# Klever - Feature #10488

## Develop models for devm memory allocating functions

09/03/2020 02:48 PM - Evgeny Novikov

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 09/03/2020 |
| **Priority:** | Urgent | **Due date:** | |
| **Assignee:** | Evgeny Novikov | **% Done:** | 0% |
| **Category:** | Environment model | **Estimated time:** | 0.00 hour |
| **Target version:** | 3.0 | | |
| **Published in build:** | | | |

**Description**

At the moment there just models for *devm_kzalloc* and *devm_iio_device_alloc* used for checking memory safety. Those models are not accurate since allocated memory is not tracked by CPAchecker SMG.

I suggest to develop accurate models that will cause a verifier to track the memory. In addition, they will store pointers to allocated memory within a global list, but just for memory safety checking since lists are too complicated for reachability checking.

### History

#### #1 - 09/03/2020 09:51 PM - Evgeny Novikov

*- Status changed from New to Resolved*

I implemented models in branch *devm-alloc-models*. Since they are quite important, I will perform several large experiments for evaluation.

#### #2 - 09/04/2020 05:48 PM - Evgeny Novikov

*- Status changed from Resolved to Closed*

Surprisingly new models demonstrated numerous problems with verifiers. Likely this is the case because of corresponding functions are quite popular in the Linux kernel.

CPAchecker BAM started to fail sometimes. Besides, it reported timeouts rather than finding some good results even when models do not affect corresponding verification tasks.

CPAchecker SMG works much worse. It started to produce plenty of new false alarms due to inaccurate analysis of predicates, lack of type attributes support and so on.

Despite bad verification results I merged the branch to master:018aa6a68 with hope that one day CPAchecker developers will fix crucial issues within their tool.