

Lasso - Bug #86472

Segmentation fault inside test suite

01 février 2024 20:17 - Martin Schreiner

Statut:	Résolu (à déployer)	Début:	26 janvier 2024
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposé:	Oui		

Description

Hello,

On some systems, such as SUSE Linux Enterprise 15 SP5, we're seeing that **lasso-2.6.1** and **lasso-2.8.2** fail to build, as its **test suite hits a segmentation fault**.

Through careful analysis, we've discovered the exact instruction that triggers the segfault.

```
0x7ffff7c84b00 <xmlDictOwns>; test %rsi,%rsi

0x7ffff7c84b03 <xmlDictOwns+3>; sete %cl

0x7ffff7c84b06 <xmlDictOwns+6>; test %rdi,%rdi

0x7ffff7c84b09 <xmlDictOwns+9>; je 0x7ffff7c84b4e <xmlDictOwns+78>;

0x7ffff7c84b0b <xmlDictOwns+11>; test %cl,%cl

0x7ffff7c84b0d <xmlDictOwns+13>; jne 0x7ffff7c84b4e <xmlDictOwns+78>;

--> 0x7ffff7c84b0f <xmlDictOwns+15>; mov 0x20(%rdi),%rax

0x7ffff7c84b13 <xmlDictOwns+19>; test %rax,%rax

0x7ffff7c84b16 <xmlDictOwns+22>; je 0x7ffff7c84b37 <xmlDictOwns+55>;

0x7ffff7c84b18 <xmlDictOwns+24>; nopl 0x0(%rax,%rax,1)

0x7ffff7c84b20 <xmlDictOwns+32>; lea 0x28(%rax),%rdx

0x7ffff7c84b24 <xmlDictOwns+36>; cmp %rdx,%rsi

0x7ffff7c84b27 <xmlDictOwns+39>; jb 0x7ffff7c84b2f <xmlDictOwns+47>;

0x7ffff7c84b29 <xmlDictOwns+41>; cmp %rsi,0x8(%rax)

0x7ffff7c84b2d <xmlDictOwns+45>; jae 0x7ffff7c84b48 <xmlDictOwns+72>;
```

This happens when running the following test: **test16_test_get_issuer_fn (basic_tests.c:1019)**.

This test contains a loop, and it doesn't happen the first time the instruction is executed. It takes over 30 thousand attempts, but then it always causes a segfault.

Various other tests, typically login-related ones, also trigger this issue.

On SLE 15 SP5 specifically, we're using libxml2 version 2.10.3.

I'm including a patch we've written that seems to mitigate the issue, hopefully you can have a look and see how it might mitigate this problem, and maybe other people are also being affected.

We have a build of lasso-2.8.2 running here, with the patch:

<https://build.opensuse.org/package/show/home:pgajdos/lasso>

Thanks.

Révisions associées

Révision 534d2b96 - 01 février 2024 21:50 - Benjamin Dauvergne

Do not free xmlDoc before unlinking its tree (#86472)

Historique

#1 - 01 février 2024 21:50 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 01 février 2024 21:54 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

```
commit 534d2b96985714598d58b2da947d5813efe1e67c
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date: Thu Feb 1 21:50:21 2024 +0100
```

```
Do not free xmlDoc before unlinking its tree (#86472)
```

#3 - 01 février 2024 21:54 - Benjamin Dauvergne

- Catégorie Tests supprimé

It's fixed in main, thanks for the report.

#4 - 01 février 2024 23:08 - Martin Schreiner

Do you think it'd be possible to backport a patch, fix it for 2.6.X as well?
I mean, if that commit applies cleanly for 2.6.X, should it be good to go?

I want to fix this for SLE 15 SP5.

Thank you very much!

#5 - 02 février 2024 00:26 - Benjamin Dauvergne

Martin Schreiner a écrit :

```
Do you think it'd be possible to backport a patch, fix it for 2.6.X as well?
I mean, if that commit applies cleanly for 2.6.X, should it be good to go?
```

Sorry but we do not manage backports upstream, we provide fixes only in the latest version.

Fichiers

lasso.patch

461 octets

01 février 2024

Martin Schreiner