Lasso - Bug #1582

Segmentation fault in load_endpoint_type2()

03 août 2012 23:12 - Hiromitsu Fujita

Statut:	Fermé	**Début:**	03 août 2012
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	90%
Catégorie:	SAMLv2	**Temps estimé:**	0:00 heure
Version cible:	2.3.6		
Patch proposed:		**Planning:**	

Description

Hi,

I'm using lasso-2.3.6 on Linux.
And I called lasso_server_new() function as follow:

```
lasso_server_new("sp-metadata.xml", NULL, NULL, NULL);
```

If sp-metadata.xml has an AssertionConsumerService element without index attribute,
SIGSEGV occurs in stdlib's strtol() function which is called by xsdUnsignedShortParse() in lasso/saml-2.0/provider.c.
The reason why SIGSEGV occurs is that NULL is passed to the first argument of strtol().
The NULL comes from the variable 'index' in load_endpoint_type2() function.

I think the index attribute in AssertionConsumerService element is optional,
so the 'index' returned by getSaml2MdProp() may be NULL.
However, the 'index' is not asserted before calling xsdUnsignedShortParse().

I attach a patch to fix this problem.

Regards,
Hiro

Révisions associées

Révision e94015f8 - 26 septembre 2012 21:01 - Benjamin Dauvergne

fix segfault in saml-2.0/provider.c:load_endpoint_type2

Thanks to Hiromitsu Fujita for the patch. fixes #1582.

Historique

#1 - 03 août 2012 23:24 - Hiromitsu Fujita

> I think the index attribute in AssertionConsumerService element is optional,

Sorry, I was wrong. The index attribute is required.
But this problem should be fixed for in case if a metadata is not valid.

#2 - 20 août 2012 08:43 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

- Priorité changé de Normal à Haut

#3 - 26 septembre 2012 21:05 - Benjamin Dauvergne

- Statut changé de Nouveau à Solution déployée

- % réalisé changé de 0 à 90

Appliqué par commit e94015f8bcc168c9882348d2e8c5a5138ea56676.

#4 - 19 novembre 2012 14:08 - Benjamin Dauvergne

- Statut changé de Solution déployée à Fermé

- Priorité changé de Haut à Normal

Fichiers

fix-lasso-saml2-provider-segfault.patch	487 octets	03 août 2012	Hiromitsu Fujita