打开 wps 就崩溃，看看啥原因呗，为了防止被它的异常上报程序捕获，首先先挂上调试器

代码:

```
(1e60.1a6c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception han
dling.
This exception may be expected and handled.
*** ERROR: Symbol file could not be found.  Defaulted to e
xport symbols for D:\Program Files (x86)\Kingsoft\WPS Office\9.
1.0.4867\office6\officespace.DLL -
eax=00000000 ebx=00000011 ecx=0036ee80 edx=003428c3 esi=776a8ad0
 edi=00000000
eip=7748f3c4 esp=09b3fd00 ebp=09b3fd0c iopl=0                 nv
 up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b
                  efl=00010202
officespace!KActiveLoginInfoCache::vipUrl+0x9e8:
7748f3c4 8b480c                 mov         ecx,dword ptr [eax
+0Ch] ds:002b:0000000c=????????
```

分析下栈

代码:

```
0:017> kvn
 # ChildEBP RetAddr    Args to Child
WARNING: Stack unwind information not available. Following fra
mes may be wrong.
00 09b3fd0c 7749235b acc53f64 00000000 09b3fd8c officespace!KAc
tiveLoginInfoCache::vipUrl+0x9e8
01 09b3fd40 77491f93 09b3fd5c acc53f74 06b50300 officespace!KAc
tiveLoginInfoCache::vipUrl+0x397f
02 09b3fd74 774996cf acc53f9c 06b50220 06b50300 officespace!KAc
tiveLoginInfoCache::vipUrl+0x35b7
*** ERROR: Symbol file could not be found.  Defaulted to e
xport symbols for D:\Program Files (x86)\Kingsoft\WPS Office\9.
1.0.4867\office6\QtCore4.dll -
03 09b3fdb8 668fb948 00000000 00000000 09b3fe00 officespace!KAc
tiveLoginInfoCache::vipUrl+0xacf3
04 09b3fdc8 57b7c556 06b50300 acb26a30 00000000 QtCore4!QThread
::setPriority+0x25d
05 09b3fe00 57b7c600 00000000 09b3fe18 76a0338a MSVCR100!_endth
readex+0x3f (FPO: [Non-Fpo])
06 09b3fe0c 76a0338a 06cc4178 09b3fe58 771c9f72 MSVCR100!_endth
readex+0xce (FPO: [Non-Fpo])
```

```
07 09b3fe18 771c9f72 06cc4178 2660fcd4 00000000 kernel32!BaseTh
readInitThunk+0xe (FPO: [Non-Fpo])
08 09b3fe58 771c9f45 57b7c59c 06cc4178 00000000 ntdll!__RtlUser
ThreadStart+0x70 (FPO: [Non-Fpo])
09 09b3fe70 00000000 57b7c59c 06cc4178 00000000
ntdll!_RtlUserThreadStart+0x1b (FPO: [Non-Fpo])
```

看看出错的东西是哪儿来的吧

代码:

```
7748f3a7 55                              push        ebp
7748f3a8 8bec                          mov           ebp,esp
7748f3aa 51                              push        ecx
7748f3ab 53                              push        ebx
7748f3ac 57                              push        edi
7748f3ad 8d45fc                      lea           eax,[ebp-4]
7748f3b0 50                              push        eax
7748f3b1 ff1518e45b77        call        dword ptr [officespace!KQ
ingClient::trUtf8+0x7a638 (775be418)]
7748f3b7 8d4dfc                      lea           ecx,[ebp-4]
7748f3ba ff151ce45b77        call        dword ptr [officespace!KQ
ingClient::trUtf8+0x7a63c (775be41c)]
7748f3c0 8bd8                          mov           ebx,eax
7748f3c2 8b06                          mov           eax,dword ptr [e
si]
0:017> ?(.-7748f3a7)
Evaluate expression: 29 = 0000001d
0:017> r
eax=00000000 ebx=00000011 ecx=0036ee80 edx=003428c3 esi=776a8ad0
 edi=00000000
eip=7748f3c4 esp=09b3fd00 ebp=09b3fd0c iopl=0                nv
 up ei pl nz na po nc
cs=0023   ss=002b   ds=002b   es=002b   fs=0053   gs=002b
                  efl=00010202
officespace!KActiveLoginInfoCache::vipUrl+0x9e8:
7748f3c4 8b480c                      mov           ecx,dword ptr [eax
+0Ch] ds:002b:0000000c=????????
0:017> ?(0x9e8-0x1d)
Evaluate expression: 2507 = 000009cb
0:017> x officespace!KActiveLoginInfoCache::vipUrl+000009cb
```

