Lasso - Bug #12829

Misleading error message when SAML response does not conform to the XML schema (patch included)

04 août 2016 00:03 - Ivan Krivyakov

Statut:	Fermé	**Début:**	03 août 2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.6.1		
Patch proposed:	Non	**Planning:**	Non

Description

We are using mod_auth_mellon 0.11.0 with lasso 2.5.0. So, my patch is based on 2.5.0 (sorry).

We discovered that when our SAML response (attached) request does not follow the expected schema (e.g. has "Signature" node out of place), we get the following very undescriptive error, that looks more like a bug:

```
(process:25058): Lasso-CRITICAL **: 2016-08-03 20:59:52 (xml.c/:1708) Trying to add to a GList* a
non GObject pointer dest=*list src=subnode
[Wed Aug 03 20:59:52.105237 2016] [:error] [pid 25058] [client 10.90.8.176:60095] Error processing
 authn response. Lasso error: [-427] When looking for an assertion we did not found it.
```

Before I move on, you may want to change "When looking for an assertion we did not found it", to
"When looking for an assertion, we did not find it".

The research showed that this stems from the following sequence of events:

In lasso/xml/xml.c, line 1703 we find
subnode = lasso_node_new_from_xmlNode_with_type(t, matched_snippet->class_name);

For node <Assertion> this returns NULL (see below). Then, without checking whether subnode is NULL,
there is an attempt to add it to a list on line 1708, which causes a CRITICAL error. This is then followed by
a misleading Mellon error in the next line: the **Assertion** node is there, but it did not match the expected schema.

The reason lasso_node_new_from_xmlNode_with_type() returns NULL for assertion is as follows:

1. It calls lasso_node_init_from_xml() on line 2541.
2. This ultimately calls lasso_node_impl_init_from_xml() with type LassoSaml2Assertion.
3. It proceeds to process the child of the Assertion element according to the schema.
4. When it reaches **Signature**, it finds that there is no matching snippet, since **Signature** is out of place.
5. For the reason I did not have time to find, the error() macro does not print anything. If I replace it with call for message(), it prints the error, but the text "Node Signature cannot be parsed" is still misleading. The node is perfectly alright, but it is out of place due to the XML schema restrictions.

The patch that I propose:

- Avoids GList error when subnode is NULL
- Adds some diagnostics messages for debugging; I was not able to show Lasso's DEBUG messages in Apache Log, so I made a #define to raise their level to WARNING
- Prints more descriptive error messages that explain exactly what happened; I actually used this traces to figure out where the root cause of the problem is

Resulting error output (without debug traces) looks like this:

```
====================
process:27762): Lasso-CRITICAL **: 2016-08-03 21:48:15 (xml.c/:1709) Element &lt;http://www.w3.org
/2000/09/xmldsig#:Signature&gt; was not expected at this location inside element &lt;Assertion&ht;
. Please ensure the XML correctly follows XML schema

(process:27762): Lasso-CRITICAL **: 2016-08-03 21:48:15 (xml.c/:2570) Lasso node initialization fa
iled for node 'Assertion', type 'LassoSaml2Assertion': error 1
```

```
(process:27762): Lasso-CRITICAL **: 2016-08-03 21:48:15 (xml.c/:1721) Failed to create LassoNode f
rom XML node
[Wed Aug 03 21:48:15.889516 2016] [:error] [pid 27762] [client 10.90.8.176:61773] Error processing
 authn response. Lasso error: [-427] When looking for an assertion we did not found it.
====================
```

Demandes liées:

Lié à Lasso - Bug #12830: Macros WARNING, CRITICAL and ERROR log at the DEBUG...	**Fermé**	**04 août 2016**

Révisions associées

Révision db7e2528 - 06 septembre 2019 15:32 - Benjamin Dauvergne

Improve error logging during node parsing (#12829)

Révision 37a0fa6f - 09 septembre 2019 13:31 - Benjamin Dauvergne

Fix tests broken by new DEBUG logs (#12829)

Historique

#1 - 04 août 2016 00:12 - Ivan Krivyakov

The actual error text after patching, with the > garbage:

```
(process:27762): Lasso-CRITICAL **: 2016-08-03 21:48:15 (xml.c/:1709) Element <http://www.w3.org/2000/09/xmlds
ig#:Signature> was not expected at this location inside element <Assertion>. Please ensure the XML correctly f
ollows XML schema

(process:27762): Lasso-CRITICAL **: 2016-08-03 21:48:15 (xml.c/:2570) Lasso node initialization failed for nod
e 'Assertion', type 'LassoSaml2Assertion': error 1

(process:27762): Lasso-CRITICAL **: 2016-08-03 21:48:15 (xml.c/:1721) Failed to create LassoNode from XML node
Wed Aug 03 21:48:15.889516 2016] [:error] [pid 27762] [client 10.90.8.176:61773] Error processing authn respon
se. Lasso error: [-427] When looking for an assertion we did not found it.
```

#2 - 04 août 2016 00:44 - Benjamin Dauvergne

First thank you for the clear report and the patches; I'm currently on vacation but I will look at all that ASAP.

#3 - 04 août 2016 00:49 - Benjamin Dauvergne

- Lié à Bug #12830: Macros WARNING, CRITICAL and ERROR log at the DEBUG level when __GNUC__ is defined ajouté

#4 - 30 avril 2018 07:59 - Benjamin Dauvergne

Hi, your patch is ok, could I add an header to it with License: MIT ? It follows our contribution policy.

#5 - 28 juin 2018 10:43 - Benjamin Dauvergne

Ping.

#6 - 28 juin 2018 12:19 - Benjamin Dauvergne

- Version cible mis à future

#7 - 06 septembre 2019 14:49 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#8 - 06 septembre 2019 14:51 - Benjamin Dauvergne

- Version cible changé de future à 2.6.1

#9 - 06 septembre 2019 15:33 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

```
commit db7e25287aa48f6c5830f9e5c37b2bafb3f8bd6c
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Sep 6 14:50:24 2019 +0200

    Improve error logging during node parsing (#12829)
```

#10 - 22 avril 2020 21:51 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-Added-better-error-handing-to-xml.c.patch	5,58 ko	03 août 2016	Ivan Krivyakov
xml.c	103 ko	03 août 2016	Ivan Krivyakov
response.txt	5,99 ko	03 août 2016	Ivan Krivyakov
response.xml	3,92 ko	03 août 2016	Ivan Krivyakov