Subject: armv5l/linux: apps crash from huge mmap2() calls
Posted by jcheek on Tue, 13 Nov 2007 19:38:45 GMT
View Forum Message <> Reply to Message

Hi,

We're cross-compiling u++ on linux for an armv5l target. We've gotten the apps to compile fine with a few patches but they crash when run. This is on a board with 64M RAM. It appears to be happening when loading images and occurs with the three programs we have tried: Clock, HomeBudget, and theIDE.

relevant part of Clock strace without -DflagUSEMALLOC:

```
munmap(0x40b9c000, 4096)                = 0
write(3, "u\0\1\0", 4)                   = 4
read(3, "\1 Q\0\10\0\0\0\0\20\0\0\36%\22\10\340\301\33\10@\25\343"..., 32) = 32
read(3, "\1\2\3\4\5\6\7\10\t\n\v\f\r\16\17\20\21\22\23\24\25\26"..., 32) = 32
write(3, "\20\0\6\0\16\0\0\0_NET_SUPPORTED\0\0", 24) = 24
read(3, "\1\230R\0\0\0\0\0\r\1\0\0\36%\22\10\340\301\33\10@\25\343"..., 32) = 32
write(3, "\24\0\6\0\246\1\0\0\r\1\0\0\0\0\0\0\0\0\0\0\233\377\0\0"..., 24) = 24
read(3, 0xbebf2ba0, 32)                 = -1 EAGAIN (Resource temporarily unavai
lable)
poll([{fd=3, events=POLLIN, revents=POLLIN}], 1, -1) = 1
read(3, "\1 S\0B\0\0\0\4\0\0\0\0\0\0B\0\0\0\36%\22\10\340\301"..., 32) = 32
read(3, "\r\1\0\0;\1\0\0<\1\0\0=\1\0\0>\1\0\0?\1\0\0007\1\0\0A\1"..., 264) = 264
mmap2(NULL, 44306432, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
0x40ba0000
munmap(0x40ba0000, 44306432)            = 0
mmap2(NULL, 69210112, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
-1 ENOMEM (Cannot allocate memory)
brk(0x44af000)                          = 0x2af000
mmap2(NULL, 69341184, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
-1 ENOMEM (Cannot allocate memory)
mmap2(NULL, 2097152, PROT_NONE,
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0)
= 0x48fc2000
munmap(0x48fc2000, 253952)              = 0
munmap(0x49100000, 794624)              = 0
mprotect(0x49000000, 135168, PROT_READ|PROT_WRITE) = 0
mmap2(NULL, 69210112, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
-1 ENOMEM (Cannot allocate memory)
gettimeofday({208, 865341}, NULL)       = 0
open("/etc/localtime", O_RDONLY)        = 7
```

```
fstat64(7, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
fstat64(7, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x40
b9c000
read(7, "", 4096)                       = 0
close(7)                                = 0
munmap(0x40b9c000, 4096)                = 0
readlink("/proc/506/exe", "/usr/bin/Clock", 4096) = 14
mkdir("/root/.Clock", 0755)             = 0
unlink("/root/.Clock/Clock.1970-01-01-00-03-28.buglog.old") = -1 ENOENT (No such
 file or directory)
rename("/root/.Clock/Clock.1970-01-01-00-03-28.buglog", "/root/.Clock/Clock.1970
-01-01-00-03-28.buglog.old") = -1 ENOENT (No such file or directory)
open("/root/.Clock/Clock.1970-01-01-00-03-28.buglog", O_RDWR|O_CREAT|O_TRUNC, 06
44) = 7
gettimeofday({208, 899242}, NULL)       = 0
write(7, "* /usr/bin/Clock 01.01.1970 00:0"..., 49) = 49
write(7, "\r\n", 2)                      = 2
write(7, "PANIC: Out of memory\n", 21)  = 21
write(2, "Out of memory", 13)           = 13
write(2, "\n", 1)                       = 1
rt_sigprocmask(SIG_UNBLOCK, [ABRT], NULL,  = 0
tgkill(506, 506, SIGABRT)               = 0
--- SIGABRT (Aborted) @ 0 (0) ---
+++ killed by SIGABRT +++
```

