Начало истории для меня

http://etersoft.ru

Патчи для компиляции wine в МСВС 3.0 изм.13

Проблемы времени выполнения

wine-preloader падает с segmentation fault после загрузки кода приложения, 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,0xffffff6c(%ebp)
0x6000523d:     add    $0xfffffffc,%esp
0x60005240:     push   %edx
```

```
(gdb) info registers
eax            0x1000   4096
ecx            0x802    2050
edx            0x1000   4096
ebx            0x60013868       1610692712
esp            0xbfffdf58       0xbfffdf58
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 зарезервировал маленький стек?

From:
http://wiki.osll.ru/ - **Open Source & Linux Lab**

Permanent link:
http://wiki.osll.ru/doku.php/etc:users:jcmvbkbc:wine_mcbc?rev=1192288984

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