Authentic 2 - Development #27135

Déléguer l'authentification passive à la vue de login si aucune session n'est ouverte

09 octobre 2018 11:25 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	09 octobre 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Le but est de permettre à la vue de login de déterminer si une authentification passive déléguée est possible.

Demandes liées:

Lié à Authentic 2 - Development #33233: conversion d'un SSO SAML isPassive en...	**Fermé**	**19 mai 2019**
Lié à Authentic 2 - Bug #72507: idp_oidc : recueillir le consentement ou la s...	**Fermé**	**15 décembre 2022**

Révisions associées

Révision f34b2af3 - 14 décembre 2022 12:31 - Benjamin Dauvergne

misc: add next_url parameter to Authenticator.autorun() (#27135)

Révision 9d0d83b0 - 14 décembre 2022 12:31 - Benjamin Dauvergne

auth_oidc: make autorun go directly to the OP (#27135)

Révision e524c5f9 - 14 décembre 2022 12:34 - Benjamin Dauvergne

misc: proxy passive SSO from SAML2 services to OIDC idps (#27135)

Behaviour of the SAML2 when receiving a Passive AuthnRequest and not user is logged is modified. Before an immediate response with StatusCode no-passive was returned. Now if one authenticator with the method passive_login is found, the request is transferred to this authentication source.

Historique

#1 - 18 mars 2019 10:15 - Benjamin Dauvergne

- Tracker changé de Support à Development

#2 - 05 décembre 2022 10:36 - Benjamin Dauvergne

- Lié à Development #33233: conversion d'un SSO SAML isPassive en OIDC prompt=none ajouté

#4 - 07 décembre 2022 13:36 - Benjamin Dauvergne

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

- 0001: modification de la signature des méthodes autorun pour avoir un next_url explicite (nécessaire pour l'utiliser depuis une vue de l'IdP SAML)
- 0002: modification de l'autorun de auth_oidc pour économiser un redirect local et lancer directement la redirection vers l'IdP OIDC
- 0003: ajout d'un paramètre optionne passive à la méthode autorun de OIDCProvider pour pouvoir déclencher un SSO passif
- 0004: création d'une vue utilisateur passive_login() utilisable par un IdP pour lancer un SSO passif (quelque soit la source)
- 0005: utilisation de passive_login dans l'IdP SAML2 lorsqu'une AuthnRequest passive est reçu à la place de la réponse immédiate actuelle

Finalement on ne passe pas par la vue de login, ça évite de la complexifier.

#5 - 13 décembre 2022 15:06 - Benjamin Dauvergne

- Fichier 0001-misc-add-next_url-parameter-to-Authenticator.autorun.patch ajouté

- Fichier 0003-misc-proxy-passive-SSO-from-SAML2-services-to-OIDC-i.patch ajouté

- Fichier 0002-auth_oidc-make-autorun-go-directly-to-the-OP-27135.patch ajouté

En 3 patchs finalement:

- 0001 & 0002: pareil qu'avant
- 0003: toute la partie passive_login qui est maintenant complètement séparée de la méthode autorun() ça évite de jouer avec inspect et ça fait un code plus simple. Par rapport au dernier passave j'avais oublié de gérer le retour en cas de SSO passif qui échoue dans la partie IdP SAML2 (on serait revenu sur continue_sso() qui aurait relancé un SSO passif vers l'IdP OIDC, maintenant ça ne boucle plus).

#6 - 13 décembre 2022 15:34 - Benjamin Dauvergne

- Fichier 0001-misc-add-next_url-parameter-to-Authenticator.autorun.patch ajouté

- Fichier 0003-misc-proxy-passive-SSO-from-SAML2-services-to-OIDC-i.patch ajouté

- Fichier 0002-auth_oidc-make-autorun-go-directly-to-the-OP-27135.patch ajouté

Et un test passant de retour de SSO passif (on revient sur continue_sso() en étant connecté).

#7 - 14 décembre 2022 10:19 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

- Planning mis à Non

0001 et 0002 ok.

