CentraleSupélec

université PARIS-SACLAY

TP n°1

AnaStat

Réalisé par :
Merlin Baviere

1 CERT C EXP33-C. Do not read uninitialized memory

On lance frama-c -eva -main is_negative cert_exp_33.c. On a une alarme access to uninitialized left-values [Figure 1]. Elle provient du fait que le cas number = 0 n'est pas traité. En ouvrant l'interface [Figure 2] on ne remarque aucune Red Alarm

```
[eva] ====== VALUES COMPUTED ======
[eva:final-states] Values at end of function set_flag:
  sign ∈ {-1; 1} or UNINITIALIZED
[eva:final-states] Values at end of function is_negative:
  sign ∈ {-1; 1}
  __retres ∈ {0; 1}
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 9 statements reached (out of 11): 81% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  1 alarm generated by the analysis:
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  No logical properties have been reached by the analysis.
  ------------------------------------------------------------------------------
```

FIGURE 1 – frama-c -eva -main is_negative cert_exp_33.c

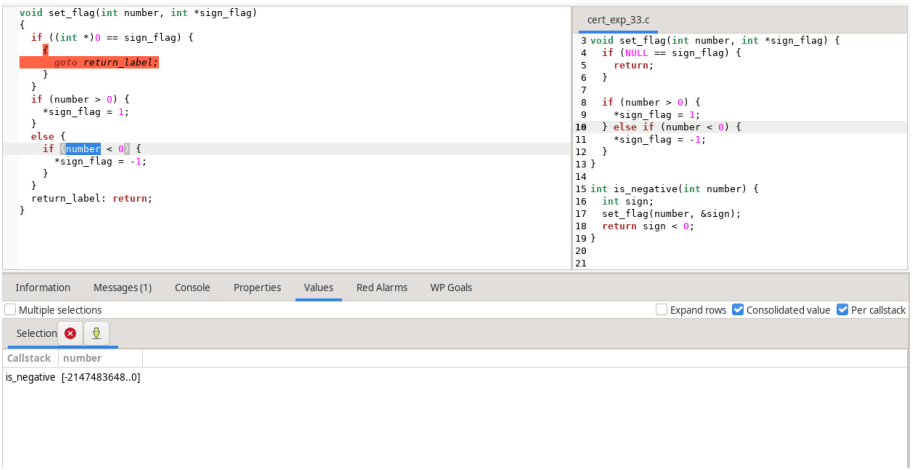

FIGURE 2 – frama-c-gui -eva -main is_negative cert_exp_33.c

1.1 Afficher des valeurs en cours d'analyse

Avec l'ajout des appels Frama_C_show_each_*, on observe le résultat [Figure 3]

```
[eva] cert_exp_33.c:13:
  Frama_C_show_each_set_flag: [-2147483648..2147483647], {-1; 1}
[eva] cert_exp_33.c:19:
  Frama_C_show_each_is_negative: [-2147483648..2147483647], {-1; 1}
[eva:alarm] cert_exp_33.c:20: Warning:
  accessing uninitialized left-value. assert \initialized(&sign);
```

FIGURE 3 – Avec Frama_C_show_each_*

1.2 Partitionner les traces

Avec l'option -eva-partition-history, on obtient les résultats [Figure 4] et [Figure 5].

```
[eva:initial-state] Values of globals at initialization

[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: [-2147483648..0], {-1}
[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: [1..2147483647], {1}
[eva] cert_exp_33.c:19:
  Frama_C_show_each_is_negative: [-2147483648..2147483647], {-1; 1}
[eva:alarm] cert_exp_33.c:20: Warning:
  accessing uninitialized left-value. assert \initialized(&sign);
[eva] ====== VALUES COMPUTED ======
[eva:final-states] Values at end of function set_flag:
  sign ∈ {-1; 1} or UNINITIALIZED
[eva:final-states] Values at end of function is_negative:
  sign ∈ {-1; 1}
  __retres ∈ {0; 1}
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 11 statements reached (out of 13): 84% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  1 alarm generated by the analysis:
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  No logical properties have been reached by the analysis.
  ------------------------------------------------------------------------------
```

