Klever - Bug #7670

Instrumentation of memory allocation functions from driver code should correctly pass size of memory

11/01/2016 04:02 PM - Vadim Mutilin

Status:	Closed	**Start date:**	11/01/2016
Priority:	Urgent	**Due date:**	
Assignee:	Anton Vasilyev	**% Done:**	100%
Category:	Rule specifications	**Estimated time:**	0.00 hour
Target version:	1.0		
Detected in build:	svn	**Published in build:**	
Platform:			

Description

Now function allocations with known size like kmalloc are replaced with ldv_malloc_unknown_size.
Thus size parameter is lost.

See for example aspect

```
around: ALLOC_KNOWN_SIZE
{
        void *res;
        ldv_check_alloc_flags(flags);
        res = ldv_malloc_unknown_size();
        ldv_after_alloc(res);
        return res;
}
```

In correct case ldv_malloc(size) should be called.

Related issues:

Related to Klever - Feature #7481: Try to use memory allocating function mode...	**New**	**08/17/2016**
Related to Klever - Feature #7971: Rule specification generic:memory lacks te...	**Closed**	**02/13/2017**

History

#1 - 11/01/2016 04:03 PM - Vadim Mutilin

- Description updated

#2 - 11/01/2016 04:05 PM - Vadim Mutilin

- Description updated

#3 - 12/27/2016 09:43 AM - Evgeny Novikov

- Assignee set to Evgeny Novikov

I also noticed this issue and I hope that I will be able to fix it together with fixes and improvements in other rule specifications.

#4 - 08/31/2017 10:26 AM - Evgeny Novikov

- Priority changed from Urgent to High

Let's fix and improve specifications after we will have good tests and a testing infrastructure (version:0.3) and likely after we will complete a considerable refactoring of Core (1.0).

#5 - 06/18/2018 02:29 PM - Evgeny Novikov

- Target version set to 1.0

- Priority changed from High to Urgent

- Assignee changed from Evgeny Novikov to Anton Vasilyev

It seems that we lose dozens of bugs and hundreds of false alarms due to this issue. Since its fix is trivial, we can include into Klever 1.0.

#6 - 06/18/2018 02:29 PM - Evgeny Novikov

- Related to Feature #7971: Rule specification generic:memory lacks test cases added

#7 - 06/19/2018 04:48 PM - Anton Vasilyev

- % Done changed from 0 to 100

- Assignee changed from Anton Vasilyev to Evgeny Novikov

- Status changed from New to Resolved

Fixed on branch fix_alloc_known_size, 68b24c59214

#8 - 06/20/2018 06:53 PM - Anton Vasilyev

Rebase on master is done in branch fix_alloc_known_size_rebase 92d9f523f ready to merge

#9 - 06/21/2018 04:50 PM - Anton Vasilyev

- Assignee changed from Evgeny Novikov to Anton Vasilyev

Tested with generic:memory

#10 - 06/22/2018 10:22 AM - Evgeny Novikov

I fixed it a bit in the same branch, updated preset marks and scheduled a comprehensive testing. If it will pass, I will merge the branch to master.

#11 - 06/22/2018 05:38 PM - Evgeny Novikov

I had to update the branch one more time and started one more iteration of testing, since tests identified differences in associated marks. Indeed, this happens first of all because of we still have very bad aspects for some rule specifications causing auxiliary functions ending with \d+ in error trace patterns (of course any slight change in instrumentation can result in changes in error trace patterns). Other cases can be expected because of there were calls to *kmalloc* in test drivers and in corresponding error trace patterns. Now there are calls to *ldv_kmalloc*.

#12 - 06/23/2018 08:14 AM - Evgeny Novikov

- Status changed from Resolved to Closed

Tests passed, so I merged the branch to master in a354b4c6.

Besides, there isn't any feature requests for Klever 1.0. So, that commit is tagged with *1.0rc1*! From now until release just bug fixes can find their way to master.