Authentic 2 - Development #48347

auth_oidc: contourner le bug SameSite=None dans Safari

06 novembre 2020 10:45 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	06 novembre 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 est toujours en Django 1.11 en production, qui ne gère pas SameSite dans set_cookie() mais on peut contourner ça.

Révisions associées

Révision 7514632f - 08 février 2021 16:00 - Benjamin Dauvergne

auth_oidc: enforce SameSite=Lax on the state cookie (#48347)

SameSite=Lax is needed for the cookie to be sent by the browser during
redirection chain from the provider. We could just depend on the fact
that cookie without SameSite are Lax by default, but it's better to be
explicit.

Historique

#1 - 07 novembre 2020 11:33 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-enforce-SameSite-Lax-on-the-state-cookie-4.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Je me suis aperçu en le codant que Lax étant la valeur par défaut et oidc-state étant un nouveau cookie qui ne reçoit pas SameSite=None comme le cookie CSRF et de session (configuration par défaut dans debian_config_common.py), ce ticket n'est pas vraiment nécessaire, le fait d'utiliser un nouveau cookie au lieu de la session avec SameSite=None corrige déjà le bug dans Safari, mais j'ai préféré être explicite pour qu'on ne se pose pas la question dans le futur de le passer en Strict ou None.

#2 - 16 novembre 2020 10:27 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-enforce-SameSite-Lax-on-the-state-cookie-4.patch ajouté

#3 - 16 novembre 2020 11:50 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-enforce-SameSite-Lax-on-the-state-cookie-4.patch ajouté

#4 - 08 février 2021 16:00 - Benjamin Dauvergne

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

```
commit 7514632fe6ba93afd039490c73fa00e726ae9a9a
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sat Nov 7 11:30:21 2020 +0100

    auth_oidc: enforce SameSite=Lax on the state cookie (#48347)

    SameSite=Lax is needed for the cookie to be sent by the browser during
    redirection chain from the provider. We could just depend on the fact
    that cookie without SameSite are Lax by default, but it's better to be
    explicit.
```

#5 - 08 février 2021 21:16 - Frédéric Péters

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

Fichiers

0001-auth_oidc-enforce-SameSite-Lax-on-the-state-cookie-4.patch	4,47 ko	07 novembre 2020	Benjamin Dauvergne
0001-auth_oidc-enforce-SameSite-Lax-on-the-state-cookie-4.patch	4,48 ko	16 novembre 2020	Benjamin Dauvergne
0001-auth_oidc-enforce-SameSite-Lax-on-the-state-cookie-4.patch	4,48 ko	16 novembre 2020	Benjamin Dauvergne