# CN REST - Task #8533

## evaluate and mitigate ORCID OpenId subject change on authentication infrastructure

2018-04-09 17:33 - Matthew Jones

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2018-04-09 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Chris Jones | **% Done:** | 100% |
| **Category:** | d1_portal_servlet | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Story Points:** | | | |

**Description**

I suspect this policy change at ORCID could impact our authentication on production systems. We've been wanting to revisit how ORCIDs are handled in our logins, and it looks like we may now have that opportunity. How should we go about evaluating this and mitigating?

---------- Forwarded message ----------
From: Basney, Jim jbasney@illinois.edu
Date: Mon, Apr 9, 2018 at 6:48 AM
Subject: RE: [ORCID API] OpenID 'sub' mismatch.
To: ORCID API Users orcid-api-users@googlegroups.com

Tom,

When their sub claim changes, I expect users will no longer be able to sign in to their accounts on our systems via ORCID unless we do a manual mapping from the https://orcid.org/0000-0000-0000-0000 to 0000-0000-0000-0000 form, similar to the change from the http://orcid.org/0000-0000-0000-0000 to https://orcid.org/0000-0000-0000-0000 form. Since [1] tells us to always use the full URI form, I'm surprised that the API is reverting the sub claim to the 0000-0000-0000-0000 form.

To help us plan for the operational impact of this change, can you provide a more precise schedule? Will this trigger an API version change to help us manage the timing of the change for our systems?

Thanks,

Jim

[1] https://support.orcid.org/knowledgebase/articles/116780

From: orcid-api-users@googlegroups.com orcid-api-users@googlegroups.com On Behalf Of Demeranville, Tom
Sent: Monday, April 9, 2018 6:36 AM
To: ORCID API Users orcid-api-users@googlegroups.com
Subject: [ORCID API] OpenID 'sub' mismatch.

All,

It's been brought to our attention that there is a mismatch between the 'sub' provided within our OpenID tokens and the 'sub' provided by the userinfo endpoint. Specifically, the id_token contains https://orcid.org/0000-0000-0000-0000 but the user info contains 0000-0000-0000-0000.

We will be changing the id_token so that it matches the user info endpoint, meaning we are removing the domain prefix. The prefix can be derived from the 'iss', i.e. issuer, which is changing to be relative to the service, e.g. https://orcid.org or https://sandbox.orcid.org/

This change will happen in the next few weeks. Please get in touch if you'd like more info.

Best,

Tom Demeranville

Technology Advocate

ORCID Inc

https://orcid.org/0000-0003-0902-4386

--
You received this message because you are subscribed to the Google Groups "ORCID API Users" group.
To unsubscribe from this group and stop receiving emails from it, send an email to orcid-api-users+unsubscribe@googlegroups.com.
To post to this group, send email to orcid-api-users@googlegroups.com.
Visit this group at https://groups.google.com/group/orcid-api-users.
For more options, visit https://groups.google.com/d/optout.

--
You received this message because you are subscribed to the Google Groups "ORCID API Users" group.
To unsubscribe from this group and stop receiving emails from it, send an email to orcid-api-users+unsubscribe@googlegroups.com.
To post to this group, send email to orcid-api-users@googlegroups.com.
Visit this group at https://groups.google.com/group/orcid-api-users.
For more options, visit https://groups.google.com/d/optout.

**Related issues:**

| | | |
|---|---|---|
| Related to CN REST - Task #8469: evaluate if ORCID API will continue to work ... | **In Progress** | **2018-03-02** |

## History

#### #1 - 2018-04-09 17:33 - Matthew Jones

*- Related to Task #8469: evaluate if ORCID API will continue to work after 1.2 is deprecated added*

#### #2 - 2018-04-10 19:29 - Chris Jones

So yes, this will affect our production logins. We currently set the user's DN based on the content of the sub claim, which so far has remained the http://orcid.org/xxxx-xxxx-xxxx-xxxx format. Because we are planning on creating equivalent identities for the https a bare ORCID string versions of these identities, this is probably a good time to make this change as well. We currently set the prefix in portal.properties to vary between the sandbox and production ORCID services. Changing to use the iss claim concatenated with the sub claim is overall a minimal change.

That said, timing is everything. We'll need to know when this change is available on https://sandbox.orcid.org so we can test it out, and then will need to know the precise date and time of the https://orcid.org production switchover so we can upgrade the portal at the same time to avoid authentication downtime. I'll chime in on the email list so Tom is aware that this affects our production service.

I'll make the changes and work with Jing and Dave to get it into the next release. We might want to have the tagged portal package ready and just wait until ORCID is ready for their switch.

#### #3 - 2018-04-24 21:52 - Chris Jones

Here's a copy of my response to Tom Demeranville at orcid.org:

```
Begin forwarded message:

From: Christopher Jones <cjones@nceas.ucsb.edu>
Subject: Re: [ORCID API] OpenID 'sub' change schduled for May 16th
Date: April 19, 2018 at 4:52:12 PM MDT
To: "Demeranville, Tom" <t.demeranville@orcid.org>
Cc: ORCID API Users <orcid-api-users@googlegroups.com>

Hi Tom,

Thanks for the note, and for the timing.  This change will definitely affect our
authentication service in the DataONE network, and so we'd like to request two things:

1) Having the switch be done in the sandbox.orcid.org environment at least two weeks
before the production switch.  That will allow us to change our code and test it
in the sandbox beforehand.

2) Identify the exact time that the production switch will occur on May 16th.
This will allow us to  coordinate our switch at the same time to avoid downtime
as much as possible.  We can let our community know that there will be a slight
```

```
downtime during a defined window, and that they'll need to authenticate again.

Thanks very much,
Chris
```

I'm working on a fix for this, and am thinking about handling the scenario where they don't provide time in their sandbox environment for testing, but just make the switch on the 16th.  I haven't heard back at all, so it'll be good to be prepared either way.  Dave, it might be helpful for you to respond as well at the google group to try to bump this a bit.

#### #4 - 2018-06-17 01:00 - Chris Jones

*- % Done changed from 0 to 100*

*- Status changed from New to Closed*

After getting into the details of this change, I found that we were not using the particular sub claim in the JWT, so we were unaffected by this issue in the end. Closing.