LTTng-tools - Bug #833

memcpy of non-packed struct into packed struct (possible layout mismatch)

09/09/2014 09:17 AM - Mathieu Desnoyers

Status:	Confirmed	**Start date:**	09/09/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2.9		

Description

lttng-tools src/lib/lttng-ctl/lttng-ctl.c:

lttng_enable_event_with_exclusions()

memcpy(&lsm.u.enable.event, ev, sizeof(lsm.u.enable.event));

copy "ev" (non-packed) into a packed structure.

We should copy each field one by one (create a copy_event_to_event_packed() helper to do so).

History

#1 - 09/11/2014 02:17 PM - David Goulet

- Status changed from New to Feedback

How do you copy the union in the lttng_event field by field... ? That union contains non packed structure.

#2 - 09/30/2014 02:16 PM - David Goulet

- Status changed from Feedback to Confirmed

- Assignee deleted (David Goulet)

We need helper functions to copy field by field depending on the union type also.

#3 - 11/07/2014 02:52 PM - Christian Babeux

- Target version set to 20

#4 - 12/12/2014 11:19 AM - Christian Babeux

- Target version changed from 20 to 2.7

#5 - 08/14/2015 03:09 PM - Michael Jeanson

The "lttng_event" struct is not defined with the packed attribute, this attribute is only added when "lttng_event" is declared as a member of the "lttcomm_session_msg" struct. Adding the packed attribute to an already defined struct is ignored by the compiler, when it's done outside of a parent struct it generates a warning.

What this all means is that we are not copying a non-packed struct into a packed struct because there is no packed version of lttng_event. This also means we are using unpacked structures in the communication protocol between the client and the sessiond.

#6 - 09/01/2015 04:09 PM - Jérémie Galarneau

- Target version changed from 2.7 to 2.8

#7 - 05/04/2016 10:34 PM - Jérémie Galarneau

- Target version changed from 2.8 to 2.9