Authentic 2 - Bug #29009

OIDC: l'authentification OIDC ne conserve pas le nonce dans l'evènement d'authentification

14 décembre 2018 10:23 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	14 décembre 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

La conservation du nonce est nécessaire pour le bon suivi d'une authentification forcé (forceAuthn utilisé avec SSO SAML par exemple).

Révisions associées

Révision b4110b3b - 18 décembre 2018 17:15 - Benjamin Dauvergne

auth_oidc: verify and store id_token nonce (fixes #29009)

Historique

#1 - 14 décembre 2018 10:42 - Benjamin Dauvergne

- Patch proposed changé de Non à Oui

#2 - 14 décembre 2018 10:43 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-verify-and-store-id_token-nonce-fixes-2900.patch ajouté

- Statut changé de Nouveau à Solution proposée

Voilà le nonce est bien threadé à travers toute l'authentification pour finir
en session dans le tableau des évènements d'authentification, SAML sera
content.

#3 - 14 décembre 2018 15:09 - Benjamin Dauvergne

Les nonces sont utilisés dans a2 pour s'assurer qu'une réponse à une requête de SSO a bien donné lieu à une authentification, seul moyen de forcer une réauthentification.

En SAML on reprend l'ID unique du message de SSO qu'on passe à la vue /login/ dans le paramètre nonce, si on choisit l'authentification OIDC, ce nonce est passé ensuite à /accounts/oidc/login/, qui s'en sert pour le nonce du protocole OIDC.

Le nonce dans le protocole OIDC est une valeur unique passé dans la requête d'authentification OIDC et retournée uniquement dans l'id token, elle permet comme dans A2 de faire le lien entre une réponse et une requête.

#4 - 14 décembre 2018 15:25 - Thomas Noël

Dans src/authentic2_auth_oidc/views.py, ces deux lignes :

```
            ...
            oidc_request = oidc_state.get('request')
            nonce = oidc_request.get('nonce')
            ...
```

je les mettrais pas dans le try/except lié à get_provider_by_issuer, plutôt après.

Et sur la première ligne, plutôt faire un « oidc_request = oidc_state.get('request') or {} », au cas où.

Voilà, c'est tout ce que j'ai a dire, en vérité l'objet du patch m'échappe un peu.

#5 - 15 décembre 2018 09:47 - Benjamin Dauvergne

- Fichier 0001-auth_oidc-verify-and-store-id_token-nonce-fixes-2900.patch ajouté

- Fichier 0002-ajustement-remarque-tnoel.patch ajouté

Remarque intégrée, je rebaserai avant de pousser.

#6 - 17 décembre 2018 10:00 - Thomas Noël

- Statut changé de Solution proposée à Solution validée

#7 - 18 décembre 2018 17:20 - Benjamin Dauvergne

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

- % réalisé changé de 0 à 100

Appliqué par commit authentic2|b4110b3b3c0534aca523e1c025ae424cb9a32d1e.

#8 - 24 décembre 2018 11:21 - Frédéric Péters

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

Fichiers

0001-auth_oidc-verify-and-store-id_token-nonce-fixes-2900.patch	11,4 ko	14 décembre 2018	Benjamin Dauvergne
0001-auth_oidc-verify-and-store-id_token-nonce-fixes-2900.patch	11,4 ko	15 décembre 2018	Benjamin Dauvergne
0002-ajustement-remarque-tnoel.patch	1,26 ko	15 décembre 2018	Benjamin Dauvergne