FIGURE 4 – Avec -eva-partition-history 1

```
[eva:initial-state] Values of globals at initialization

[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: {0}, ⊥
[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: [-2147483648..-1], {-1}
[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: [1..2147483647], {1}
[eva] cert_exp_33.c:19:
  Frama_C_show_each_is_negative: [-2147483648..2147483647], {-1; 1}
[eva:alarm] cert_exp_33.c:20: Warning:
  accessing uninitialized left-value. assert \initialized(&sign);
[eva] ====== VALUES COMPUTED ======
[eva:final-states] Values at end of function set_flag:
  sign ∈ {-1; 1} or UNINITIALIZED
[eva:final-states] Values at end of function is_negative:
  sign ∈ {-1; 1}
  __retres ∈ {0; 1}
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 11 statements reached (out of 13): 84% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  1 alarm generated by the analysis:
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  No logical properties have been reached by the analysis.
  ------------------------------------------------------------------------------
```

FIGURE 5 – Avec -eva-partition-history 5

1.3 Partitionnement inter-procédural

Avec un partitionnement inter-procédural, Frama-C semble mieux distinguer les différentes valeurs possibles de sign et set_flag [Figure 6]. Avec cette nouvelle option, on observe bien une alarme rouge [Figure 7].

```
[eva:initial-state] Values of globals at initialization

[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: {0}, ⊥
[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: [-2147483648..-1], {-1}
[eva] cert_exp_33.c:13: Frama_C_show_each_set_flag: [1..2147483647], {1}
[eva] cert_exp_33.c:19: Frama_C_show_each_is_negative: {0}, ⊥
[eva] cert_exp_33.c:19: Frama_C_show_each_is_negative: [-2147483648..-1], {-1}
[eva] cert_exp_33.c:19: Frama_C_show_each_is_negative: [1..2147483647], {1}
[eva:alarm] cert_exp_33.c:20: Warning:
  accessing uninitialized left-value. assert \initialized(&sign);
[eva] ====== VALUES COMPUTED ======
[eva:final-states] Values at end of function set_flag:
  sign ∈ {-1; 1} or UNINITIALIZED
[eva:final-states] Values at end of function is_negative:
  sign ∈ {-1; 1}
  __retres ∈ {0; 1}
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 11 statements reached (out of 13): 84% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  1 alarm generated by the analysis:
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  No logical properties have been reached by the analysis.
  ------------------------------------------------------------------------------
```

FIGURE 6 – Avec un partitionnement inter-procédural

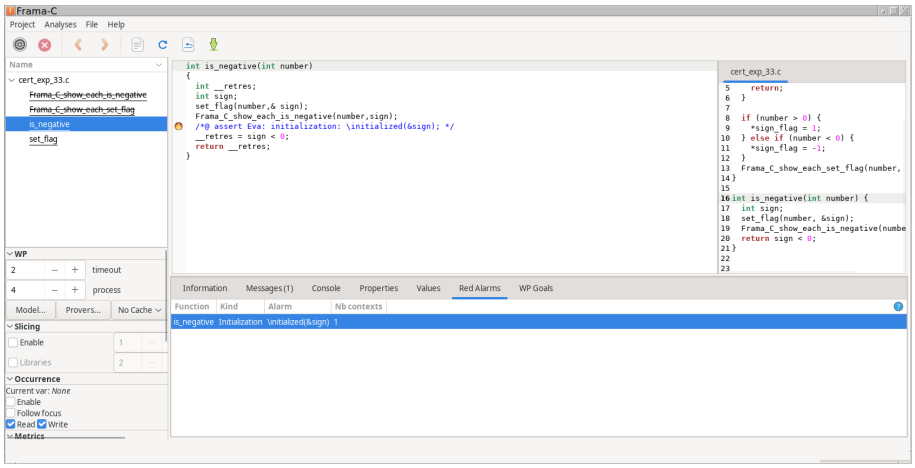

FIGURE 7 – Alarme Rouge

1.4 Analyse du code corrigé

2 CERT C EXP33-C bis

2.1 Première analyse

On lance Eva en prenant func comme point d'entrée [Figure 9]. On a une alarme escaping address et une access to uninitialized left-values. La seconde correspond à la lecture d'une location mémoire non-initialisée.