那就是这里了，断下重启

代码:

```
Breakpoint 0 hit
eax=0b1cf83c ebx=00000000 ecx=0b1cf864 edx=00d40174 esi=05fc8ad0
 edi=00000000
```

```
eip=05daf3a7  esp=0b1cf818  ebp=0b1cf848  iopl=0                  nv
  up  ei  pl  nz  na  po  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9cb:
05daf3a7  55                            push        ebp
0:017>  dd  esi
05fc8ad0    00000000  00000001  05f5c5e4  06fefc48
05fc8ae0    00000000  00000000  00000000  66d13d90
05fc8af0    00000000  66d13d90  66d13d90  00000000
05fc8b00    66d13d90  66d13d90  00000000  66d13d90
05fc8b10    66d13d90  66d13d90  66d13d90  66d13d90
05fc8b20    00000000  66d13d90  66d13d90  66d13d90
05fc8b30    66d11874  00000000  66d13d90  00000000
05fc8b40    66d13d90  66d13d90  00000000  00000001
0:017>  p
eax=0b1cf83c  ebx=00000000  ecx=0b1cf864  edx=00d40174  esi=05fc8ad0
  edi=00000000
eip=05daf3a8  esp=0b1cf814  ebp=0b1cf848  iopl=0                  nv
  up  ei  pl  nz  na  po  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9cc:
05daf3a8  8bec                          mov         ebp,esp
0:017>
eax=0b1cf83c  ebx=00000000  ecx=0b1cf864  edx=00d40174  esi=05fc8ad0
  edi=00000000
eip=05daf3aa  esp=0b1cf814  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  po  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9ce:
05daf3aa  51                            push        ecx
0:017>
eax=0b1cf83c  ebx=00000000  ecx=0b1cf864  edx=00d40174  esi=05fc8ad0
  edi=00000000
eip=05daf3ab  esp=0b1cf810  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  po  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9cf:
05daf3ab  53                            push        ebx
0:017>
```

```
eax=0b1cf83c ebx=00000000 ecx=0b1cf864 edx=00d40174 esi=05fc8ad0
  edi=00000000
eip=05daf3ac esp=0b1cf80c ebp=0b1cf814 iopl=0                  nv
  up ei pl nz na po nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9d0:
05daf3ac 57                            push        edi
0:017>
eax=0b1cf83c ebx=00000000 ecx=0b1cf864 edx=00d40174 esi=05fc8ad0
  edi=00000000
eip=05daf3ad esp=0b1cf808 ebp=0b1cf814 iopl=0                  nv
  up ei pl nz na po nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9d1:
05daf3ad 8d45fc                    lea          eax,[ebp-4]
0:017>
eax=0b1cf810 ebx=00000000 ecx=0b1cf864 edx=00d40174 esi=05fc8ad0
  edi=00000000
eip=05daf3b0 esp=0b1cf808 ebp=0b1cf814 iopl=0                  nv
  up ei pl nz na po nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9d4:
05daf3b0 50                            push        eax
0:017>
eax=0b1cf810 ebx=00000000 ecx=0b1cf864 edx=00d40174 esi=05fc8ad0
  edi=00000000
eip=05daf3b1 esp=0b1cf804 ebp=0b1cf814 iopl=0                  nv
  up ei pl nz na po nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9d5:
*** ERROR: Symbol file could not be found.   Defaulted to e
xport symbols for D:\Program Files (x86)\Kingsoft\WPS Office\9.
1.0.4867\office6\QtCore4.dll -
05daf3b1 ff1518e4ed05        call        dword ptr [officespace!KQ
ingClient::trUtf8+0x7a638 (05ede418)] ds:002b:05ede418={QtCore4!QDa
teTime::time (665bffde)}
0:017>
eax=0b1cf810 ebx=00000000 ecx=03ddee82 edx=00d40174 esi=05fc8ad0
  edi=00000000
```

```
eip=05daf3b7  esp=0b1cf808  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  po  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9db:
05daf3b7  8d4dfc                  lea          ecx,[ebp-4]
0:017>
eax=0b1cf810  ebx=00000000  ecx=0b1cf810  edx=00d40174  esi=05fc8ad0
  edi=00000000
eip=05daf3ba  esp=0b1cf808  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  po  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000202
officespace!KActiveLoginInfoCache::vipUrl+0x9de:
05daf3ba  ff151ce4ed05        call        dword  ptr  [officespace!KQ
ingClient::trUtf8+0x7a63c  (05ede41c)]  ds:002b:05ede41c={QtCore4!QTi
me::hour  (665bf3d9)}
0:017>
eax=00000012  ebx=00000000  ecx=0036ee80  edx=00012982  esi=05fc8ad0
  edi=00000000
eip=05daf3c0  esp=0b1cf808  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  pe  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000206
officespace!KActiveLoginInfoCache::vipUrl+0x9e4:
05daf3c0  8bd8                        mov          ebx,eax
0:017>
eax=00000012  ebx=00000012  ecx=0036ee80  edx=00012982  esi=05fc8ad0
  edi=00000000
eip=05daf3c2  esp=0b1cf808  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  pe  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000206
officespace!KActiveLoginInfoCache::vipUrl+0x9e6:
05daf3c2  8b06                        mov          eax,dword  ptr  [e
si]    ds:002b:05fc8ad0=00000000
0:017>
eax=00000000  ebx=00000012  ecx=0036ee80  edx=00012982  esi=05fc8ad0
  edi=00000000
eip=05daf3c4  esp=0b1cf808  ebp=0b1cf814  iopl=0                  nv
  up  ei  pl  nz  na  pe  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000206
officespace!KActiveLoginInfoCache::vipUrl+0x9e8:
```

```
05daf3c4  8b480c                    mov          ecx,dword  ptr  [eax
+0Ch]  ds:002b:0000000c=????????
```

