w.c.s. - Development #42193

saml: ajouter l'extension "login-hint" dans la requete d'authentification vers l'idp lors de l'accès au backoffice

28 avril 2020 14:51 - Serghei Mihai

Statut:	Fermé	**Début:**	28 avril 2020
Priorité:	Normal	**Echéance:**	03 juin 2020
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Dans le même esprit que cela a été fait dans mellon.
Valeur backoffice pour informer l'idp qu'il s'agit d'un accès au backoffice.

Demandes liées:

Lié à Hobo - Development #42191: Poser un setting MELLON_LOGIN_HINTS pour tou...	**Fermé**	**28 avril 2020**

Révisions associées

Révision d4d4a682 - 29 mai 2020 10:27 - Serghei Mihai

saml: add login-hint extension on backoffice access (#42193)

Historique

#1 - 28 avril 2020 14:53 - Serghei Mihai

- Lié à Development #42191: Poser un setting MELLON_LOGIN_HINTS pour toutes les briques n'ayant pas de front ajouté

#2 - 18 mai 2020 09:43 - Serghei Mihai

- Assigné à mis à Serghei Mihai

#3 - 26 mai 2020 16:23 - Serghei Mihai

- Fichier 0001-saml-add-login-hint-extension-on-backoffice-access-4.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#4 - 26 mai 2020 16:36 - Frédéric Péters

next_url (login.msgRelayState en fait) pourrait contenir uniquement le chemin, c'est géré côté continue_to_after_url,

```
        elif relay_state:
            parsed_url = urlparse.urlparse(relay_state)
            scheme = parsed_url.scheme or request.get_scheme()
            netloc = parsed_url.netloc or request.get_server()
            after_url = urlparse.urlunsplit((scheme, netloc, parsed_url.path, parsed_url.query,
                                             parsed_url.fragment))
```

Ça devrait être géré également ici, histoire de ne pas casser de manière discrète au moment où seul un chemin sera passé.

#5 - 26 mai 2020 19:17 - Benjamin Dauvergne

Le relaystate n'est pas signé au retour et comme on est dans la correction des open-redirection, sans vouloir casser des trucs existants, ça m'irait que soit soumis à la validation des URLs comme cancel_url et /login/?next=. La vrai bonne façon de faire c'est de ne passer qu'un jeton qui doit faire référence à une donnée en session ou alors signée la valeur, w.c.s. (ou tout SP) doit s'assurer que c'est bien lui qui a envoyé ce relay-state ou alors que ce n'est vraiment pas important (genre si seulement deux valeurs "front" ou "back" sont acceptés pour dire de rediriger en front ou en back).

Si on accepte juste les URLs locales (commençant par un slash unique) et ça ne casse rien ça me va aussi (et sinon ça serait bien ce soit géré correctement mais ça urge moins).

#6 - 26 mai 2020 19:27 - Frédéric Péters

La correction dans #43279 concerne déjà ça (i.e. il n'y a pas de vérification ajoutée dans /login/?next=... la vérification se fait après le tour de manège et l'extraction de l'url (passée de ?next= à relayState)).

Par rapport à ce ticket, donc, mon commentaire il est que next_url = login.msgRelayState... peut donner un chemin, et qu'il faut prendre en compte cette possibilité.

#7 - 26 mai 2020 21:37 - Benjamin Dauvergne

Frédéric Péters a écrit :

> La correction dans #43279 concerne déjà ça (i.e. il n'y a pas de vérification ajoutée dans /login/?next=... la vérification se fait après le tour de manège et l'extraction de l'url (passée de ?next= à relayState)).

Ok.

#8 - 27 mai 2020 10:11 - Serghei Mihai

- Fichier 0001-saml-add-login-hint-extension-on-backoffice-access-4.patch ajouté

Prise en compte du path.

#10 - 28 mai 2020 10:35 - Serghei Mihai

- Echéance mis à 03 juin 2020

#11 - 29 mai 2020 10:21 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

Ok, sans discuter que ça modifie ce qui était passé dans eo:next_url. (qu'il faudra veiller plus tard à retirer).

#12 - 29 mai 2020 10:28 - Serghei Mihai

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

```
commit d4d4a682ab0ea260dc83117e3324bffa2c1f704a
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Tue May 26 14:09:33 2020 +0200

    saml: add login-hint extension on backoffice access (#42193)
```

#13 - 29 mai 2020 14:16 - Frédéric Péters

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

Fichiers

0001-saml-add-login-hint-extension-on-backoffice-access-4.patch	2,95 ko	26 mai 2020	Serghei Mihai
0001-saml-add-login-hint-extension-on-backoffice-access-4.patch	3,36 ko	27 mai 2020	Serghei Mihai