


## 2 Improper access control to messages of Social app

Share:     

### TIMELINE

 **sanktjodel** submitted a report to [Nextcloud](#). Jul 12th (2 ye  
The Social App (<https://apps.nextcloud.com/apps/social>) lacks access controls in the `displayPost` function ( `/@{username}/{token}` ) allowing an unauthenticated user to view any message content by knowing or guessing the message ID.

The vulnerable code is at

<https://github.com/nextcloud/social/blob/97fb063479d4c0ad6fccdea3774601a619f8a886/lib/Controller/ActivityPubController.php#L367>.

Note the TODO comment and the lack of authentication and authorization checks.

The following is a sample curl request to access a direct (private) message (replace the host, username, and the token value):

**Code** 112 Bytes [Wrap lines](#) [Copy](#) [Down](#)  

```
1 curl -X 'GET' -H 'Accept: application/activity+json' 'http://{{nextcloudHost}}/apps/social/@{username}/{token}' | jq
```

The `token` value consists of digits only and is based on the unix time.

An attacker would have to know or guess (e.g. brute force) this message ID.


### Impact

An unauthenticated attacker can view any social message, including private (direct) messages from one user to another.

The attacker would have to know or guess the token value.


 OT: posted a comment. Jul 12th (2 ye  
Thanks a lot for reporting this potential issue back to us!

Our security team will take a look at this issue as soon as possible. We will reply to your report within 72 hours, usually much faster. For obvious reasons we'd like to you to not disclose this issue to any other party.


 **nickvergessen** Nextcloud staff posted a comment. Jul 13th (2 ye  
Thanks for your report.  
That looks indeed fishy. I will forward your report to the author of the app.

 **nickvergessen** Nextcloud staff changed the status to 🔍 **Triaged**. Jul 13th (2 ye


 **maxence** Nextcloud staff posted a comment. Jul 13th (2 ye  
Hello,  
  
It is a known issue but I will work on a fix as soon as possible.  
  
Thanks for your report/remember!  
  
Maxence.

 **maxence** Nextcloud staff posted a comment. Jul 27th (2 ye  
Hello,  
  
A PR is available on <https://github.com/nextcloud/social/pull/952> that should filter the displayed post using the current viewer if authenticated.  
  
Regards,  
  
Maxence.

 **sanktjodel** posted a comment. Nov 3rd (2 ye  
This issue has been fixed over 3 months ago. Can we resolve this issue and make it public?


 **nickvergessen** Nextcloud staff closed the report and changed the status to ✅ **Resolved**. Nov 3rd (2 ye  
Thanks a lot for your report again. This has been resolved in a maintenance releases and we're working on the advisories at the moment.  
  
Please let us know how you'd like to be credited in our official advisory. We require the following information:

- Name / Pseudonym
- Email address (optional)
- Website (optional)
- Company (optional)

 **sanktjodel** posted a comment. Nov 4th (2 ye  
Thank you.  
  
Name: Roger Meyer  
Website: <https://twitter.com/sanktjodel>

 Nextcloud has decided that this report is not eligible for a bounty. Nov 17th (2 ye


- Nov 17th (2 years ago)

nickvergessen

Nextcloud staff

changed the report title from Social App lacks access controls on messages allowing unauthenticated users to view any message to Unauthenticated access to messages of Social app.


Nov 17th (2 years ago)

nickvergessen

Nextcloud staff


changed the report title from Unauthenticated access to messages of Social app to Improper access control to messages of Social app.

Nov 17th (2 years ago)

nickvergessen

Nextcloud staff

added weakness "Improper Access Control - Generic" and removed weakness "Improper Authentication - Generic".

nickvergessen


Nextcloud staff

posted a comment.

CVE pending: [CVE-2020-8278](#)

Advisory will be published at <https://nextcloud.com/security/advisory/?id=NC-SA-2020-042>


Nov 17th (2 years ago)

nickvergessen

Nextcloud staff

requested to disclose this report.

Nov 17th (2 years ago)

sanktjodel

agreed to disclose this report.

Nov 17th (2 years ago)

This report has been disclosed.