UE Etude de cas
Annexe Valgrind Client_brute_force

Université de la Rochelle
Licence Informatique (L3)
Années 2016-2017

Nicola Foissac <nicola.foissac@etudiant.univ-lr.fr>
Quentin Rouanet <quentin.rouanet@etudiant.univ-lr.fr>
Quentin Pouvreau <quentin.pouvreau@etudiant.univ-lr.fr>

Annexe Valgrind Client_brute_force

```
==11016== Memcheck, a memory error detector
==11016== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==11016== Using Valgrind-3.12.0.SVN and LibVEX; rerun with -h for copyright info
==11016== Command: ./client_brute_force
==11016== Parent PID: 2187
==11016==
==11016== Invalid write of size 1
==11016==    at 0x10980A: gen_random (client_brute_force.c:171)
==11016==    by 0x10A342: main (client_brute_force.c:415)
==11016==  Address 0x63c5c8f is 0 bytes after a block of size 15 alloc'd
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x10A306: main (client_brute_force.c:413)
==11016==
==11016== Invalid read of size 1
==11016==   at 0x4C2FD44: strlen (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x1091AC: open_client_sockets (client_brute_force.c:20)
==11016==    by 0x109463: create_client_data (client_brute_force.c:78)
==11016==    by 0x10A37E: main (client_brute_force.c:419)
==11016==  Address 0x63c5c8f is 0 bytes after a block of size 15 alloc'd
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x10A306: main (client_brute_force.c:413)
==11016==
==11016== Invalid read of size 1
==11016==   at 0x4C2FD44: strlen (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x109218: open_client_sockets (client_brute_force.c:23)
==11016==    by 0x109463: create_client_data (client_brute_force.c:78)
==11016==    by 0x10A37E: main (client_brute_force.c:419)
==11016==  Address 0x63c5c8f is 0 bytes after a block of size 15 alloc'd
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x10A306: main (client_brute_force.c:413)
==11016==
==11016== Invalid write of size 8
==11016==    at 0x109C71: unserialize_word_list (client_brute_force.c:253)
==11016==    by 0x10A402: main (client_brute_force.c:429)
```

```
==11016==  Address 0x63f18b0 is 0 bytes after a block of size 16 alloc'd
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x109B52: unserialize_word_list (client_brute_force.c:236)
==11016==    by 0x10A402: main (client_brute_force.c:429)
==11016==
==11016== Invalid read of size 8
==11016==    at 0x10AF96: force_brute (force_brute.c:196)
==11016==    by 0x10A4C4: main (client_brute_force.c:448)
==11016==  Address 0x63f18b0 is 0 bytes after a block of size 16 alloc'd
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x109B52: unserialize_word_list (client_brute_force.c:236)
==11016==    by 0x10A402: main (client_brute_force.c:429)
==11016==
==11016== Thread 4:
==11016== Invalid read of size 4
==11016==    at 0x4E7C3E0: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==   by 0x4E9AEA7: zmq_recv (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x1099FA: rnb (client_brute_force.c:211)
==11016==    by 0x109FA2: game_timer (client_brute_force.c:322)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==  Address 0x63cd2d0 is 1,152 bytes inside a block of size 1,496 free'd
==11016==   at 0x4C2E26B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd6
==11016==    by 0x4E5CA4D: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x4E9234B: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==  Block was alloc'd at
==11016==   at 0x4C2D43F: operator new(unsigned long, std::nothrow_t const&) (in /usr/lib/valgr
==11016==    by 0x4E7C589: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x4E4B50D: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x109186: open_client_sockets (client_brute_force.c:17)
==11016==    by 0x109463: create_client_data (client_brute_force.c:78)
==11016==    by 0x10A37E: main (client_brute_force.c:419)
==11016==
==11016== Invalid read of size 4
==11016==    at 0x4E7C3E0: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==   by 0x4E9AA1F: zmq_getsockopt (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x109A2D: rnb (client_brute_force.c:213)
==11016==    by 0x109FA2: game_timer (client_brute_force.c:322)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==  Address 0x63cd2d0 is 1,152 bytes inside a block of size 1,496 free'd
==11016==   at 0x4C2E26B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd6
==11016==    by 0x4E5CA4D: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x4E9234B: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==  Block was alloc'd at
```

```
==11016==   at 0x4C2D43F: operator new(unsigned long, std::nothrow_t const&) (in /usr/lib/valgr
==11016==    by 0x4E7C589: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x4E4B50D: ??? (in /usr/lib/x86_64-linux-gnu/libzmq.so.5.0.0)
==11016==    by 0x109186: open_client_sockets (client_brute_force.c:17)
==11016==    by 0x109463: create_client_data (client_brute_force.c:78)
==11016==    by 0x10A37E: main (client_brute_force.c:419)
==11016==
==11016== Thread 1:
==11016== Invalid free() / delete / delete[] / realloc()
==11016==   at 0x4C2DD6B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x10A5E0: main (client_brute_force.c:470)
==11016==  Address 0x63c5c80 is 0 bytes inside a block of size 64 free'd
==11016==   at 0x4C2DD6B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x109A39: rnb (client_brute_force.c:214)
==11016==    by 0x109FA2: game_timer (client_brute_force.c:322)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==  Block was alloc'd at
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x1099D5: rnb (client_brute_force.c:210)
==11016==    by 0x109FA2: game_timer (client_brute_force.c:322)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==
==11016== Invalid free() / delete / delete[] / realloc()
==11016==   at 0x4C2DD6B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x10A5FB: main (client_brute_force.c:473)
==11016==  Address 0x63c5cd0 is 16 bytes after a block of size 64 free'd
==11016==   at 0x4C2DD6B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x109A39: rnb (client_brute_force.c:214)
==11016==    by 0x109FA2: game_timer (client_brute_force.c:322)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==  Block was alloc'd at
==11016==   at 0x4C2EB55: calloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==11016==    by 0x1099D5: rnb (client_brute_force.c:210)
==11016==    by 0x109FA2: game_timer (client_brute_force.c:322)
==11016==    by 0x50C2709: start_thread (pthread_create.c:333)
==11016==    by 0x53E10AE: clone (clone.S:105)
==11016==
==11016==
==11016== HEAP SUMMARY:
==11016==     in use at exit: 6,260,416 bytes in 4 blocks
==11016==  total heap usage: 6,365,164 allocs, 6,365,162 frees, 438,891,169 bytes allocated
==11016==
==11016== LEAK SUMMARY:
==11016==    definitely lost: 0 bytes in 0 blocks
==11016==    indirectly lost: 0 bytes in 0 blocks
==11016==      possibly lost: 288 bytes in 1 blocks
```

```
==11016==    still reachable: 6,260,128 bytes in 3 blocks
==11016==         suppressed: 0 bytes in 0 blocks
==11016== Rerun with --leak-check=full to see details of leaked memory
==11016==
==11016== For counts of detected and suppressed errors, rerun with: -v
==11016== ERROR SUMMARY: 5490020 errors from 9 contexts (suppressed: 0 from 0)
```