

Forefront TMG BSOD in FWENG.SYS

Grundlagen

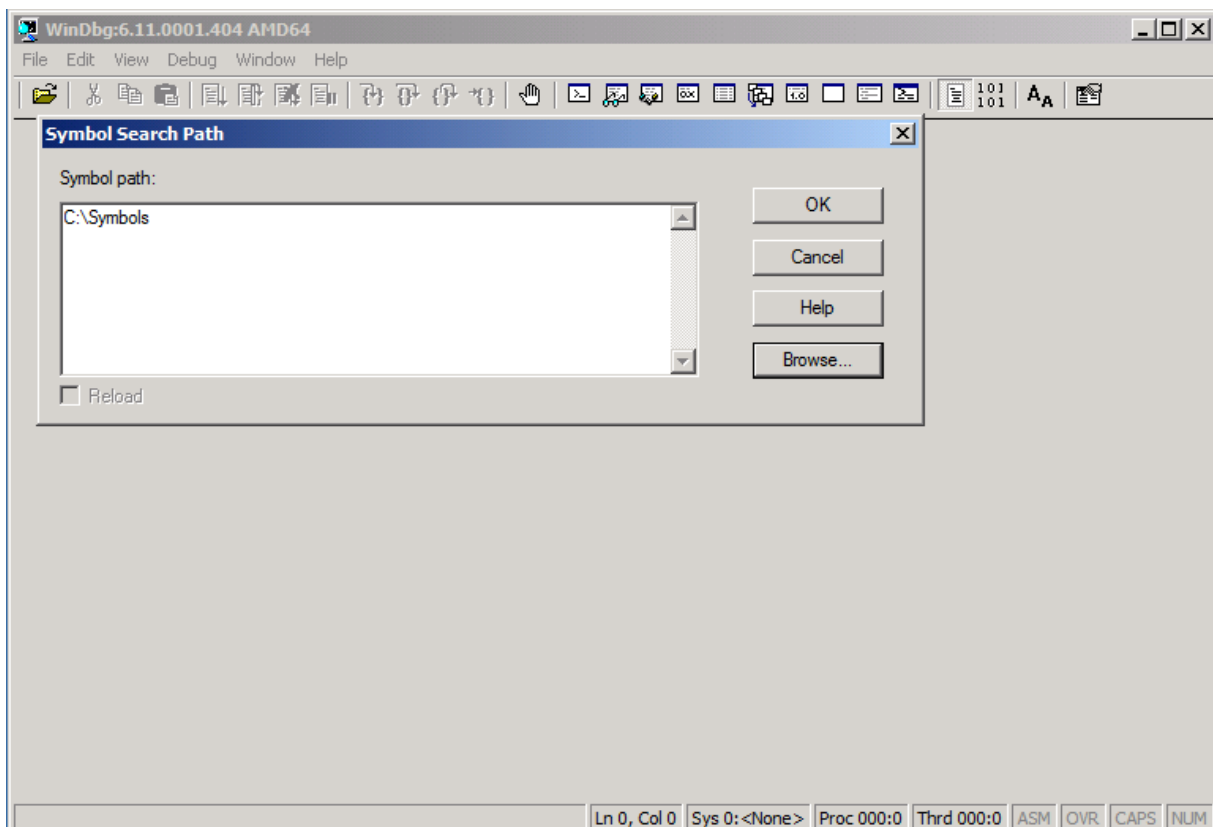
<http://support.microsoft.com/kb/315263>

