


```
ZGhIM0JSLysxbFZWTkdSVlkycUgzSDQrOGNEYW9mZzVneTZvYXpnQi9xv1RaaXhtK2V1WkYxd1YKYS9UNVNSMENCZUZGNEpZQm
1DMEhXbDM5YjJicw9OR1YwSUXMS3lqRHJFODhwsFArazVQqkZlYjk4elJBWtk1ZgpQRE9QZmdGYzRnNjRXNzZmdnJpOHFmWHgz
NjY1VUFUT1RYbnZxbkZPbmlsQS9NbDkwMHVzdDVEeS9JS3lHZ1ZUCjR4Z20yblZRRDZlWW1nN1JqeWdhL0xCdFRFZUtnYzNrKy
tmTTV00EF6aGrvTknPr1ovRXoxUnp0YW5qRW9CelcKZFNybUhbR3N1bU1VeEZMUHBRSh5Z2xJWW1MN2ZFa3lRMEtNd1JjVERr
MHBWem1ORXFUTktRM2lQd3BNeitUVwpNOct3TWM5RmpOdFphR2MyMTNvbVdRPT0KPC9Nb2R1bHVzPgo8RXhwb25lbnQ%2BCkFR
QUIKPC9FeHBvbmVudD4KPC9SU0FLZXlWYwX1ZT4KPC9LZXlWYwX1ZT4KPC9LZXlJbmZvPgo8L1NpZ25hdHVyZT48c2FtbDpTdW
JqZWN0PjxzYW1sOk5hbWVJRCBGB3JtYXQ9InVybJjpvYXNpczpuYW1lc2p0YzptQU1MOjIuMDpuYW1laWQtZm9ybWF0OnBlcnNp
c3RlbnQiIE5hbWVRdWFSaWZpZXI9Imh0dHA6Ly9pZHA1L21ldGFkYXRhIiBTUE5hbWVRdWFSaWZpZXI9Imh0dHA6Ly90ZXN0c2
VydmVyL21ldGFkYXRhLyI%2BXzZFN0E2RDQwNUI3ODQyQjVFOUQ0NDQ3MDk3NzE0MDhBPC9zYW1sOk5hbWVJRD48c2FtbDpTdW
JqZWN0Q29uZml5bWF0aW9uIE1ldGhvZD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmNtOmJlYXJlciI%2BPHNhbWw6U3
ViamVjdENvbmZpcmlhdGlvbkrhdGEGTm90T25PckFmdGVyPSJGSVhNRSIgUmVjaXBpZW50PSJodHRwOi8vdGVzdHNNlcnZlci9s
b2dpbi8iIEluUmVzcG9uc2VUubz0iXzBFRDY2RkjcNkNENjU1ODc4Nj1lGOTMyMDA1NTA4NDNFIEi8%2BPC9zYW1sOlN1YmplY3RD
b25maxJtYXRpb24%2BPC9zYW1sOlN1YmplY3Q%2BPHNhbWw6Q29uZG10aW9ucyBob3RCZwZvcuU9IkZJWE1FIiBob3Rpbk9yQW
Z0ZXI9IkZJWE1FIj48c2FtbDpBdWRpZW5jZVJlc3RyaWN0aW9uPjxzYW1sOkF1ZG1lbmNlPmh0dHA6Ly90ZXN0c2VydmVyL21l
dGFkYXRhLzZwvc2FtbDpBdWRpZW5jZT48L3NhbWw6QXVkaWVuY2VSZXN0cm1jdGlvbj48L3NhbWw6Q29uZG10aW9uc248c2FtbD
pBdXRoblN0YXRlbWVudCBDbXRokluc3Rhbnc3RkZJWE1FIiBTZXNzaW9uSW5kZXg9Ii19BQThCQzE3NUMyMjNBRDQyREM5QzE4
QkFFODEzmg4NSI%2BPHNhbWw6QXV0aG5Db250ZXh0PjxzYW1sOkF1dGhuQ29udGV4dENsYXNzUmVmPnVybJjpvYXNpczpuYW1l
czp0YzptQU1MOjEuMDphbTpWYXNzd29yZDwvc2FtbDpBdXRokNvbnRleHRDbGFzc1JlZj48L3NhbWw6QXV0aG5Db250ZXh0Pj
wvc2FtbDpBdXRoblN0YXRlbWVudD48L3NhbWw6QXNzZXJ0aW9uPjwvc2FtbHA6UmVzcG9uc2U%2B')
```

No handlers could be found for logger "Lasso"
Erreur de segmentation

Whereas <http://rnd.feide.no/simplesaml/module.php/saml2debug/debug.php> seems to indicate that the SAML message is valid.

Révisions associées

Révision f33d51db - 28 juin 2018 23:16 - Benjamin Dauvergne

tools: set output buffer size in lasso_inflate to 20 times the input size (fixes #24853)

Historique

#1 - 28 juin 2018 22:51 - Benjamin Dauvergne

Sur le dernier Lasso je n'ai pas de segfault, tu peux retester en installant le dernier lasso de eobuilder ?

#2 - 28 juin 2018 23:04 - Benjamin Dauvergne

C'est bon j'ai trouvé le souci, ça compresse trop bien.

Par souci de simplicité plutôt que de chercher à allouer dynamiquement le buffer après décompression d'une requête j'alloue directement 10 fois la taille de la chaîne compressée en me disant que ça passerait toujours et puis paf là ça dépasse un facteur 10.