———————

Dans 0003 :

——

```
def passive_login(request, *, next_url, login_hint=None):
    # […]
    if len(visible_authenticators) != 1:
        return None
    unique_authenticator = visible_authenticators[0]
```

On peut peut-être virer cette contrainte peut-être pas nécessaire pour que le tout fonctionne ? utils_misc.get_authenticators() les renvoie triés par ordre d'apparition donc simplement tester sur le premier même s'il y en a plusieurs ?

——

Juste du détail, dans tests/test_idp_saml2.py::test_sso_with_authenticator_passive_sso_authenticated, tu as recopié le commentaire du test d'avant

```
# check NoPassive status code response after if conitnue is called and still no user is loggued in
```

alors que ce n'est pas ce que ce test fait.

——

Sinon les tests sont clairs (à part les quelques lignes qui semblent propres au structures de données lasso genre les codes de retour qui sont différents dans scenario.sp.login.response.status.statusCode.value et scenario.sp.login.response.status.statusCode.statusCode.value), c'est bon pour moi. Ack.

#8 - 14 décembre 2022 12:35 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> On peut peut-être virer cette contrainte peut-être pas nécessaire pour que le tout fonctionne ? utils_misc.get_authenticators() les renvoie triés par ordre d'apparition donc simplement tester sur le premier même s'il y en a plusieurs ?

Ok.

> Juste du détail, dans tests/test_idp_saml2.py::test_sso_with_authenticator_passive_sso_authenticated, tu as recopié le commentaire du test d'avant
> [...]
> alors que ce n'est pas ce que ce test fait.

J'ai mis le bon commentaire.

> Sinon les tests sont clairs (à part les quelques lignes qui semblent propres au structures de données lasso genre les codes de retour qui sont différents dans scenario.sp.login.response.status.statusCode.value et scenario.sp.login.response.status.statusCode.statusCode.value), c'est bon pour moi. Ack.

SAML structure les codes d'erreur, générique au premier niveau (denied/success) puis plus spécifique en dessous.

#9 - 14 décembre 2022 12:53 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> SAML structure les codes d'erreur, générique au premier niveau (denied/success) puis plus spécifique en dessous.

Ok, j'ignorais ça, merci pour la précision.

#10 - 14 décembre 2022 14:37 - Benjamin Dauvergne

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

```
commit e524c5f94d0c7e9a62e4fd245e477a3c45f6cb10
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Nov 29 16:32:45 2022 +0100

    misc: proxy passive SSO from SAML2 services to OIDC idps (#27135)

    Behaviour of the SAML2 when receiving a Passive AuthnRequest and not
    user is logged is modified. Before an immediate response with StatusCode
    no-passive was returned. Now if one authenticator with the method
    passive_login is found, the request is transferred to this authentication
    source.

commit 9d0d83b0e52af3604292aed894d846900729f1cc
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Nov 29 16:32:00 2022 +0100

    auth_oidc: make autorun go directly to the OP (#27135)

commit f34b2af379f49f8ad8b60b774ebad8ea621f7425
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Dec 7 10:58:26 2022 +0100

    misc: add next_url parameter to Authenticator.autorun() (#27135)
```

#11 - 15 décembre 2022 16:55 - Benjamin Dauvergne

- Lié à Bug #72507: idp_oidc : recueillir le consentement ou la sélection de profil de l'usager même lors d'un SSO passif (prompt=none) ajouté

#12 - 23 décembre 2022 10:16 - Transition automatique

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

#13 - 26 février 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-misc-add-next_url-parameter-to-Authenticator.autorun.patch	4,71 ko	13 décembre 2022	Benjamin Dauvergne
0003-misc-proxy-passive-SSO-from-SAML2-services-to-OIDC-i.patch	14,8 ko	13 décembre 2022	Benjamin Dauvergne
0002-auth_oidc-make-autorun-go-directly-to-the-OP-27135.patch	1,99 ko	13 décembre 2022	Benjamin Dauvergne
0001-misc-add-next_url-parameter-to-Authenticator.autorun.patch	4,71 ko	13 décembre 2022	Benjamin Dauvergne
0003-misc-proxy-passive-SSO-from-SAML2-services-to-OIDC-i.patch	16,3 ko	13 décembre 2022	Benjamin Dauvergne
0002-auth_oidc-make-autorun-go-directly-to-the-OP-27135.patch	1,99 ko	13 décembre 2022	Benjamin Dauvergne