

Re: access violation 0x77f64874

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress/2004-05/4

From: Robert Aldwinckle (*robald_at_techemail.com*)

Date: 05/24/04

Date: Mon, 24 May 2004 11:42:38 -0400

> *Is this a bug or what?*

A guess at the most likely cause without any other information would be that it could be corrupted heap due to third-party interference.

You have done a fine job of capturing salient information from your dump but unfortunately you truncated it just where it gets interesting: the Stack Back Trace. That may show you which other modules were involved in this crash and what they were doing. Also, in the section of the dump after that, the Raw Stack Dump, if it contains any readable data in the interpreted portion sometimes you can even see there clues which can help identify the interfering program.

HTH

Robert Aldwinckle

"oe6 user" <anonymous@discussions.microsoft.com> wrote in message news:1114801c44155\$91a43560\$a001280a@phx.gbl...

```
> OE6 (IE6 SP1 and NT4.0 SP6a)
> - generate error and quit
>
> Drwatson (drwtsn32.log):
>
> Application exception occurred:
>   App: (pid=344)
>   When: 5/24/2004 @ 14:3:21.145
>   Exception number: c0000005 (access violation)
>
> function: RtlAllocateHeap
>   77f6484d 0f84ac000000    je
> RtlAllocateHeap+0x233 (77f648ff)
>   77f64853 83f802          cmp     eax,0x2
>   77f64856 0f84b4000000    je
> RtlAllocateHeap+0x244 (77f64910)
>   77f6485c 83f803          cmp     eax,0x3
>   77f6485f 0f84b9000000    je
> RtlAllocateHeap+0x252 (77f6491e)
>   77f64865 8d83b8000000    lea    eax,
> [ebx+0xb8]      ds:000700b8=0451aca0
```

```
> 77f6486b 8b08 mov ecx,
> [eax] ds:000700b8=0451aca0
> 77f6486d 3bc1 cmp eax,ecx
> 77f6486f 7415 jz
> RtlAllocateHeap+0x1ba (77f64886)
> 77f64871 8d71f8 lea esi,[ecx-
> 0x8] ds:0890dc06=????????
> FAULT ->77f64874 0fb716 movzx edx,word ptr
> [esi] ds:070df1f8=????
> 77f64877 3b55f4 cmp edx,[ebp-
> 0xc] ss:0189dd96=7777772f
> 77f6487a 0f83db010000 jnb
> RtlAllocateHeap+0x38f (77f64a5b)
> 77f64880 8b09 mov ecx,
> [ecx] ds:070df200=????????
> 77f64882 3bc1 cmp eax,ecx
> 77f64884 75eb jnz
> RtlAllocateHeap+0x1a5 (77f64871)
> 77f64886 ff75f0 push dword ptr [ebp-
> 0x10] ss:0189dd96=7777772f
> 77f64889 53 push ebx
> 77f6488a e85ff8ffff call
> LdrGetDllHandle+0x51c (77f640ee)
> 77f6488f 8bf0 mov esi,eax
> 77f64891 85f6 test esi,esi
> 77f64893 0f846d040000 je
> RtlAllocateHeap+0x63a (77f64d06)
>
> Is this a bug or what?
```