Authentic 2 - Development #61592

Ajout de logs en cas de refus de requête de déconnexion CAS

09 février 2022 12:52 - Benjamin Renard

Statut:	En cours	**Début:**	09 février 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Renard	**% réalisé:**	0%
Catégorie:	authentic2-idp-cas	**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Lors d'une déconnexion CAS, pour que celle-ci soit traitée, il faut :

- que l'entête *HTTP_REFERER* soit présente dans la requête
- qu'un service CAS soit trouvé en correspondance avec le *referer* de la requête

Si l'une ou l'autre de ces conditions n'est pas respectée, la requête est ignorée.

Ce patch ajoute un message *WARNING* logué pour chacun de ces deux cas de refus, facilitant grandement la résolution de problème à ce niveau.

Historique

#2 - 09 février 2022 15:06 - Thomas Noël

- Statut changé de Nouveau à En cours

- Assigné à mis à Benjamin Renard

La seule question que je me pose c'est le niveau "warning" au lieu d'un simple "info". J'imagine que "warning" exprime un besoin de remonter ça en alerte à un moment (et pas juste une trace dans les logs), donc ok pour ça.

Ensuite, peux-tu modifier ainsi le message de commit :

```
idp cas: log why CAS logout request was rejected (#61592)

License: MIT
```

#3 - 10 février 2022 19:02 - Benjamin Renard

- Fichier 0001-idp-cas-log-why-CAS-logout-request-was-rejected-6159.patch ajouté

Thomas Noël a écrit :

> La seule question que je me pose c'est le niveau "warning" au lieu d'un simple "info". J'imagine que "warning" exprime un besoin de remonter ça en alerte à un moment (et pas juste une trace dans les logs), donc ok pour ça.

Tout à fait, c'est l'idée.

> Ensuite, peux-tu modifier ainsi le message de commit :
> [...]

Voilà.

#4 - 13 février 2022 13:23 - Benjamin Dauvergne

Ici le code devrait surtout être corrigé, le logout CAS n'est pas sûr, n'importe qui peut faire un SLO, le check du Referer est une validation un peu has-been.

Plutôt que de refuser tacitement on devrait systématiquement présenter un écran de confirmation, c'est beaucoup plus user friendly (il faudrait faire pareil coté OIDC, dans le cas un peu équivalent de authentic2_idp_oidc.views.logout ou l'URL de retour est inconnue), il suffit de faire un redirect vers /logout/?next=<next_url> pour cela.

Fichiers

0001-Log-why-CAS-logout-request-was-rejected.patch	1,43 ko	09 février 2022	Benjamin Renard
0001-idp-cas-log-why-CAS-logout-request-was-rejected-6159.patch	1,46 ko	10 février 2022	Benjamin Renard