Authentic 2 - Support #40175

bookmark de page de connexion avec ?nonce= dedans

25 février 2020 11:35 - Frédéric Péters

Statut:	Nouveau	**Début:**	25 février 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Je vais sur le portail agent, il me redirige vers <authentic>/login/?nonce=_51678...&service=portal-agent...&next=/idp/saml2/continue%3Fnonce%3D_51678..., je mets cette adresse en bookmark.

J'utilise mon bookmark une semaine plus tard, ça échoue avec un message "request has expired", le nonce étant expiré.

~~

On pourrait détecter à l'affichage de la page de connexion que le nonce est expiré et le zapper et il faudrait aussi zapper le ?next=, mais résultat l'agent pourra se connecter mais il sera envoyé sur le portail usager. (déjà mieux qu'avoir le "request has expired).

Plus loin, on pourrait aussi profiter de service=portail-agent dans la query string, pour savoir qu'après authentification il faut lancer un SSO initié par l'IdP vers le service en question. (pour les services/protocoles où un SSO initié par l'IdP est possible).

Historique

#1 - 26 février 2020 10:13 - Benjamin Dauvergne

Pour l'instant il faut juste ne pas bookmarker cette page... actuellement on a aucun moyen de savoir si un nonce est expiré les nonces n'existant pas en base; si jamais on avait ça il faudrait déterminer une URL de retour dépendante du service plutôt qu'une URL unique et directement renvoyer vers le service (et différencier le service du service BO encore plus chiant) en question plutôt que l'URL de retour par défaut qui est le portail usager.

Une possibilité plus simple ce serait de laisser la personne se connecter mais de déterminer l'URL de retour basée sur son OU, pour rediriger les agents vers le portail agent.

#2 - 26 février 2020 10:16 - Frédéric Péters

> si un nonce est expiré les nonces n'existant pas en base

En l'espèce, ils sont bien en base.

```
        messages.warning(request, _('request has expired'))
→
        login_dump, consent_obtained, nid_format = get_and_delete_key_values(nonce)
→
        kv = KeyValue.objects.get(key=key)
```

#3 - 26 février 2020 10:36 - Benjamin Dauvergne

Frédéric Péters a écrit :

> > si un nonce est expiré les nonces n'existant pas en base
>
> En l'espèce, ils sont bien en base.
>
> [...]

Oui mais non c'est spécifique.

#4 - 26 février 2020 11:44 - Frédéric Péters

Ok mais ça a du sens alors de ramener/limiter le ticket à la situation commune SAML, où :

- on sait que les nonces sont en base
- on peut faire un SSO initié par l'IdP vers ce qui sera trouvé en query string (service=portal-agent)

?

#6 - 23 septembre 2021 15:57 - Benjamin Dauvergne

1ère chose, on pourrait juste virer le warning, ça supprimera la page intermédiaire au SSO vers le portail usager qui suit forcément cette erreur.

2ème chose, il faudrait propager le paramètre service de /login/ vers la destination, ici /idp/saml2/continue chose qui ne me semble pas faite actuellement, à partir de là on pourra donc utiliser ce slug pour trouver le LibertyProvider concerné et ainsi déclencher un SSO initié par l'IdP (via authentic2.idp.saml2.saml2_endpoints.idp_sso).