

Valgrind - Memcheck

Excuse the ads! We need some help to keep our site up.

List

- [Valgrind - Memcheck](#)
- [Example](#)
 - [Sample code](#)
 - [Build](#)
 - [Run memcheck](#)
- [Related site](#)

Valgrind - Memcheck

- Memcheck는 C, C++ 프로그램에서 메모리 관리 문제를 탐지합니다.
- Memcheck는 프로그램이 실행되면 메모리의 모든 읽기와 쓰기가 검사 되고 malloc / new / delete에 대한 호출이 인터셉트됩니다.
- Memcheck는 다음과 같은 내용을 탐지 할 수 있습니다.
 - 불필요한 메모리 액세스
 - 할당되지 않은 영역
 - 해제된 영역
 - 스택 블록의 끝 부분
 - 액세스 할 수 없는 영역
 - 초기화 되지 않은 값 사용
 - 메모리 누수
 - Heap 블록의 잘못된 해제
 - Double free
 - mismatched free
- Memcheck는 오류가 발생하면 즉시 오류를 보고하고 오류가 발생한 영역에 대한 스택 추적 정보를 제공합니다.
- Memcheck는 바이트 수준에서 주소 지정 가능성을 추적하고 비트 수준에서 값을 초기화합니다.
- Memcheck는 프로그램을 정상 속도보다 느린 약 10~30배 속도로 실행합니다

Example

Sample code

Sample.c

```
#include <stdio.h>

int main(){
    char *p;

    p = (char *) malloc(19);
    p = (char *) malloc(12);
    free(p);
    p = (char *) malloc(16);

    return 0;
}
```

Build

- 다음과 같이 Sample 코드를 빌드합니다.

gcc -o test -g test.c

```
lazenca0x0@ubuntu:~$ gcc -o test -g test.c
test.c: In function 'main':
test.c:8:16: warning: implicit declaration of function 'malloc' [-Wimplicit-function-declaration]
    p = (char *) malloc(19);
                ^
test.c:8:16: warning: incompatible implicit declaration of built-in function 'malloc'
test.c:8:16: note: include '<stdlib.h>' or provide a declaration of 'malloc'
test.c:12:3: warning: implicit declaration of function 'free' [-Wimplicit-function-declaration]
    free(p);
    ^
test.c:12:3: warning: incompatible implicit declaration of built-in function 'free'
test.c:12:3: note: include '<stdlib.h>' or provide a declaration of 'free'
```

Run memcheck

- 다음과 같이 valgrind의 옵션과 분석 할 대상 바이너리의 경로를 전달하면, 탐지된 Errors의 정보를 출력합니다.

Run valgrind

```
lazenca0x0@ubuntu:~$ valgrind --tool=memcheck --leak-check=yes --show-reachable=yes --num-callers=20 --track-fds=yes ./test
==54123== Memcheck, a memory error detector
==54123== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==54123== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==54123== Command: ./test
==54123==
==54123==
==54123== FILE DESCRIPTORS: 3 open at exit.
==54123== Open file descriptor 2: /dev/pts/18
==54123==   <inherited from parent>
==54123==
==54123== Open file descriptor 1: /dev/pts/18
==54123==   <inherited from parent>
==54123==
==54123== Open file descriptor 0: /dev/pts/18
==54123==   <inherited from parent>
==54123==
==54123== HEAP SUMMARY:
==54123==   in use at exit: 35 bytes in 2 blocks
==54123==   total heap usage: 3 allocs, 1 frees, 47 bytes allocated
==54123==
==54123== 16 bytes in 1 blocks are definitely lost in loss record 1 of 2
==54123==   at 0x4C2DBF6: malloc (vg_replace_malloc.c:299)
==54123==   by 0x40059F: main (test.c:15)
==54123==
==54123== 19 bytes in 1 blocks are definitely lost in loss record 2 of 2
==54123==   at 0x4C2DBF6: malloc (vg_replace_malloc.c:299)
==54123==   by 0x400577: main (test.c:8)
==54123==
==54123== LEAK SUMMARY:
==54123==   definitely lost: 35 bytes in 2 blocks
==54123==   indirectly lost: 0 bytes in 0 blocks
==54123==   possibly lost: 0 bytes in 0 blocks
==54123==   still reachable: 0 bytes in 0 blocks
==54123==   suppressed: 0 bytes in 0 blocks
==54123==
==54123== For counts of detected and suppressed errors, rerun with: -v
==54123== ERROR SUMMARY: 2 errors from 2 contexts (suppressed: 0 from 0)
lazenca0x0@ubuntu:~$
```

Related site

- Memcheck: <http://valgrind.org/docs/manual/mc-manual.html>
- <http://cs.ecs.baylor.edu/~donahoo/tools/valgrind/>
- <http://www.thegeekstuff.com/2011/11/valgrind-memcheck/>