看看这个值哪儿来的？

代码:

```
05db22b1  bed08afc05           mov          esi,offset  officespace!
KxKuaiPanInfoGetter::staticMetaObject+0x5998  (05fc8ad0)

0:017>  dd  05fc8ad0
05fc8ad0    00000000
```

果然是空指针，往上追溯

代码:

```
05db22ff  8b0d74ffed05        mov          ecx,dword  ptr  [officespa
ce!KQingClient::trUtf8+0x7c194  (05edff74)]
...
05db2307  890dd08afc05        mov          dword  ptr  [officespace!K
xKuaiPanInfoGetter::staticMetaObject+0x5998  (05fc8ad0)],ecx
```

在 officespace 里面，那么重启，加 ba r1

代码:

```
0:000>  sxe  ld  officespace
0:000>  g
ModLoad:  0f3e0000  0f63b000      D:\Program  Files  (x86)\Kingsoft\W
PS  Office\9.1.0.4867\office6\officespace.DLL
eax=00000000  ebx=00000000  ecx=00000000  edx=00000000  esi=7efdd000
  edi=0032edf4
eip=771afc62  esp=0032ecc8  ebp=0032ed1c  iopl=0                  nv
  up  ei  pl  zr  na  pe  nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00000246
ntdll!ZwMapViewOfSection+0x12:
771afc62  83c404                    add          esp,4
0:000>  x  officespace!KQingClient::trUtf8
***  ERROR:  Symbol  file  could  not  be  found.    Defaulted  to  e
xport  symbols  for  D:\Program  Files  (x86)\Kingsoft\WPS  Office\9.
1.0.4867\office6\officespace.DLL  -
0f4a3d9b                    officespace!KQingClient::trUtf8  (<no  pa
rameter  info>)
0f4a3de0                    officespace!KQingClient::trUtf8  (<no  pa
rameter  info>)
0:000>  ba  r1  0f4a3d9b+0x7c194  "r;k;g;"
0:000>  ba  r1  0f4a3de0+0x7c194  "r;k;g;"
0:000>  g
```

