

Re: Compiler bug in the DDK--be aware of it

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-08/msg00275.1>

- *From:* "kalden" <uberkalden@xxxxxxxxxxx>
 - *Date:* 25 Jul 2006 06:35:51 -0700
-

I am new to driver development. Can you actually build drivers with the visual studio 2005 C compiler, or did you compile that piece of code just to show the bug in the DDK build environment?

440gtx@xxxxxxxxxxx wrote:

Hi guys, I ran into a compiler bug in the latest ddk that is very serious. I have a piece of code I want to execute exactly one time, but discovered it gets run every single time. It is written as follows:

```
void func(void)
{
    static LONG Init = 0;

    if (InterlockedOr(&Init, 1) == 0)
    {
        ...do one time stuff here...
    }
}
```

The problem is the inner code executes every single time the function is invoked. I traced it down to a bug in the compiler. I then recompiled the driver using the Visual Studio 2005 compiler and the problem was fixed. I have attached the code each generated below. I'm now concerned about shipping any future drivers compiled using the DDK build environment because I don't know what all functions besides this particular example would generate corrupt code.

```
;-----;
; Windows 2003 DDK SP1 (3790.1830)
;-----;
mov ecx, 1
mov edx, OFFSET FLAT:?Init
```

Re: Compiler bug in the DDK--be aware of it

```
mov eax, DWORD PTR [edx]
$L14033:
mov esi, eax
or esi, ecx
lock cmpxchg DWORD PTR [edx], esi
jne $L14033
jne $L14011
```

```
;-----
; Visual Studio 2005
;-----
mov ecx, 1
mov edx, OFFSET ?Init
mov eax, DWORD PTR [edx]
$LN4
mov esi, eax
or esi, ecx
lock cmpxchg DWORD PTR [edx], esi
jne SHORT $LN4
test eax, eax ; <-----fixed
jne SHORT $LN2
```