Authentic 2 - Development #47825

auth_oidc : sur un évènement "lost state" s'arranger pour conserver next_url et continuer

18 octobre 2020 12:38 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	18 octobre 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

On rapport l'évènement "lost state" car actuellement on ne conserve pas suffisamment d'information pour continuer correctement, il suffirait de conserver next_url en plus de l'uuid du state pour pouvoir s'en sortir.

Révisions associées

Révision 7b002f86 - 29 octobre 2020 00:34 - Benjamin Dauvergne

auth_oidc: use a signed state (#47825)

State is no more stored in the session, it's made using signing.dumps()
instead, to be more resilient. It's associated to a cookie scoped to the
callback path and the nonce created from the state id using an HMAC
construction with settings.SECRET_KEY.

Historique

#2 - 18 octobre 2020 12:38 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#3 - 18 octobre 2020 12:56 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#4 - 19 octobre 2020 16:24 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

(C'est rouge.)

#5 - 19 octobre 2020 18:08 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch ajouté

- Fichier 0002-tests-PEP8-47825.patch ajouté

- Statut changé de En cours à Solution proposée

#6 - 27 octobre 2020 17:04 - Paul Marillonnet

Je remplacerais, dans 0001 :

```
    raw_state = request.GET.get('state')
```

par

```
    raw_state = request.GET.get('state', '')
```

parce que sur les deux raw_state.split(…) juste en dessous ça va péter à coup sûr si raw_state vaut None.

#7 - 27 octobre 2020 17:09 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch ajouté

- Fichier 0002-tests-PEP8-47825.patch ajouté

Good catch.

#8 - 27 octobre 2020 17:13 - Paul Marillonnet

Et il manque une vérification du genre good_next_url(request, state_next_url).

De façon générale je ne sais pas ce que ça implique que de perdre la propriété d'opacité du state.

#9 - 27 octobre 2020 17:23 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch ajouté

- Fichier 0002-tests-PEP8-47825.patch ajouté

Tu as encore raison.

#10 - 27 octobre 2020 17:24 - Paul Marillonnet

Paul Marillonnet a écrit :

> Et il manque une vérification du genre good_next_url(request, state_next_url).

Et en fait je crois comprendre maintenant que c'est l'esprit du patch que de rediriger vers un truc non vérifié, et dont on ne vérifie pas non plus l'unicité tout au long du login. Je vais regarder plus en détail parce qu'à vue de nez ça me paraît être la fête au csrf, non ?

#11 - 27 octobre 2020 17:28 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Paul Marillonnet a écrit :
>
> > Et il manque une vérification du genre good_next_url(request, state_next_url).
>
> Et en fait je crois comprendre maintenant que c'est l'esprit du patch que de rediriger vers un truc non vérifié, et dont on ne vérifie pas non plus l'unicité tout au long du login. Je vais regarder plus en détail parce qu'à vue de nez ça me paraît être la fête au csrf, non ?

Sur les next_url on doit s'assurer qu'ils font partie d'une whitelist, ici pour aller plus loin il faudrait signer state, genre signing.sign({'state': state, 'next_url': next_url}) pour s'assurer qu'il n'a pas été modifié (en plus ça devient plus opaque ça évite que les gens jouent avec). Il faudrait vérifier les contraintes sur la longueur de state aussi.

#12 - 27 octobre 2020 18:54 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-use-a-signed-state-47825.patch ajouté

Bon finalement une autre approche :

- state devient un signing.dumps() de ce dont j'ai besoin, next_url, l'URL du fournisseur OIDC et un id
- le nonce est la signature HMAC de cet id
- je pose un cookie scopé sur le chemin du callback avec l'id pour vérifier l'id plus tard
- dans tous les cas sur un accès à callback, je vire le cookie
- si pas de cookie ou cookie différent, comme j'ai l'URL du fournisseur, je relance un login, ça supprime un cas d'erreur

#13 - 28 octobre 2020 10:57 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Ok top, je trouve ça vraiment mieux comme ça.

Juste histoire de trouver à y redire, il y a un

```
logger.debug('auth_oidc: sent request to token endpoint %r', token_endpoint_request)
```

qui a été retiré. On a conservé le log de debug sur la requête vers l'endpoint d'authz alors je conserverais bien aussi celui ci sur l'endpoint de jeton, juste pour la cohérence des logs.

Sinon c'est bon pour moi.

#14 - 29 octobre 2020 01:24 - Benjamin Dauvergne

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

```
commit 7b002f861fc1dd77edd31121f5a74e33ccd5c60f
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sun Oct 18 12:54:50 2020 +0200

    auth_oidc: use a signed state (#47825)

    State is no more stored in the session, it's made using signing.dumps()
    instead, to be more resilient. It's associated to a cookie scoped to the
    callback path and the nonce created from the state id using an HMAC
    construction with settings.SECRET_KEY.
```

#16 - 03 novembre 2020 10:16 - Frédéric Péters

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

Fichiers

0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch	4,5 ko	18 octobre 2020	Benjamin Dauvergne
0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch	7,59 ko	19 octobre 2020	Benjamin Dauvergne
0002-tests-PEP8-47825.patch	4,94 ko	19 octobre 2020	Benjamin Dauvergne
0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch	7,6 ko	27 octobre 2020	Benjamin Dauvergne
0002-tests-PEP8-47825.patch	4,94 ko	27 octobre 2020	Benjamin Dauvergne
0001-auth_oidc-dont-stop-redirect-on-state-lost-47825.patch	7,73 ko	27 octobre 2020	Benjamin Dauvergne
0002-tests-PEP8-47825.patch	4,94 ko	27 octobre 2020	Benjamin Dauvergne
0001-auth_oidc-use-a-signed-state-47825.patch	31,9 ko	27 octobre 2020	Benjamin Dauvergne