Subject: : AmigaOS4
Topic: : Porting to AmigaOS4 thread
Re: Porting to AmigaOS4 thread
Author: : kas1e
Date: : 2021/1/13 15:32:39
URL:

@sTix
Quote:

> With gcc 10 you can also use the -fanalyzer option to find even more bugs

Wow, tried simple test case with wrong-double-free:

```
 #include<stdio.h>
#include <stdlib.h>

int main()
{
	int *ptr_one;

	ptr_one = (int *)malloc(sizeof(int));

	if (ptr_one == 0)
	{
		printf("ERROR: Out of memoryn");
		return 1;
	}

	*ptr_one = 25;
	printf("%dn", *ptr_one);

	free(ptr_one);
	free(ptr_one);

	return 0;
}
```

And -fanalyzer works, see:

```
 user@DESKTOP-3NFAB0O /amiga
$ ppc-amigaos-gcc -fanalyzer 1.c -o 1
1.c: In function ‘main’:
1.c:20:9: warning: double-‘free’ of ‘ptr_one’ [CWE-415] [-Wanalyzer-double-free]
   20 |         free(ptr_one);
      |         ^~~~~~~~~~~~~
  ‘main’: events 1-6
    |
    |    8 |         ptr_one = (int *)malloc(sizeof(int));
    |      |                   ^~~~~~~~~~~~~~~~~~~~~~~~~~
    |      |                   |
    |      |                   (1) allocated here
    |    9 |
    |   10 |         if (ptr_one == 0)
    |      |            ~
    |      |            |
    |      |            (2) assuming ‘ptr_one’ is non-NULL
    |      |            (3) following ‘false’ branch (when ‘ptr_one’ is non-NULL)...
    |......
    |   16 |         *ptr_one = 25;
    |      |         ~~~~~~~~~~~~~
    |      |                 |
    |      |                 (4) ...to here
    |      |                 (5) first ‘free’ here
    |......
    |   20 |         free(ptr_one);
    |      |         ~~~~~~~~~~~~~
    |      |         |
    |      |         (6) second ‘free’ here; first ‘free’ was at (5)
    |

user@DESKTOP-3NFAB0O /amiga
```