<http://www.microsoft.com/whdc/devtools/debugging/default.aspx>

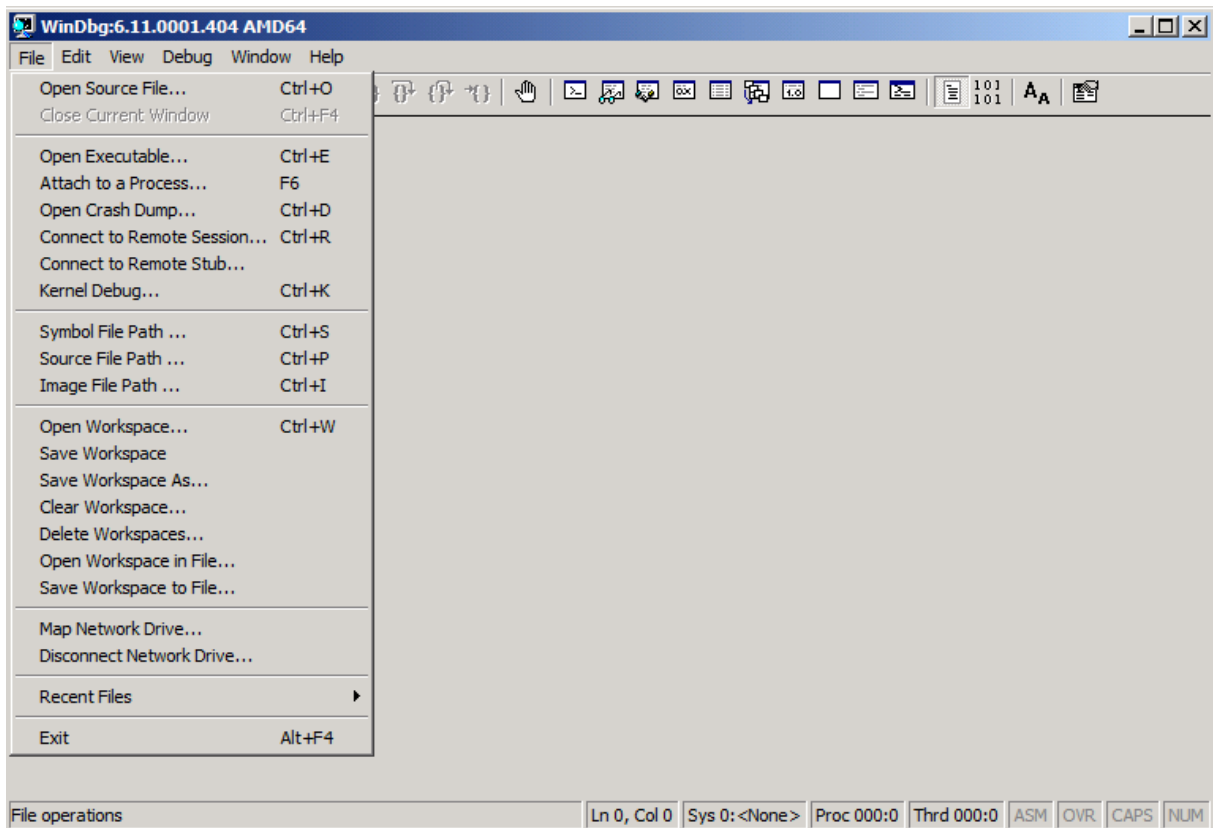
<http://support.microsoft.com/kb/254649/>

WinDbg ausfuehren

Symbol Path festlegen (Standard Symbole von der MS Webseite)



Open Crash Dump



Symbols fuer FWENG.SYS koennen nicht geladen werden

Microsoft (R) Windows Debugger Version 6.11.0001.404 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [C:\temp\010410-12183-01.dmp]
Mini Kernel Dump File: Only registers and stack trace are available

