Linux Kernel Safety RuleDB - Feature #3317

010: Usage of a GFP_ATOMIC flag in functions of memory allocation in a context of interrupt.

08/01/2012 07:08 PM - Vladimir Gratinskiy

Status:	Resolved	**Start date:**	08/01/2012
Priority:	Normal	**Due date:**	08/08/2012
Assignee:	Vladimir Gratinskiy	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			
Published in build:			

Description

When calling memory allocation function from the context of interrupt it's required to ensure a non-preemptible execution of the function; but in the case of GFP_KERNEL flag, function execution can be preempted, because a greater number of operations to find and allocate memory blocks is executed.

Verification: If some function is positioned as one that "is executed in a context of interrupt" then it's required to ensure checking for a necessary usage of the GFP_ATOMIC flag in the memory allocation functions for kernel modules.

Example:
void* ptr = kmalloc(size, GFP_ATOMIC);

Related issues:

Related to C Instrumentation Framework - Feature #3802: Add ability to refer ...	**Closed**	**12/14/2012**

History

#1 - 08/06/2012 12:38 PM - Vladimir Gratinskiy

- % Done changed from 10 to 90

I've found 5 unsafes.

#2 - 08/08/2012 02:34 PM - Vladimir Gratinskiy

- Due date set to 08/08/2012

- Status changed from Open to Resolved

- % Done changed from 90 to 100

I've found 2 true unsafes. Results here:
http://itgdev.intra.ispras.ru/wiki/index.php/Nice_table

Now this rule's name is 10_2a.

#3 - 08/19/2012 07:50 PM - Evgeny Novikov

Vladimir Gratinskiy wrote:

> Now this rule's name is 10_2a.

More correctly, *10_2a* is a model identifier (or model name), since the same rule may have different models implementing it. This rule seems to have 2 models for instance.
And another question. What is the difference between 10_1a and 10_2a models? If 10_1a is included into 10_2a model then it should be completely replaced with it.

#4 - 08/20/2012 02:23 PM - Vladimir Gratinskiy

Rule model 10_1a have been deleted. 10_2a includes functions that was in 10_1a but I've added some new similar functions. So, "10_2a" means that rule 10 wasn't changed, but now its model version is 2.

#5 - 08/20/2012 04:15 PM - Evgeny Novikov

Vladimir Gratinskiy wrote:

> Rule model 10_1a have been deleted. 10_2a includes functions that was in 10_1a but I've added some new similar functions. So, "10_2a"

means that rule 10 wasn't changed, but now its model version is 2.

A number used in a model identifier after a rule identifier isn't a model *version*. That number is intended to distinguish models implementing different approaches for the same rule. For instance, one rule may have a rerouting model and a non rerouting model. This case to distinguish these models one should use different postfixes.
So, to correspond to the common naming scheme you have to use *10_1a* identifier instead of *10_2a*.

#6 - 01/29/2013 08:30 PM - Evgeny Novikov

- Status changed from Resolved to Open

Please, use ability to refer to function argument by its name specified in aspect file (implemented in #3802).

#7 - 01/29/2013 08:31 PM - Evgeny Novikov

- Assignee changed from Vladimir Gratinskiy to Ilya Shchepetkov

#8 - 02/11/2013 08:37 PM - Ilya Shchepetkov

- Status changed from Open to Resolved

The ability to refer to function argument by its name specified in aspect file was added in the commit b4b7331 of master branch.

Tests passed.

#9 - 05/27/2013 11:31 AM - Evgeny Novikov

- Assignee changed from Ilya Shchepetkov to Vladimir Gratinskiy

Ilya just has developed a small part of the rule specification.

#10 - 09/26/2014 07:27 PM - Vitaly Mordan

Some functions in "before: ALLOC", "around: ALLOC_AROUND" and "before: ALLOC_WITHOUT" (for example, static inline void *kmalloc(.., gfp_t flags, ..) and static inline void *kzalloc(.., gfp_t flags, ..)) will always return 0, which makes some pathes in program infeasible.