w.c.s. - Bug #9855

redirect en 303 n'est pas joué

03 février 2016 11:31 - Thomas Noël

Statut:	Fermé	**Début:**	03 février 2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Thomas Noël	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	v1.31		
Patch proposed:	Oui	**Planning:**	

Description

constaté sur la production (apache/scgi)

```
          response.set_status(303)
          response.headers['location'] = after_url
          response.content_type = 'text/plain'
          return "Your browser should redirect you"
```

le 303 n'est pas renvoyé si after_url est relatif (/) au lieu d'absolu (http://...)

C'est lié à cette partie du code dans scgi :

```
if (location && location[0] == '/' &&
        ((r->status == HTTP_OK) || ap_is_HTTP_REDIRECT(r->status))) {
...
        /* Internal redirect -- fake-up a pseudo-request */
        r->status = HTTP_OK;
...
```

Cela a un impact suite à 926780efa6a0e9036787c3e13dcf55790f3cc6f7 #5637

Révisions associées

Révision 2ba77ca6 - 03 février 2016 14:24 - Thomas Noël

saml/continue_to_after_url: build absolute URL from RelayState (#9855)

Historique

#1 - 03 février 2016 11:39 - Thomas Noël

- Fichier 0001-saml-continue_to_after_url-use-redirect-instead-of-3.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

#2 - 03 février 2016 11:41 - Thomas Noël

nope ; ne passe pas les tests

#3 - 03 février 2016 11:44 - Benjamin Dauvergne

Plutôt ça peut-être:

```
if after_url.startswith('/'):
    after_url = request.get_scheme() + '://' + request.get_server() + after_url
```

#4 - 03 février 2016 12:14 - Thomas Noël

- Fichier 0001-saml-continue_to_after_url-use-qommon.redirect-for-r.patch ajouté

Yep. Suivant la même idée, je propose plutôt ceci, donc (c'est ce que j'ai patché à la rude en prod, en reprenant la logique du code d'avant #5637 qui utilisait redirect() sur les relay_state)

#5 - 03 février 2016 13:32 - Frédéric Péters

Il manque un test exposant le problème. (et pratiquement, le problème, il est arrivé où/comment ?)

Pourquoi passer par des 303 dans les autres situations mais pas là ? (ça ne doit avoir aucune incidence parce qu'on fait de l'artifact mais pour que ça soit correct on doit utiliser le code 303).

Je préférerais l'urlparse du relaystate et l'ajout des éléments nécessaires à l'URL s'ils n'existent pas.

#6 - 03 février 2016 13:55 - Benjamin Dauvergne

Frédéric Péters a écrit :

> Il manque un test exposant le problème. (et pratiquement, le problème, il est arrivé où/comment ?)

Le problème vient d'un accès sur /tryauth provoquant une authentification SAML passive qui se termine après la réception du statut NO_PASSIVE, car aucune session n'est disponible, par un redirect vers RelatyState=/, en 303 (problème vu partout en prod, où on utilise du tryauth sur la racine de w.c.s. ex.: https://eservices.mymeaux.fr/tryauth dans le lien Téléservices de www.mymeaux.fr). Ce 303 n'est jamais reçu par le navigateur qui reçoit à la place un 200 et comme contenu la page d'accueil de w.c.s, seulement l'URL est toujours /saml/assertionConsumerArtifact et donc les URLs relatives vers les formulaires pointent vers /saml/nom-du-formulaire au lieu de /nom-du-formulaire, et là boum plus rien ne marche.

La cause du problème c'est mod_scgi (apache) qui a un comportement particulier de refaire lui même la requête quand une redirection utilise une URL relative, ce qui faisait sens peut-être il y a 10 ans quand un navigateur quelque part ne le gérait pas mais maintenant que ça ne concerne aucun navigateur utilisé c'est idiot.

On n'a pas vu le problème avant car on a encore un différentiel entre prod et recette/dév: le premier utilise toujours apache quand les 2 autres utilise nginx, dont le module scgi n'a pas ce souci.

> Pourquoi passer par des 303 dans les autres situations mais pas là ? (ça ne doit avoir aucune incidence parce qu'on fait de l'artifact mais pour que ça soit correct on doit utiliser le code 303).

Oui, c'est pour ça que corriger le champ location est la bonne approche.

> Je préférerais l'urlparse du relaystate et l'ajout des éléments nécessaires à l'URL s'ils n'existent pas.

Très bien ça marche aussi.

#7 - 03 février 2016 13:57 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

> La cause du problème c'est mod_scgi (apache) qui a un comportement particulier de refaire lui même la requête quand une redirection utilise une URL relative, ce qui faisait sens peut-être il y a 10 ans quand un navigateur quelque part ne le gérait pas mais maintenant que ça ne concerne aucun navigateur utilisé c'est idiot.

En fait je pense que dans tous les cas ce comportement est idiot, il ferait mieux de réécrire le Location à l'aide du champ Host et ce qu'il sait être le scheme.

#8 - 03 février 2016 14:25 - Thomas Noël

- Fichier 0001-saml-continue_to_after_url-build-absolute-URL-from-R.patch ajouté

#9 - 03 février 2016 14:45 - Frédéric Péters

Nickel. (et ça peut aller dans le dépôt et puis je mettrai #9831 aussi, et on pourra voir pour faire une release)

#10 - 03 février 2016 14:58 - Thomas Noël

- Statut changé de En cours à Résolu (à déployer)

- Priorité changé de Immediat à Normal

- Version cible mis à v1.31

```
commit 2ba77ca6e486ff35c1adfb937b397e13bd0bbb72
Author: Thomas NOEL <tnoel@entrouvert.com>
Date:   Wed Feb 3 14:24:16 2016 +0100

    saml/continue_to_after_url: build absolute URL from RelayState (#9855)
```

#11 - 04 février 2016 15:13 - Thomas Noël

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-saml-continue_to_after_url-use-redirect-instead-of-3.patch	1,24 ko	03 février 2016	Thomas Noël
0001-saml-continue_to_after_url-use-qommon.redirect-for-r.patch	1,39 ko	03 février 2016	Thomas Noël
0001-saml-continue_to_after_url-build-absolute-URL-from-R.patch	2,41 ko	03 février 2016	Thomas Noël