Symbol search path is: C:\Symbols
Executable search path is:
Unable to load image \SystemRoot\system32\ntoskrnl.exe, Win32 error 0n2
*** WARNING: Unable to verify timestamp for ntoskrnl.exe
*** ERROR: Module load completed but symbols could not be loaded for ntoskrnl.exe
Windows 7 Kernel Version 7600 MP (2 procs) Free x64
Product: Server, suite: Enterprise TerminalServer SingleUserTS
Built by: 7600.16385.amd64fre.win7_rtm.090713-1255
Machine Name:
Kernel base = 0xfffff800`01650000 PsLoadedModuleList = 0xfffff800`0188de50
Debug session time: Mon Jan 4 17:24:37.353 2010 (GMT+1)
System Uptime: 0 days 0:12:01.890
Unable to load image \SystemRoot\system32\ntoskrnl.exe, Win32 error 0n2
*** WARNING: Unable to verify timestamp for ntoskrnl.exe
*** ERROR: Module load completed but symbols could not be loaded for ntoskrnl.exe
Loading Kernel Symbols

.....
.....
.....
Loading User Symbols
Loading unloaded module list
.....

* Bugcheck Analysis *
* *

Use [!analyze -v](#) to get detailed debugging information.

BugCheck D1, {6, 2, 1, fffff88002926a9d}

Unable to load image \SystemRoot\system32\DRIVERS\fweng.sys, Win32 error 0n2
*** WARNING: Unable to verify timestamp for fweng.sys
*** ERROR: Module load completed but symbols could not be loaded for fweng.sys
***** Kernel symbols are WRONG. Please fix symbols to do analysis.

*** Your debugger is not using the correct symbols ***

*** In order for this command to work properly, your symbol path ***
*** must point to .pdb files that have full type information. ***

Modulname FWENG

```

ADDITIONAL_DEBUG_TEXT:
Use '!findthebuild' command to search for the target build information.
If the build information is available, run '!findthebuild -s ; .reload' to set symbol path and load symbols.

MODULE_NAME: fweng

FAULTING_MODULE: fffff80001650000 nt

DEBUG_FLR_IMAGE_TIMESTAMP: 4ad4f8bc

WRITE_ADDRESS: unable to get nt!MmSpecialPoolStart
unable to get nt!MmSpecialPoolEnd
unable to get nt!MmPoolCodeStart
unable to get nt!MmPoolCodeEnd
0000000000000006

CURRENT_IRQL: 0

FAULTING_IP:
fweng+56a9d
ffff880`02926a9d 66891401      mov     word ptr [rcx+rax],dx

CUSTOMER_CRASH_COUNT: 1

DEFAULT_BUCKET_ID: DRIVER_FAULT_SERVER_MINIDUMP

BUGCHECK_STR: 0xD1

LAST_CONTROL_TRANSFER: from fffff800016c1469 to fffff800016c1f00

STACK_TEXT:
ffff800`0145cc58 fffff800`016c1469 : 00000000`0000000a 00000000`00000006 00000000`00000002 00000000`00000001 : nt+0x71f00
ffff800`0145cc60 00000000`0000000a : 00000000`00000006 00000000`00000002 00000000`00000001 fffff880`02926a9d : nt+0x71469
ffff800`0145cc68 00000000`00000006 : 00000000`00000002 00000000`00000001 fffff880`02926a9d fffff8a0`02b9c3d0 : 0xa
ffff800`0145cc70 00000000`00000002 : 00000000`00000001 fffff880`02926a9d fffff8a0`02b9c3d0 00000000`00000000 : 0x6
ffff800`0145cc78 00000000`00000001 : fffff880`02926a9d fffff8a0`02b9c3d0 00000000`00000000 00000000`00000000 : 0x2
ffff800`0145cc80 fffff880`02926a9d : fffff8a0`02b9c3d0 00000000`00000000 00000000`00000000 00000000`00000000 : 0x1
ffff800`0145cc88 fffff8a0`02b9c3d0 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : fweng+0x56a9d
ffff800`0145cc90 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 0xfffffa80`02

STACK_COMMAND: kb

FOLLOWUP_IP:
fweng+56a9d
ffff880`02926a9d 66891401      mov     word ptr [rcx+rax],dx

SYMBOL_STACK_INDEX: 6

SYMBOL_NAME: fweng+56a9d

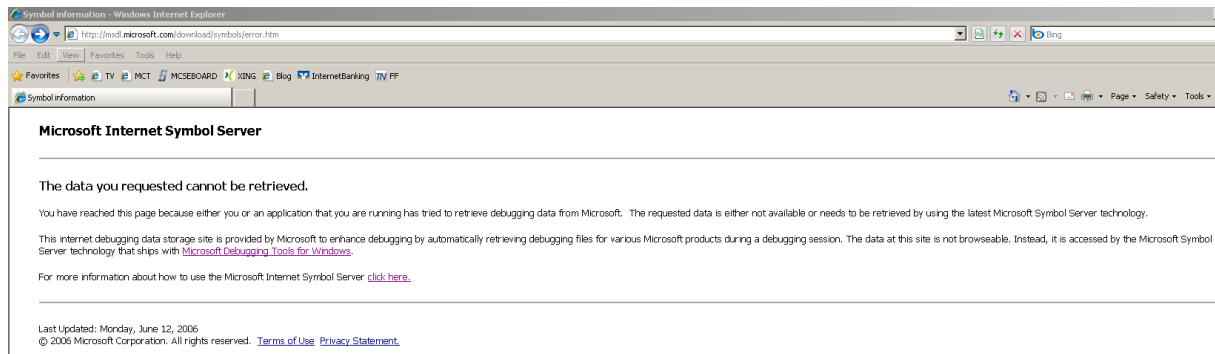
```

