method leaks Channel Owner

Share:

SUMMARY BY ROCKET.CHAT

Summary

Lack of ACL checks in the `getRoomRoles` Meteor method leak channel members with special roles to unauthorized clients.

Description

Lack of ACL checks in the `getRoomRoles` Meteor method allow unauthorized clients to query channel members with special roles:

Code 300 Bytes

```
Meteor.methods({
    getRoomRoles(rid) {
        check(rid, String);

        if (!Meteor.userId() && settings.get('Accounts_AllowAnonymousRead') === fa
            throw new Meteor.Error('error-invalid-user', 'Invalid user', { method:
        }

        check(rid, String);

        return getRoomRoles(rid);
    },
});
```

The `rid` argument must be a String but is not further validated.

Releases Affected:

- 4.3.1

Steps To Reproduce (from initial installation to vulnerability):

1. Open Rocket.Chat
2. (Optional) Login as low-privileged user
3. Query `getRoomRoles` Meteor method with target Room ID

Supporting Material/References:

Proof of Concept

Code 93 Bytes

```
const TARGET_ROOM_ID = "<ROOM_ID>";
Meteor.call("getRoomRoles", TARGET_ROOM_ID, console.log);
```

Suggested mitigation

- Check for the users access to the channel with given Room ID `rid`.

Impact

Unauthorized clients can leak members with special permission of private channels.

Fix

Fixed in versions 4.7.5, 4.8,2 and 5.0.0>

TIMELINE

gronke submitted a report to Rocket.Chat. Jan 11th (11 months ago)

lucas_magno Rocket.Chat staff changed the status to ○ **Triaged**. Jan 14th (11 months ago)

lucas_magno Rocket.Chat staff posted a comment. Jan 14th (11 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)