Lasso - Bug #4804

Lasso error code 609: No default endpoint

12 mai 2014 16:22 - David Coutadeur

Statut:	Rejeté	**Début:**	12 mai 2014
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:	Core	**Temps estimé:**	0:00 heure
Version cible:	2.4.0		
Patch proposed:		**Planning:**	

Description

Hi all,

I get this error code when lasso is trying to read a saml auth request:
Lasso error code 609: No default endpoint

Lasso is configured as an Identity Provider.

Fortunatelly, this error code is present only once in the code:

lasso/saml-2.0/login.c:325

```
                int service_index = authn_request->AssertionConsumerServiceIndex;

                binding = lasso_saml20_provider_get_assertion_consumer_service_binding(
                                remote_provider, service_index);
                if (binding == NULL) {
                        if (service_index == -1) {
                                debug("LASSO: LASSO_LOGIN_ERROR_NO_DEFAULT_ENDPOINT");
                                return LASSO_LOGIN_ERROR_NO_DEFAULT_ENDPOINT;
                }
```

More precisely, I don't understand why service index is checked before this message is displayed.
If I refer to SAML documentation, the AssertionConsumerServiceURL is optional in the request, and in this case, the Serrvice URL must be checked against the metadata, so is this case managed through lasso ?

```
AssertionConsumerServiceURL [Optional]
Specifies by value the location to which the <Response> message MUST be returned to the
requester. The responder MUST ensure by some means that the value specified is in fact associated
with the requester. [SAMLMeta] provides one possible mechanism; signing the enclosing
<AuthnRequest> message is another. This attribute is mutually exclusive with the
AssertionConsumerServiceIndex attribute and is typically accompanied by the
ProtocolBinding attribute.
```

For convenience, here are the SAML Request and metadata:

```
<samlp:AuthnRequest
    Version="2.0"
    ID="wp1i7UN-hRIu1w.tEt1jiwAaaa"
    IssueInstant="2014-05-12T08:14:24.907Z"
    Destination="https://login-test.domain.org/saml/singleSignOn"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://id-test.iso.org/proxy
  </saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="true"/>
</samlp:AuthnRequest>
```

metadata:

```
<md:EntityDescriptor
   ID="Y3cs0y9pKSSGmOcGA0phaaa.L.4"
```

```
   cacheDuration="PT1440M"
   entityID="https://id-test.iso.org/proxy"
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
        <ds:X509Certificate>
mycertificatevalue
        </ds:X509Certificate>
    </ds:X509Data>
    </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:AssertionConsumerService index="0" Location="https://id-test.iso.org/sp/ACS.saml2" Binding
="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Thank you in advance for your help.

Sincerely,

David

Historique

#1 - 12 mai 2014 17:09 - Benjamin Dauvergne

David Coutadeur a écrit :

> Hi all,
>
> I get this error code when lasso is trying to read a saml auth request:
> Lasso error code 609: No default endpoint
>
> Lasso is configured as an Identity Provider.
>
> Fortunatelly, this error code is present only once in the code:
>
> lasso/saml-2.0/login.c:325
>
> [...]

The real problem here is that lasso_saml20_provider_get_assertion_consumer_service_binding() is not returning your default assertion consumer which I see is correctly declared in your metadata file. You should step in the body of the loop in lasso/saml-2.0/provider.c:700 to see what's happening there. A printf of endpoint_type->{role,kind,binding} would be enough.

#2 - 12 mai 2014 18:25 - David Coutadeur

Hi, here is the result of printf in the corresponding loop (the one you have indicated)

LASSO: endpoint_type->role 2
LASSO: endpoint_type->kind SingleLogoutService
LASSO: endpoint_type->binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
LASSO: endpoint_type->role 2
LASSO: endpoint_type->kind SingleSignOnService
LASSO: endpoint_type->binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

#3 - 12 mai 2014 18:35 - Benjamin Dauvergne

David Coutadeur a écrit :

> Hi, here is the result of printf in the corresponding loop (the one you have indicated)
>
> LASSO: endpoint_type->role 2
> LASSO: endpoint_type->kind SingleLogoutService
> LASSO: endpoint_type->binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
> LASSO: endpoint_type->role 2
> LASSO: endpoint_type->kind SingleSignOnService
> LASSO: endpoint_type->binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

There is something wrong, those are the endpoints of an IdP not an SP, coud you report the same thing but adding the field endpoint_type->url (it's a string); are you sure that you are loading the metadata file you quoted ? There is not even a declaration of a logout service but here there is.

#4 - 12 mai 2014 19:04 - David Coutadeur

Ok, sorry for disturbing.
The problem was due to the entityID. In the product, I have 2 SP and 1 IdP, and one of the SP entityID is identical to the IdP entityID, which as you can guess, leads to this major "bug". So, no bug in Lasso, again : sorry.

#5 - 12 mai 2014 19:23 - Benjamin Dauvergne

- Statut changé de Nouveau à Rejeté