2.2 Augmenter la précision des boucles

On choisit d'utiliser l'option -eva-min-loop-unroll 10. On observe le résultat [Figure 10]. On remarque qu'à chaque itération dans la boucle, on a soit un chiffre soit UNINITIALIZED. On décide de rajouter un Frama_C_show_each_func(array) dans la boucle for [Figure 11], cela ne semble pas donner de renseignements supplémentaires analysables.

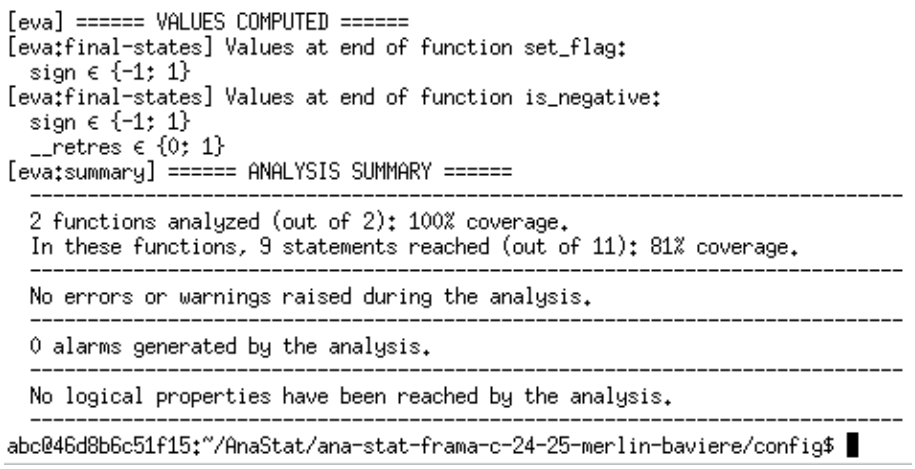

FIGURE 8 – Analyse du code corrigé, il n'y a pas d'erreur

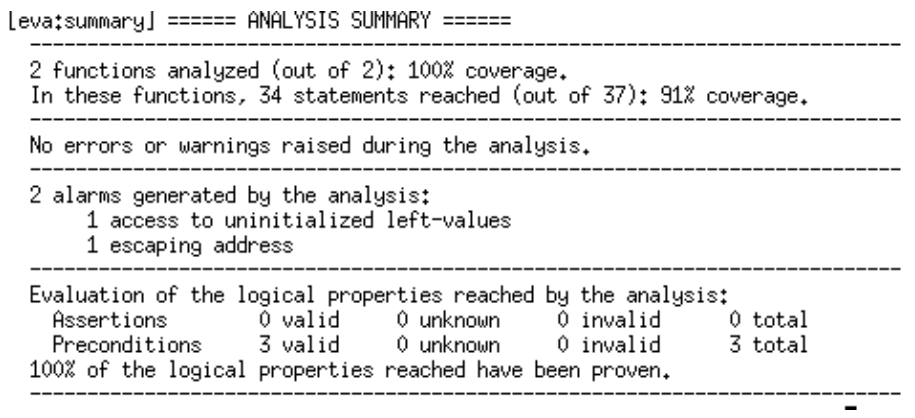

FIGURE 9 – Première analyse

2.3 Analyse précise de realloc

On ajoute //@ split ret==0 ; pour analyser séparément quand ret vaut 0 ou non. Avec cet ajout, l'alarme sur free(array) disparait bien. [Figure 12]

2.4 Analyse de la version corrigée

En utilisant la version corrigée on obtient toujours les mêmes erreurs [Figure 13]. Elles disparaissent si on rajoute //@ split ret==0 ; après l'appel à realloc et on utilise l'argument -eva-min-loop-unroll 10.

