Lasso - Bug #25640

Bug in saml2_authn_context.c, XmlSnippet

12 août 2018 15:02 - Paul Meurer

Statut:	Fermé	**Début:**	12 août 2018
Priorité:	Haut	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:	SAMLv2	**Temps estimé:**	0:00 heure
Version cible:	2.6.1		
Patch proposed:	Oui	**Planning:**	Non

Description

The definition of the struct XmlSnippet in lasso-2.6.0/lasso/xml/saml-2.0/saml2_authn_context.c seems to be wrong.

I append a saml response XML file that doesn't parse with this wrong XmlSnippet.

Here is the fixed version (SNIPPET_JUMP_ON_MISS should be SNIPPET_JUMP_ON_MATCH in both occurrences).

static struct XmlSnippet schema_snippets[] = { { "AuthnContextClassRef", SNIPPET_CONTENT | SNIPPET_OPTIONAL | SNIPPET_JUMP_ON_MATCH | SNIPPET_JUMP_3, G_STRUCT_OFFSET(LassoSaml2AuthnContext, AuthnContextClassRef), NULL, NULL, NULL}, { "AuthnContextDecl", SNIPPET_NODE | SNIPPET_OPTIONAL | SNIPPET_JUMP_ON_MATCH | SNIPPET_JUMP_4, G_STRUCT_OFFSET(LassoSaml2AuthnContext, AuthnContextDecl), NULL, NULL, NULL}, { "AuthnContextDeclRef", SNIPPET_CONTENT | SNIPPET_MANDATORY | SNIPPET_JUMP_3, G_STRUCT_OFFSET(LassoSaml2AuthnContext, AuthnContextDeclRef), NULL, NULL, NULL}, { "AuthnContextDecl", SNIPPET_NODE | SNIPPET_OPTIONAL | SNIPPET_JUMP_ON_MATCH | SNIPPET_JUMP_2, G_STRUCT_OFFSET(LassoSaml2AuthnContext, AuthnContextDecl), NULL, NULL, NULL}, { "AuthnContextDeclRef", SNIPPET_CONTENT | SNIPPET_OPTIONAL, G_STRUCT_OFFSET(LassoSaml2AuthnContext, AuthnContextDeclRef), NULL, NULL, NULL}, { "AuthenticatingAuthority", SNIPPET_CONTENT | SNIPPET_OPTIONAL, G_STRUCT_OFFSET(LassoSaml2AuthnContext, AuthenticatingAuthority), NULL, NULL, NULL}, {NULL, 0, 0, NULL, NULL, NULL}
};

Best regards,
Paul Meurer

Révisions associées

Révision b891ed7d - 04 septembre 2018 10:42 - Benjamin Dauvergne

xml: fix parsing of saml:AuthnContext (fixes #25640)

Decl/DeclRef are alternatives, when matching a Decl we should jump over the DeclRef.

Révision 5070a06a - 14 octobre 2018 20:35 - Benjamin Dauvergne

xml: fix parsing of saml:AuthnContext (fixes #25640)

Decl/DeclRef are alternatives, when matching a Decl we should jump over the DeclRef.

Historique

#1 - 04 septembre 2018 10:43 - Benjamin Dauvergne

No only the second JUMP_ON_MISS should be a JUMP_ON_MATCH, see the schema :

```
* <complexType name="AuthnContextType">
*   <sequence>
*     <choice>
*       <sequence>
*         <element ref="saml:AuthnContextClassRef"/>
*         <choice minOccurs="0">
*           <element ref="saml:AuthnContextDecl"/>
```

```
*           <element ref="saml:AuthnContextDeclRef"/>
*         </choice>
*       </sequence>
*       <choice>
*         <element ref="saml:AuthnContextDecl"/>
*         <element ref="saml:AuthnContextDeclRef"/>
*       </choice>
*     </choice>
*     <element ref="saml:AuthenticatingAuthority" minOccurs="0" maxOccurs="unbounded"/>
*   </sequence>
* </complexType>
```

Decl/DeclRef become mandatory if there is no ClassRef, it's optional otherwise, with a regexp like syntax :

```
( ClassRef ( Decl | DeclRef )? | ( Decl | DeclRef ) AuthenticatingAuthority* )
```

#2 - 04 septembre 2018 10:43 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#3 - 04 septembre 2018 10:43 - Benjamin Dauvergne

- Fichier 0001-xml-fix-parsing-of-saml-AuthnContext-fixes-25640.patch ajouté

- Statut changé de Nouveau à Solution proposée

Could you check this smaller patch fix your instance of the problem ?

#4 - 01 octobre 2018 22:30 - Paul Meurer

Yes, you are correct, obviously.
The smaller patch works for my problem. Thanks!

#5 - 14 octobre 2018 20:26 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#6 - 14 octobre 2018 20:30 - Benjamin Dauvergne

- Statut changé de Solution validée à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit b891ed7dca9c93c5ec6f2ce2408681cab2a74a8b.

#7 - 27 août 2019 09:20 - Thijs Kinkhorst

We ran into the same issue with the latest version of lasso (this is with NetIQ AM as an IdP). The patch indeed fixes it for us. So it would be great if a new release could be tagged!

#8 - 06 septembre 2019 14:40 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Solution déployée

Fichiers

authn-context-bug.xml	7,31 ko	12 août 2018	Paul Meurer
0001-xml-fix-parsing-of-saml-AuthnContext-fixes-25640.patch	1,33 ko	04 septembre 2018	Benjamin Dauvergne