Symbol Files

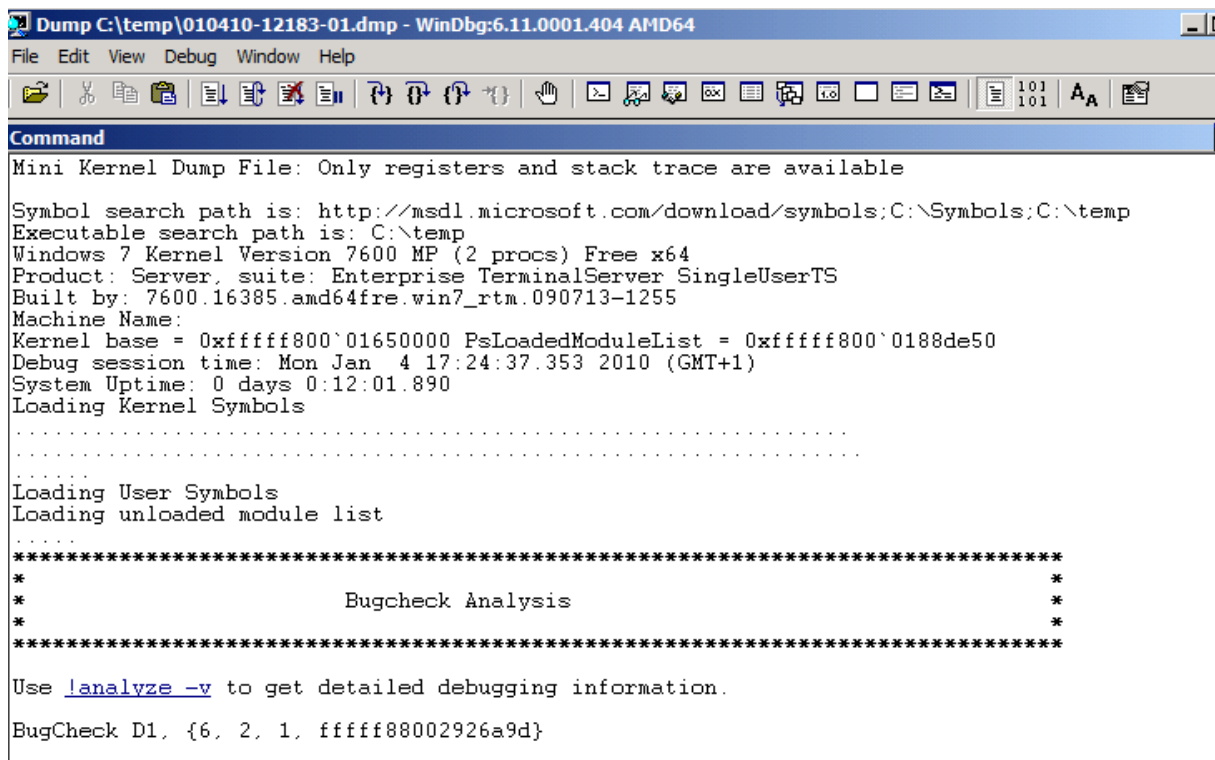
sum	Symbols	Symbol file
62c		mrxsmb20.sys
79f		srv2.sys
32f		srvnet.sys
542		tcpipreg.sys
370		HTTP.sys
7c9		peauth.sys
b40		secdrv.SYS
47a		srv.sys
c26		rdpdr.sys
a52		tdtcp.sys
7ce		tssecsrv.sys
48c		RDPWD.SYS
82a		asyncmac.sys
623		win32k.sys
5d4		dxg.sys
e96		TSDDD.dll
000		framebuf.dll
000	None	spsys.sys
000	None	\SystemRoot\system32\DRIVERS\hidusb.sys
000	None	\SystemRoot\System32\Drivers\dump_HpSAMD.sys
000	None	dump_HpSAMD.
000	None	\SystemRoot\system32\DRIVERS\HIDCLASS.SYS