relevant part of Clock strace with -DflagUSEMALLOC:

```
_llseek(10, 86016, [86016], SEEK_SET)   = 0
close(7)                                = 0
munmap(0x40b7b000, 4096)                = 0
write(3, "u\0\1\0", 4)                   = 4
read(3, "\1 Q\0\10\0\0\0\0\20\0\0\36%\22\10\340\301\33\10@\25\343"..., 32) = 32
read(3, "\1\2\3\4\5\6\7\10\t\n\v\f\r\16\17\20\21\22\23\24\25\26"..., 32) = 32
write(3, "\20\0\6\0\16\0\0\0_NET_SUPPORTED\0\0", 24) = 24
read(3, "\1\'R\0\0\0\0\0\r\1\0\0\36%\22\10\340\301\33\10@\25\343"..., 32) = 32
write(3, "\24\0\6\0\246\1\0\0\r\1\0\0\0\0\0\0\0\0\0\0\233\377\0\0"..., 24) = 24
read(3, 0xbee59b90, 32)                 = -1 EAGAIN (Resource temporarily unavai
lable)
poll([{fd=3, events=POLLIN, revents=POLLIN}], 1, -1) = 1
read(3, "\1 S\0B\0\0\0\4\0\0\0\0\0\0\0B\0\0\0\36%\22\10\340\301"..., 32) = 32
read(3, "\r\1\0\0;\1\0\0<\1\0\0=\1\0\0>\1\0\0?\1\0\0007\1\0\0A\1"..., 264) = 264
mmap2(NULL, 44306432, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
0x40b7f000
munmap(0x40b7f000, 44306432)            = 0
```

```
mmap2(NULL, 69210112, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
-1 ENOMEM (Cannot allocate memory)
brk(0x4498000)                          = 0x298000
mmap2(NULL, 69341184, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
-1 ENOMEM (Cannot allocate memory)
mmap2(NULL, 2097152, PROT_NONE,
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0)
= 0x48fa1000
munmap(0x48fa1000, 389120)              = 0
munmap(0x49100000, 659456)              = 0
mprotect(0x49000000, 135168, PROT_READ|PROT_WRITE) = 0
mmap2(NULL, 69210112, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,
-1, 0) =
-1 ENOMEM (Cannot allocate memory)
write(2, "terminate called after throwing "..., 48) = 48
write(2, "std::bad_alloc", 14)          = 14
write(2, "\'\n", 2)                     = 2
write(2, "  what():  ", 11)              = 11
write(2, "std::bad_alloc", 14)          = 14
write(2, "\n", 1)                       = 1
rt_sigprocmask(SIG_UNBLOCK, [ABRT], NULL,  = 0
tgkill(411, 411, SIGABRT)               = 0
--- SIGABRT (Aborted) @ 0 (0) ---
+++ killed by SIGABRT +++
```

Note that if we enable swap on the board we can get these applications to start.

Subject: Re: armv5l/linux: apps crash from huge mmap2() calls
Posted by mirek on Wed, 14 Nov 2007 18:53:09 GMT
View Forum Message <> Reply to Message

jcheek wrote on Tue, 13 November 2007 14:38Hi,
Note that if we enable swap on the board we can get these applications to start.

"swap"? Is that about little endian / big endian?

I am sorry, my knowledge about ARM platform is quite limited.

Anyway, if it is LE/BE issue (if it works with swap, almost absolutely certain...), my guess is that the problem can be either

```
#define CPU_LE
#define CPU_LITTLE_ENDIAN
```

in Core.h or perhaps zlib is not compiled properly.

Mirek

Subject: Re: armv5l/linux: apps crash from huge mmap2() calls
Posted by jcheek on Thu, 13 Dec 2007 21:19:04 GMT
View Forum Message <> Reply to Message

Hi,

When I mean swap, i am talking about virtual memory, not swapping endianness.

Thanks!

Joseph Cheek
joseph.cheek@timesys.com

Subject: Re: armv5l/linux: apps crash from huge mmap2() calls
Posted by mirek on Sun, 16 Dec 2007 22:23:25 GMT
View Forum Message <> Reply to Message

Anyway, even so, wrong endian seems to be the most likely cause.

The issue is that image loading code is "deserializing" certain 32 bit values to get the image dimension. If endianess is buggy, you are very likely to obtain some pretty big numbers....

If you have any means of debuging / logging, it would be interesting to inspect image dimensions, a result of Peek16le, ImageBlit.cpp 354. I bet they are wrong, because Peek16le does not work properly

Mirek