Un fix locale mais pas suffisant (mais pour comprendre le truc):

```
diff --git a/lasso/xml/tools.c b/lasso/xml/tools.c
index 6a9ce187..01533419 100644
--- a/lasso/xml/tools.c
+++ b/lasso/xml/tools.c
@@ -1353,11 +1353,11 @@ lasso_inflate(unsigned char *input, size_t len)
     zstr.zfree = NULL;
     zstr.opaque = NULL;

-    output = g_malloc(len*10);
+    output = g_malloc(len*100);
     zstr.avail_in = len;
     zstr.next_in = (unsigned char*)input;
     zstr.total_in = 0;
-    zstr.avail_out = len*10;
+    zstr.avail_out = len*100;
     zstr.total_out = 0;
     zstr.next_out = output;
```

#3 - 28 juin 2018 23:07 - Benjamin Dauvergne

Bon la connerie est pas de moi à l'origine, ouf ;) Enfin bon faut améliorer ça.

#4 - 28 juin 2018 23:09 - Frédéric Péters

Indeed I thought Paul would update its lasso version before copy/pasting the error; I told him it was still failing:

```
>>> lasso.profileGetIssuer(...)
2018-06-28 23:06:17,396 - Lasso - ERROR - 2018-06-28 23:06:17 (tools.c/:1373) Failed to inflate
```

>>>

While the string is successfully read by <http://rnd.feide.no/simplesaml/module.php/saml2debug/debug.php>

#5 - 28 juin 2018 23:18 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#6 - 28 juin 2018 23:18 - Benjamin Dauvergne

- Fichier 0001-tools-set-output-buffer-size-in-lasso_inflate-to-20-.patch ajouté
- Statut changé de Nouveau à Solution proposée
- Patch proposed changé de Non à Oui

La flemme de comprendre l'API de zlib en 20 minutes, je passe le buffer à 20x la taille du buffer d'entrée (on gaspille un peu mais pas trop).

#7 - 29 juin 2018 06:32 - Frédéric Péters

Go for it.

#8 - 29 juin 2018 07:23 - Benjamin Dauvergne

- Version cible mis à 2.6.1

#9 - 29 juin 2018 07:24 - Benjamin Dauvergne

- Statut changé de Solution proposée à Résolu (à déployer)
- % réalisé changé de 0 à 100

Appliqué par commit [f33d51db53373eb1f0a6429320e9de60210d5270](https://github.com/lasso-net/lasso/commit/f33d51db53373eb1f0a6429320e9de60210d5270).

#10 - 29 juin 2018 09:53 - Paul Marillonnet (retour le 15/04)

Frédéric Péters a écrit :

Indeed I thought Paul would update its lasso version before copy/pasting the error; I told him it was still failing:

Was using the stretch-testing and not the stretch-eobuilder repo, and I forgot to update, my bad.

#11 - 11 juillet 2018 17:52 - Frédéric Péters

- Statut changé de Résolu (à déployer) à En cours

Avec les données exposées en [#19396](#) (commentaire 146...) le problème apparait toujours.

En modifiant ma copie locale pour logger davantage, et aussi en passant le buffer à len*50.

```
2018-07-11 17:44:49,361 - Lasso - ERROR - 2018-07-11 17:44:49 (tools.c/:1373) Failed to inflate -3 (invalid code lengths set)
```

3 → Z_DATA_ERROR, Z_DATA_ERROR if the input data was corrupted (input stream not conforming to the zlib format or incorrect check value, in which case strm->msg points to a string with a more specific error). (strm-> msg is "invalid code lengths set").

#12 - 12 juillet 2018 14:22 - Benjamin Dauvergne

De fait ce payload n'est pas compressé, j'ai du rater un truc, je vais relire la spéc pour voir dans quel cas ne pas tenter la décompression.

#13 - 12 juillet 2018 14:28 - Benjamin Dauvergne

<https://www.oasis-open.org/committees/download.php/35387/sstc-saml-bindings-errata-2.0-wd-05-diff.pdf> ligne 612:

A query string parameter named SAMLEncoding is reserved to identify the encoding mechanism used. If this parameter is omitted, then the value is assumed to be urn:oasis:names:tc:SAML:2.0:bindings:URL-Encoding:DEFLATE.

Donc Lasso se comporte normalement en réception, je vais chercher maintenant pourquoi on a émis un contenu non compressé.

#14 - 12 juillet 2018 14:56 - Benjamin Dauvergne

- Statut changé de En cours à Résolu (à déployer)

Et donc c'était du binding HTTP POST, dans ce cas il faut filer directement le contenu de SAMLResponse pas l'encodage du formulaire complet.

#15 - 12 juillet 2018 14:57 - Benjamin Dauvergne

```
In [6]: import urlparse
```

```
In [7]: content = urlparse.parse_qs(payload)['SAMLResponse'][0]
```

```
In [8]: lasso.profileGetIssuer(content)
```

```
Out[8]: 'http://idp5/metadata'
```

#16 - 06 septembre 2019 14:40 - Benjamin Dauvergne

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

Fichiers

0001-tools-set-output-buffer-size-in-lasso_inflate-to-20-.patch	858 octets	28 juin 2018	Benjamin Dauvergne
---	------------	--------------	--------------------