

Wine под MCBC

Начало истории для меня

<http://etersoft.ru>

Проблемы времени выполнения

Первоначальный запуск wine не полностью инициализирует ~/.wine

Симптомы:

```
$ wine
WINE@Etersoft 1.0.8
First running... Using WINEPREFIX=/home/dumb/.wine
Creating default file tree...
/usr/bin/wine: line 194: 2506 Segmentation fault      WINESAFE=yes
"${WINELOADER}" rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall
128 wine.inf
/usr/bin/wine: line 195: 2509 Segmentation fault      WINESAFE=yes
"${WINELOADER}" regedit.exe "$CROOT/windows/inf/vendor.reg"
Building local environment...
Device 'a:' created as link for '/mnt/floppy' target.
...
Device 'lpt4' created as link for '/dev/lp3' target.
/usr/bin/wine: line 268: 2535 Segmentation fault      $WINELOADER wineboot
WINE@Etersoft has been configured for the first time.
Use /home/dumb/wine_c as WINE C:\ disk.
Copy your program into and install it.
```

В результате каталог c:\windows\system32 не содержит dll, но все работает с dll из /usr/lib/wine/. Однако, взяв заполненный c:\windows\system32 ничего запустить не могу:

```
$ wine-kthread ./lcv7s.exe
wine: Unhandled page fault on read access to 0x00000000 at address
0x402586f8 (thread 0009), starting debugger...
err:seh:start_debugger Couldn't start debugger ("winedbg --auto 8 56")
(1359)
Read the Wine Developers Guide on how to set up winedbg or another debugger
```

wine-preloader загружает wine-kthread и падает с segmentation fault при попытке начать его исполнение

Ход разборок:

```
gdb --args /home/dumb/rpmbuild/BUILD/wine-20070915/loader/wine-preloader  
/home/dumb/rpmbuild/BUILD/wine-20070915/loader/wine-kthread ./NOTEPAD.EXE
```

```
(gdb) run
```

```
...  
jumping to 600019c0
```

```
Program received signal SIGSEGV, Segmentation fault.  
0x60005240 in ?? ()
```

disassemble не работает, потому что исполняемый сегмент загружен самим wine-preloader

```
(gdb) x/64i $eip-32  
0x60005220:    call    0x6000195c  
0x60005225:    add     $0x20,%esp  
0x60005228:    mov     0x164(%ebx),%eax  
0x6000522e:    mov     (%eax),%edx  
0x60005230:    lea     0xf(%edx),%eax  
0x60005233:    and     $0xf0,%al  
0x60005235:    sub     %eax,%esp  
0x60005237:    mov     %esp,0xffffffff6c(%ebp)  
0x6000523d:    add     $0xfffffffffc,%esp  
0x60005240:    push    %edx
```

```
(gdb) info registers  
eax            0x1000    4096  
ecx            0x802     2050  
edx            0x1000    4096  
ebx            0x60013868    1610692712  
esp            0xbffffdf58    0xbffffdf58  
ebp            0xbffff074    0xbffff074  
esi            0x63f2b    409387  
edi            0x0        0  
eip            0x60005240    0x60005240  
eflags         0x10293    66195  
cs             0x23      35  
ss             0x2b      43  
ds             0x2b      43  
es             0x2b      43  
fs             0x0        0  
gs             0x0        0
```

получается, после сдвига стека на 0x1000 вниз все сломалось. wine-preloader резервирует мало стека?

Написал тест:

```
void f(int i)  
{  
    int r[4096];
```

```
    f(i+1);  
}  
  
int main()  
{  
    f(0);  
}
```

падает в одном и том же (по стеку и по i) месте, как при обычном запуске, так и при запуске wine-preloader'ом. С объемом стека все в порядке.

Нашел **настоящую** разницу: после загрузки wine-kthread резервирует память. Когда он запускается сам по себе картина такова:

```
...  
stat("/usr/bin/wineserver", {st_mode=S_IFREG|0755, st_size=343953, ...}) = 0  
old_mmap(0x7ffe0000, 1073741824, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x7ffe0000  
old_mmap(0x1000, 1110016, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x1000  
old_mmap(NULL, 4096, PROT_NONE,  
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0  
open("/usr/lib/wine/ntdll.dll.so", O_RDONLY) = 4  
...
```

Когда же через wine-preloader:

```
...  
stat("/usr/bin/wineserver", {st_mode=S_IFREG|0755, st_size=343953, ...}) = 0  
old_mmap(0x7ffe0000, 1073741824, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = -1 ENOMEM (Cannot allocate  
memory)  
old_mmap(0x7ffe0000, 536870912, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = -1 ENOMEM (Cannot allocate  
memory)  
old_mmap(0x7ffe0000, 268435456, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x6021a000  
munmap(0x6021a000, 268435456) = 0  
old_mmap(0x7ffe0000, 134217728, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x6021a000  
munmap(0x6021a000, 134217728) = 0  
old_mmap(0x7ffe0000, 67108864, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x6021a000  
...  
old_mmap(0x87fe0000, 134217728, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x87fe0000  
old_mmap(0x8ffe0000, 268435456, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = -1 ENOMEM (Cannot allocate  
memory)  
old_mmap(0x8ffe0000, 134217728, PROT_NONE,  
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = 0x8ffe0000
```

```
...
old_mmap(0xbffd0000, 65536, PROT_NONE,
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = -1 ENOMEM (Cannot allocate
memory)
old_mmap(0x1000, 1110016, PROT_NONE,
MAP_PRIVATE|MAP_ANONYMOUS|MAP_NORESERVE, -1, 0) = -1 ENOMEM (Cannot allocate
memory)
brk(0x7c004000) = 0x7c004000
open("/usr/lib/wine/ntdll.dll.so", O_RDONLY) = 4
fstat(4, {st_mode=S_IFREG|0755, st_size=549156, ...}) = 0
--- SIGSEGV (Segmentation fault) @ 0 (0) ---
...
```

From:

<http://wiki.osll.ru/> - Open Source & Linux Lab

Permanent link:

http://wiki.osll.ru/doku.php/etc:users:jcmvbkbc:wine_mcbc?rev=1192482932

Last update: **2008/01/03 02:32**

