Authentic 2 - Development #66445

auth_oidc: le code de vérification des attributs requis est cassé si user_info ne contient pas exactement les mêmes attributs requis que l'idtoken

21 juin 2022 13:40 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	21 juin 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Le code se présente ainsi :

```
        for claim_mapping in provider.claim_mappings.all():
            claim = claim_mapping.claim
            if claim_mapping.required:
                if '{{' in claim or '{%' in claim:
                    logger.warning('claim \'%r\' is templated, it cannot be set as required')
                elif claim_mapping.idtoken_claim and claim not in id_token:
                    logger.warning(
                        'auth_oidc: cannot create user missing required claim %r in id_token (%r)'
,
                        claim,
                        id_token,
                    )
                    return None
                elif not user_info or claim not in user_info:
                    logger.warning(
                        'auth_oidc: cannot create user missing required claim %r in user_info (%r)
',
                        claim,
                        user_info,
                    )
                    return None
```

Deux cas ou la dernière condition (elif not user_info...) sera levé alors qu'elle ne devrait pas :

- si tous les mapping pointent vers l'idtoken alors user_info sera vide/None (car aucun mapping ne le réclamant il le user_info endpoint ne sera pas appelé), alors un claim bien présent dans l'idtoken finira par lever la dernière condition,
- si un claim requis et présent dans l'idtoken n'est pas présent aussi dans la réponse du endpoint user_info

Pour corriger cela il faudrait revoir le code ainsi :

```
        for claim_mapping in provider.claim_mappings.all():
            claim = claim_mapping.claim
            if claim_mapping.required:
                if '{{' in claim or '{%' in claim:
                    logger.warning('claim \'%r\' is templated, it cannot be set as required')
                elif claim_mapping.idtoken_claim:
                    if claim not in id_token:
                        logger.warning(
                            'auth_oidc: cannot create user missing required claim %r in id_token (
%r)',
                            claim,
                            id_token,
                        )
                        return None
                else: # user_info claim
```

```
                    if not user_info or claim not in user_info:
                        logger.warning(
                            'auth_oidc: cannot create user missing required claim %r in user_info
(%r)',
                            claim,
                            user_info,
                        )
                        return None
```

Révisions associées

Révision c0a41644 - 21 juin 2022 14:48 - Benjamin Dauvergne

auth_oidc: check required claims only from the idtoken or the user_info endpoint not both (#66445)

Historique

#1 - 21 juin 2022 13:40 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 21 juin 2022 13:42 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-check-required-claims-only-from-the-idtoke.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 21 juin 2022 14:48 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-check-required-claims-only-from-the-idtoke.patch ajouté

Avec un test c'est mieux.

#4 - 22 juin 2022 11:23 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Yes complètement, bien vu.

#5 - 22 juin 2022 11:34 - Benjamin Dauvergne

- Statut changé de Solution validée à Résolu (à déployer)

```
commit c0a41644a1ba7e893bc91b5afda806ac9159dcf9
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Jun 21 13:41:58 2022 +0200

    auth_oidc: check required claims only from the idtoken or the user_info endpoint not both (#66445)
```

#6 - 27 juin 2022 20:14 - Transition automatique

- Statut changé de Résolu (à déployer) à Solution déployée

#7 - 28 août 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-auth_oidc-check-required-claims-only-from-the-idtoke.patch	2,33 ko	21 juin 2022	Benjamin Dauvergne
0001-auth_oidc-check-required-claims-only-from-the-idtoke.patch	4,22 ko	21 juin 2022	Benjamin Dauvergne