Lasso - Bug #24830

crash in lasso_profile_get_issuer on invalid content

27 juin 2018 18:10 - Frédéric Péters

Statut:	Fermé	**Début:**	27 juin 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.6.1		
Patch proposed:	Oui	**Planning:**	Non

Description

Using the Python binding:

```
>>> import lasso
>>> msg = 'SAMLRequest=Hello!!!fZHbasMwDIZfJfi+sXtYk5okkC4NFLZRtrGL3QzXUWnAsTNL2eHt56YUOga7Ekj69P+
SMlSd6WU50NE+wvsASNFXZyzKsZCzwVvpFLYoreoAJWn5VN7fyVksZO8dOe0Mu0L+JxQieGqdZdG2ytmbSNJkvZiv01WdJDdJL
RbLzXyTlnVZ1etVmrLoBTyG/pwFPECIA2wtkrIUUmKaTsRyMkuep0spFlLMXllUhR1aq2ikjkQ9Ss5VWBAstTo+eGhi47QysWj
iPfC26fnJ+YwjOhbVzmsY75GzgzIIJ9VdMN5+wCVTZCdAjm58cdHQrtu7v/OV1m6whLwDY5wNgVSjSPGMX0/Jzp94CDfbVjtnW
v0dlQH4vPWgKEiTH4Dx4kz9flnxAw==&SigAlg=http://www.w3.org/2000/09/xmldsig'
>>> lasso.profileGetIssuer(msg)
munmap_chunk(): invalid pointer

Aborted (core dumped)
```

(hopefully nobody uses this new API)

Révisions associées

Révision e29de316 - 28 juin 2018 10:30 - Benjamin Dauvergne

tools: fix segfault in lasso_get_saml_message (fixes #24830)

We reuse the "message" local variable but we should not.
Also fix a segfault in lasso_xmltextreader_from_message() when getting
the length of "message" before checking if it is NULL or not.

Historique

#1 - 27 juin 2018 19:27 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 27 juin 2018 19:29 - Benjamin Dauvergne

- Fichier 0001-tools-fix-segfault-in-lasso_get_saml_message-fixes-2.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 27 juin 2018 19:35 - Frédéric Péters

Should it also log something?

#4 - 27 juin 2018 22:52 - Benjamin Dauvergne

I don't think so, it will return NULL/None, it seems enough for the caller to see that something is wrong (and anyway internal function already log something at the DEBUG level).

#5 - 28 juin 2018 09:02 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

Works for me, ack.

#6 - 28 juin 2018 10:31 - Benjamin Dauvergne

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

- % réalisé changé de 0 à 100

Appliqué par commit e29de3160d71d215be51f74783006d382f366f97.

#7 - 28 juin 2018 10:34 - Benjamin Dauvergne

- Version cible mis à 2.6.1

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

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

Fichiers

0001-tools-fix-segfault-in-lasso_get_saml_message-fixes-2.patch	2,5 ko	27 juin 2018	Benjamin Dauvergne