Lasso - Bug #69673

Invalid ProxyRestriction generated when Count is set

28 septembre 2022 14:29 - Maxime Besson

Statut:	Fermé	**Début:**	28 septembre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Maxime Besson	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.8.1		
Patch proposed:	Non	**Planning:**	Non

Description

Lasso 2.8.0 generates invalid AuthnRequests when a ProxyRestriction element is added with a set Count

```
...
<saml:Conditions>
  <saml:ProxyRestriction>
    <saml:Audience>http://test.example.com/saml</saml:Audience>
    <saml:Count>0</saml:Count>
  </saml:ProxyRestriction>
</saml:Conditions>
...
```

This XML is invalid per the SAML specification (and is rejected as such by Onelogin's samltool.com, keycloak, and any implementation that checks the SAML XML schema

In http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd, Count is defined as an attribute of ProxyRestriction, and not a subelement, the correct result should be:

```
<saml:Conditions>
  <saml:ProxyRestriction Count="0">
    <saml:Audience>http://test.example.com/saml</saml:Audience>
  </saml:ProxyRestriction>
</saml:Conditions>
```

This feature (ProxyRestriction) is used by LemonLDAP::NG (which relies on Lasso) and causes compatibility issues with some SAML IDPs

I have attached a C test case to show the issue

Révisions associées

Révision 3a7ad361 - 28 septembre 2022 18:18 - Benjamin Dauvergne

Fix parsing of Count attribute of saml:ProxyRestriction (#69673)

Historique

#1 - 28 septembre 2022 16:17 - Benjamin Dauvergne

Great catch. Would you provide a patch to fix it ?

#2 - 28 septembre 2022 16:17 - Benjamin Dauvergne

- Statut changé de Nouveau à Information nécessaire

- Assigné à mis à Maxime Besson

#3 - 28 septembre 2022 17:28 - Frédéric Péters

- Projet changé de Produits Entr'ouvert à Lasso

#4 - 28 septembre 2022 18:00 - Maxime Besson

- Fichier fix-ProxyRestriction-Count.diff ajouté

The attached patch solves my use case but I'm not sure if anything else needs to be done in the lib.

Perhaps a release note should mention the fact that Lasso systems connected to each other should be upgraded at the same time to avoid errors when receiving incorrect messages from an older version?

#5 - 28 septembre 2022 18:12 - Benjamin Dauvergne

Maxime Besson a écrit :

> The attached patch solves my use case but I'm not sure if anything else needs to be done in the lib.
>
> Perhaps a release note should mention the fact that Lasso systems connected to each other should be upgraded at the same time to avoid errors when receiving incorrect messages from an older version?

Of course, I'll add it but I'm pretty sure you are the sole users of this SAML feature :-) For my education, what is the use case which mandates the use of this ProxyRestriction and with which software on the other party do you use it ? Or is it used solely among LemondLDAP instances ?

#6 - 28 septembre 2022 18:19 - Benjamin Dauvergne

- Tracker changé de Support à Bug

- Statut changé de Information nécessaire à Fermé

- Version cible mis à 2.8.1

```
commit 3a7ad3610f64cfa4a231fb543712371c1828e5e4 (HEAD -> main, origin/main, origin/HEAD)
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Sep 28 18:18:36 2022 +0200

    Fix parsing of Count attribute of saml:ProxyRestriction (#69673)
```

#7 - 29 septembre 2022 09:32 - Maxime Besson

Benjamin Dauvergne a écrit :

> Of course, I'll add it but I'm pretty sure you are the sole users of this SAML feature :-) For my education, what is the use case which mandates the use of this ProxyRestriction and with which software on the other party do you use it ? Or is it used solely among LemondLDAP instances ?

LemonLDAP sets a ProxyRestriction by default when sending an AuthnRequest, the intended purpose of this is to prevent the IDP from using another IDP to authenticate the user. However, after reading the spec carefully, I think this is **not** what ProxyCondition is for.
ProxyCondition prevents a SP receiving an assertion (LemonLDAP) from using it on another service (such as a LemonLDAP-protected app) which is what we do in every case. So I think we will end up removing it.

This patch however might help with old LLNG versions, and makes Lasso more spec-compliant, so thanks for including it!

Fichiers

invalid-proxy-restriction.c	445 octets 28 septembre 2022	Maxime Besson
fix-ProxyRestriction-Count.diff	588 octets 28 septembre 2022	Maxime Besson