然后答案就揭晓了、、

代码:

```
eax=66a81874 ebx=00000000 ecx=00000001 edx=00000471 esi=075d42e8
 edi=00000000
eip=0f3eb76d esp=0032d188 ebp=0032d1a4 iopl=0                 nv
 up ei pl nz na pe nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00200206
officespace!KxKuaiPanInfoGetter::qt_metacall+0x6483:
0f3eb76d 894610                 mov          dword ptr [esi+10h
],eax  ds:002b:075d42f8=baadf00d

0:017> ln 66a81874
(66a81874)      QtCore4!QListData::shared_null      |     (66a81a40)
    QtCore4!QMapData::shared_null
Exact matches:
       QtCore4!QListData::shared_null (<no parameter info>)

SetContext failed, 0x80070005
MachineInfo::SetContext failed - Thread: 04CE8F30    Handle: 840
    Id: 4174 - Error == 0x80070005
eax=66a81874 ebx=00000001 ecx=00006379 edx=00006378 esi=66536c1f
 edi=0f608a18
eip=0f44681f esp=0032d1e0 ebp=0032d204 iopl=0                 nv
 up ei pl nz na po nc
cs=0023    ss=002b    ds=002b    es=002b    fs=0053    gs=002b
                  efl=00200202
officespace!qt_test_isFetchedRoot+0x1d040:
0f44681f a3548a600f           mov          dword ptr [officespace
!KxKuaiPanInfoGetter::staticMetaObject+0x591c (0f608a54)],eax ds:00
2b:0f608a54=00000000
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following fra
mes may be wrong.
0032d204 0f446765 officespace!qt_test_isFetchedRoot+0x1d040
0032d228 0f48a913 officespace!qt_test_isFetchedRoot+0x1cf86
0032d260 0f3e75f2 officespace!verify+0x18999
0032d26c 664d5bce officespace!KxKuaiPanInfoGetter::qt_metacall+0x23
08
```

附上minidump

(e10.3c5c): Access violation - code c0000005 (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

*** ERROR: Symbol file could not be found. Defaulted to export symbols for D:\Program Files (x86)\Kingsoft\WPS Office\9.1.0.4867\office6\officespace.DLL -
eax=00000000 ebx=00000010 ecx=0036ee80 edx=0017816e esi=512a8ad0 edi=00000000
eip=5108f3c4 esp=0afffe38 ebp=0afffe44 iopl=0 nv up ei pl nz na po nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202
officespace!KActiveLoginInfoCache::vipUrl+0x9e8:
5108f3c4 8b480c mov ecx,dword ptr [eax+0Ch] ds:002b:0000000c=????????
0:018> lmvm wps
start end module name
013a0000 0248b000 wps (deferred)
Image path: wps.exe
Image name: wps.exe
Timestamp: Mon Nov 03 15:57:32 2014 (5457356C)
CheckSum: 010D5E08
ImageSize: 010EB000
File version: 11.1.0.4867
Product version: 11.1.0.4867
File flags: 0 (Mask 3F)
File OS: 40004 NT Win32
File type: 0.0 Unknown
File date: 00000000.00000000
Translations: 0000.04b0
CompanyName: Zhuhai Kingsoft Office Software Co.,Ltd
ProductName: WPS Office
InternalName: wps
OriginalFilename: wps.exe
ProductVersion: 11,1,0,4867
FileVersion: 11,1,0,4867
FileDescription: WPS Writer
LegalCopyright: Copyright©2014 Kingsoft Office Software Co., Ltd.All rights Reserved.

---

eax=66a81874 ebx=00000000 ecx=00000001 edx=00000471 esi=075d42e8 edi=00000000
eip=0f3eb76d esp=0032d188 ebp=0032d1a4 iopl=0 nv up ei pl nz na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=

00200206
officespace!KxKuaiPanInfoGetter::qt_metacall+0x6483:
0f3eb76d 894610 mov dword ptr [esi+10h],eax ds:002b:075d42f8
=baadf00d