Authentic 2 - Bug #84017

Une configuration OIDC avec des redirect_uris ne passe plus, même sans sector_identifier

28 novembre 2023 10:43 - Frédéric Péters

Statut:	Fermé	**Début:**	28 novembre 2023
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

La validation "all redirect_uri do not have the same hostname" s'applique désormais (depuis #83365) à un moment où ça n'était pas le cas avant, parce que le get_session_id() est appelé depuis un nouvel endroit :

```
ValueError: all redirect_uri do not have the same hostname
  File "django/core/handlers/exception.py", line 47, in inner
    response = get_response(request)
  File "django/core/handlers/base.py", line 181, in _get_response
    response = wrapped_callback(request, *callback_args, **callback_kwargs)
  File "authentic2/decorators.py", line 40, in f
    return func(request, *args, **kwargs)
  File "django/views/decorators/csrf.py", line 54, in wrapped_view
    return view_func(*args, **kwargs)
  File "authentic2_idp_oidc/views.py", line 842, in token
    response = tokens_from_authz_code(request)
  File "authentic2_idp_oidc/views.py", line 815, in tokens_from_authz_code
    'sid': utils.get_session_id(request.session, client),
  File "authentic2_idp_oidc/utils.py", line 284, in get_session_id
    sector_identifier = force_bytes(client.get_sector_identifier())
  File "authentic2_idp_oidc/models.py", line 233, in get_sector_identifier
    raise ValueError('all redirect_uri do not have the same hostname')
```

https://sentry.entrouvert.org/entrouvert/publik/issues/117075/

Demandes liées:

Lié à Authentic 2 - Bug #84092: idp_oidc : l'édition BO d'un client OIDC devr...	**Fermé**	**30 novembre 2023**

Révisions associées

Révision 1d92a060 - 15 janvier 2024 09:49 - Benjamin Dauvergne

idp_oidc: build the sid using the client_id instead of the sector identifier (#84017)

Révision 28afd8c4 - 15 janvier 2024 09:49 - Benjamin Dauvergne

tox.ini: use pytest-cov test context (#84017)

Historique

#2 - 28 novembre 2023 11:17 - Benjamin Dauvergne

Je peux changer la façon de calculer le sid pour pallier à cette régression, dans l'attente il faut soit supprimer les URLs avec domaine différent (ce qui a été fait sur clermont, bien) soit choisir une URL tronquée à la racine au hasard (la première) et la définir comme sector_identifier.

#3 - 28 novembre 2023 11:20 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#4 - 28 novembre 2023 11:27 - Robot Gitea

- Statut changé de Nouveau à Solution proposée

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/190
- Titre : idp_oidc: build the sid using the client_id instead of the sector identifier (#84017)

- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/190/files

#5 - 28 novembre 2023 11:28 - Benjamin Dauvergne

J'ai choisi d'utiliser le client_id plutôt que le sector_identifier comme élément différenciant les sid entre RP OIDC, sachant qu'à ma connaissance personne n'utilise le sid à part une demande recette pas encore en prod, ça ne devrait pas provoquer trop de souci au niveau des déconnexions, en tout cas rien qui persiste.

PS: pour préciser on envoie le sid dans les requêtes frontchannel de déconnexion vers les RPs si le RP valide le sid par rapport à ce qu'il a reçu ça pourrait bloquer une requête de déconnexion.

PS2: ça n'aura pas d'effet sur les sessions en cours, l'URL de déconnexion étant prégénérée au moment du SSO et stockée en session.

#7 - 30 novembre 2023 10:22 - Abdessamad Assila

Merci Fréd. Est-ce que c'est possible de le déployer encore ce matin? merci

#8 - 30 novembre 2023 10:27 - Paul Marillonnet

- Lié à Bug #84092: idp_oidc : l'édition BO d'un client OIDC devrait échouer sur des URIs de redirection portant des noms de domaine différents tandis qu'aucune URI d'identifiant de secteur n'est définie ajouté

#9 - 23 décembre 2023 18:51 - Robot Gitea

- Statut changé de Solution proposée à En cours

Thomas NOËL (tnoel) a relu et demandé des modifications sur une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/190

#10 - 30 décembre 2023 00:00 - Benjamin Dauvergne

- Statut changé de En cours à Solution proposée

#11 - 02 janvier 2024 10:37 - Robot Gitea

- Statut changé de Solution proposée à Solution validée

Thomas NOËL (tnoel) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/190

#12 - 15 janvier 2024 09:56 - Robot Gitea

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

Benjamin Dauvergne (bdauvergne) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/190
- Titre : idp_oidc: build the sid using the client_id instead of the sector identifier (#84017)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/190/files

#15 - 15 janvier 2024 13:14 - Transition automatique

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

#16 - 17 mars 2024 04:42 - Transition automatique

Automatic expiration