Buttons: Close, Reload, Help

Nicht lokal, also Symbol File Server kontaktieren



Symbol Search Path zum Symbol File Server angeben ...



.. oder lokal downloaden (siehe Markierung)

```
Dump C:\temp\010410-12183-01.dmp - WinDbg:6.11.0001.404 AMD64
File Edit View Debug Window Help
[Icons] 101 101 A A
Command
Microsoft (R) Windows Debugger Version 6.11.0001.404 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [C:\temp\010410-12183-01.dmp]
Mini Kernel Dump File: Only registers and stack trace are available

Symbol search path is SRV*c:\websymbols*http://msdl.microsoft.com/download/symbols
Executable search path is C:\temp
Windows 7 Kernel Version 7600 MP (2 processors) Free x64
Product: Server, suite: Enterprise TerminalServer SingleUserTS
Built by: 7600.16385.amd64fre.win7_rtm.090713-1255
Machine Name:
Kernel base = 0xfffff800`01650000 PsLoadedModuleList = 0xfffff800`0188de50
Debug session time: Mon Jan  4 17:24:37.353 2010 (GMT+1)
System Uptime: 0 days 0:12:01.890
```

OK, IRQL not less or equal. MSPADMIN.EXE ist auch beteiligt

```
Dump C:\temp\010410-12183-01.dmp - WinDbg:6.11.0001.404 AMD64
File Edit View Debug Window Help
[Icons] 101 101 A A
Command
0: kd> !analyze -v
*****
*                               Bugcheck Analysis                               *
*                                                                           *
* DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If kernel debugger is available get stack backtrace.
Arguments:
Arg1: 0000000000000006, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000001, value 0 = read operation, 1 = write operation
Arg4: ffff88002926a9d, address which referenced memory

Debugging Details:
-----
WRITE_ADDRESS: GetPointerFromAddress: unable to read from fffff80018f80e0
0000000000000006

CURRENT_IRQL:  2

FAULTING_IP:
fweng+56a9d
fffff880`02926a9d 66891401      mov     word ptr [rcx+rax],dx

CUSTOMER_CRASH_COUNT:  1

DEFAULT_BUCKET_ID:  DRIVER_FAULT_SERVER_MINIDUMP

BUGCHECK_STR:  0xD1

PROCESS_NAME:  mspadmin.exe

TRAP_FRAME:  fffff8000145cda0 -- (.trap 0xfffff8000145cda0)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=0000000000000000
```