3 CWE20

On observe 5 alarmes. 5 integer overflows, 2 invalid access memory et 1 access to uninitialized left-values. Les 5 premières sont liées aux valeurs de m et n car on peut entrer des valeurs négatives, or cela ne devrait pas être possible. Les 2 suivantes sont probablement liées au malloc.

3.1 Patch 1

Le problème décrit dans la page du CWE20 repose sur les valeurs négatives possibles de m et n. On rajoute donc des gardes m,n > 0 dans le cas contraire on redirige vers die. On observe l'analyse frama-c suivante. Même en modifiant les options de précision les alarmes persistent.

3.2 Patch 2

En modifiant le programme en rajoutant une vérification sur board, les alarmes sur la mémoire persistent. Alors en rajoutant //@ split m et //@ split n avant l'assignation de board, on est capable d'enlever ces alarmes

```
[eva] ====== VALUES COMPUTED ======
[eva:final-states] Values at end of function resize_array:
  array ∈ {{ &__malloc_func_l21[0] }} or ESCAPINGADDR
  ret ∈ {{ NULL ; &__realloc_resize_array_l10[0] }}
  array ∈ {{ &__malloc_func_l21[0] }} or ESCAPINGADDR
  __retres ∈ {{ NULL ; &__realloc_resize_array_l10[0] }}
[eva:final-states] Values at end of function func:
  __fc_heap_status ∈ [--..--]
  array ∈ {0}
  S___fc_stdout[0..1] ∈ [--..--]
  __malloc_func_l21[0] ∈ {0} or UNINITIALIZED
                   [1] ∈ {1} or UNINITIALIZED
                   [2] ∈ {2} or UNINITIALIZED
                   [3] ∈ {3} or UNINITIALIZED
                   [4] ∈ {4} or UNINITIALIZED
                   [5] ∈ {5} or UNINITIALIZED
                   [6] ∈ {6} or UNINITIALIZED
                   [7] ∈ {7} or UNINITIALIZED
                   [8] ∈ {8} or UNINITIALIZED
                   [9] ∈ {9} or UNINITIALIZED
[eva:summary] ====== ANALYSIS SUMMARY ======
  ----------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 33 statements reached (out of 37): 89% coverage.
  ----------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ----------------------------------------------------------------------------
  2 alarms generated by the analysis:
       1 access to uninitialized left-values
       1 escaping address
  ----------------------------------------------------------------------------
  Evaluation of the logical properties reached by the analysis:
    Assertions        0 valid     0 unknown     0 invalid      0 total
    Preconditions     3 valid     0 unknown     0 invalid      3 total
  100% of the logical properties reached have been proven.
  ----------------------------------------------------------------------------
```

FIGURE 10 – -eva-min-loop-unroll 10

```
[eva] cert_exp_33_realloc.c:21: allocating variable __malloc_func_l21
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:29: Frama_C_show_each_func: {{ &__malloc_func_l21 }}
[eva] cert_exp_33_realloc.c:10: allocating variable __realloc_resize_array_l10
[eva:alarm] cert_exp_33_realloc.c:12: Warning:
  accessing left-value that contains escaping addresses.
  assert ¬\dangling(&array);
[eva] using specification for function printf_va_1
[eva:alarm] cert_exp_33_realloc.c:39: Warning:
  accessing uninitialized left-value. assert \initialized(array + i_0);
```

FIGURE 11 – -eva-min-loop-unroll 10 avec ajout de Frama_C_show_each_*

mémoires. [Figure 16]

4 libstring

On créé les fichiers concat.c et replace.c demandé. Leur analyse avec frama-c ne retourne pas de warning. [Figure 12] [Figure 18]

```
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 34 statements reached (out of 38): 89% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  1 alarm generated by the analysis:
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  Evaluation of the logical properties reached by the analysis:
    Assertions       0 valid     0 unknown     0 invalid      0 total
    Preconditions    3 valid     0 unknown     0 invalid      3 total
  100% of the logical properties reached have been proven.
  ------------------------------------------------------------------------------
```

FIGURE 12 – Avec //@ split ret==0 ;

```
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 36 statements reached (out of 39): 92% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  2 alarms generated by the analysis:
       1 access to uninitialized left-values
       1 escaping address
  ------------------------------------------------------------------------------
```

FIGURE 13 – Erreur zeno

```
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 35 statements reached (out of 39): 89% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  8 alarms generated by the analysis:
       5 integer overflows
       2 invalid memory accesses
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  Evaluation of the logical properties reached by the analysis:
    Assertions       0 valid     0 unknown     0 invalid      0 total
    Preconditions    8 valid     0 unknown     0 invalid      8 total
  100% of the logical properties reached have been proven.
  ------------------------------------------------------------------------------
```

FIGURE 14 – CWE20 Avant Patch

```
[eva:summary] ====== ANALYSIS SUMMARY ======
  ------------------------------------------------------------------------------
  2 functions analyzed (out of 2): 100% coverage.
  In these functions, 41 statements reached (out of 45): 91% coverage.
  ------------------------------------------------------------------------------
  No errors or warnings raised during the analysis.
  ------------------------------------------------------------------------------
  3 alarms generated by the analysis:
       2 invalid memory accesses
       1 access to uninitialized left-values
  ------------------------------------------------------------------------------
  Evaluation of the logical properties reached by the analysis:
    Assertions       0 valid     0 unknown     0 invalid      0 total
    Preconditions    8 valid     0 unknown     0 invalid      8 total
  100% of the logical properties reached have been proven.
  ------------------------------------------------------------------------------
```

FIGURE 15 – CWE20 Après Patch 1

```
------------------------------------------------------------------------------
2 functions analyzed (out of 2): 100% coverage.
In these functions, 48 statements reached (out of 52): 92% coverage.
------------------------------------------------------------------------------
No errors or warnings raised during the analysis.
------------------------------------------------------------------------------
1 alarm generated by the analysis:
    1 access to uninitialized left-values
------------------------------------------------------------------------------
Evaluation of the logical properties reached by the analysis:
  Assertions       0 valid     0 unknown     0 invalid      0 total
  Preconditions    9 valid     0 unknown     0 invalid      9 total
100% of the logical properties reached have been proven.
------------------------------------------------------------------------------
```

FIGURE 16 – CWE20 Après Patch 2

```
------------------------------------------------------------------------------
1 function analyzed (out of 12): 8% coverage.
In this function, 30 statements reached (out of 41): 73% coverage.
------------------------------------------------------------------------------
Some errors and warnings have been raised during the analysis:
  by the Eva analyzer:      0 errors    0 warnings
  by the Frama-C kernel:    0 errors    2 warnings
------------------------------------------------------------------------------
0 alarms generated by the analysis.
------------------------------------------------------------------------------
Evaluation of the logical properties reached by the analysis:
  Assertions       0 valid     0 unknown     0 invalid      0 total
  Preconditions    3 valid     0 unknown     3 invalid      6 total
50% of the logical properties reached have been proven.
------------------------------------------------------------------------------
```

FIGURE 17 – concat.c

```
------------------------------------------------------------------------------
1 function analyzed (out of 12): 8% coverage.
In this function, 32 statements reached (out of 46): 69% coverage.
------------------------------------------------------------------------------
Some errors and warnings have been raised during the analysis:
  by the Eva analyzer:      0 errors    0 warnings
  by the Frama-C kernel:    0 errors    2 warnings
------------------------------------------------------------------------------
0 alarms generated by the analysis.
------------------------------------------------------------------------------
Evaluation of the logical properties reached by the analysis:
  Assertions       0 valid     0 unknown     0 invalid      0 total
  Preconditions    4 valid     0 unknown     3 invalid      7 total
57% of the logical properties reached have been proven.
------------------------------------------------------------------------------
```

FIGURE 18 – replace.c