

# HP Power Manager

## Crash

```
(c74.60c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000041 ebx=0088963b ecx=0018f4c8 edx=00190000 esi=0018f280
edi=0018f4c8
eip=76c3c886 esp=0018f20c ebp=0018f218 iopl=0         nv up ei pl nz na pe
nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b
efl=00010206
msvcrt!_get_printf_count_output+0x2e:
76c3c886 8802          mov     byte ptr [edx],al
ds:002b:00190000=41
```

## Analyze

```
0:000> !analyze -v
*****
***
*
*
*
*
*
*
*
*
*
*
*****
***

*** WARNING: Unable to verify checksum for C:\Program Files (x86)\HP\Power
Manager\DevManBE.exe
*** ERROR: Module load completed but symbols could not be loaded for
C:\Program Files (x86)\HP\Power Manager\DevManBE.exe

KEY_VALUES_STRING: 1

TIMELINE_ANALYSIS: 1

Timeline: !analyze.Start
  Name: <blank>
  Time: 2019-05-07T13:30:15.90Z
  Diff: 4909 mSec
```

Timeline: Dump.Current  
Name: <blank>  
Time: 2019-05-07T13:30:20.0Z  
Diff: 0 mSec

Timeline: Process.Start  
Name: <blank>  
Time: 2019-05-07T13:29:27.0Z  
Diff: 53000 mSec

Timeline: OS.Boot  
Name: <blank>  
Time: 2019-05-07T13:14:12.0Z  
Diff: 968000 mSec

DUMP\_CLASS: 2

DUMP\_QUALIFIER: 0

FAULTING\_IP:  
msvcrt!\_get\_printf\_count\_output+2e  
76c3c886 8802 mov byte ptr [edx],al

EXCEPTION\_RECORD: (.exr -1)  
ExceptionAddress: 76c3c886 (msvcrt!\_get\_printf\_count\_output+0x0000002e)  
ExceptionCode: c0000005 (Access violation)  
ExceptionFlags: 00000000  
NumberParameters: 2  
Parameter[0]: 00000001  
Parameter[1]: 00190000  
Attempt to write to address 00190000

FAULTING\_THREAD: 00000dbc

DEFAULT\_BUCKET\_ID: INVALID\_POINTER\_WRITE

PROCESS\_NAME: DevManBE.exe

FOLLOWUP\_IP:  
msvcrt!\_get\_printf\_count\_output+2e  
76c3c886 8802 mov byte ptr [edx],al

WRITE\_ADDRESS: 00190000

ERROR\_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx referenced memory at 0x%08lx. The memory could not be %s.

EXCEPTION\_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx

referenced memory at 0x%08lx. The memory could not be %s.

EXCEPTION\_CODE\_STR: c0000005

EXCEPTION\_PARAMETER1: 00000001

EXCEPTION\_PARAMETER2: 00190000

WATSON\_BKT\_PROCSTAMP: 48a03a83

WATSON\_BKT\_MODULE: msvcrt.dll

WATSON\_BKT\_MODSTAMP: 4eeaf722

WATSON\_BKT\_MODOFFSET: c886

WATSON\_BKT\_MODVER: 7.0.7601.17744

MODULE\_VER\_PRODUCT: Microsoft® Windows® Operating System

BUILD\_VERSION\_STRING: 7601.23915.amd64fre.win7sp1\_ldr.170913-0600

MODLIST\_WITH\_TSCHKSUM\_HASH: e8d2d137c84067e819bda7983d27b1e0a67c4660

MODLIST\_SHA1\_HASH: 2eb8c9cb28b71df9b9c9e25ffdd6b76e261fe185

NTGLOBALFLAG: 70

APPLICATION\_VERIFIER\_FLAGS: 0

PRODUCT\_TYPE: 1

SUITE\_MASK: 272

DUMP\_TYPE: fe

ANALYSIS\_SESSION\_HOST: IEWIN7

ANALYSIS\_SESSION\_TIME: 05-07-2019 06:30:15.0090

ANALYSIS\_VERSION: 10.0.17134.226 x86fre

THREAD\_ATTRIBUTES:

OS\_LOCALE: ENU

PROBLEM\_CLASSES:

ID: [0n309]

Type: [@ACCESS\_VIOLATION]

Class: Addendum

Scope: BUCKET\_ID

```
Name: Omit
Data: Omit
PID: [Unspecified]
TID: [0xdbc]
Frame: [0] : msvcrt!_get_printf_count_output

ID: [0n282]
Type: [INVALID_POINTER_WRITE]
Class: Primary
Scope: DEFAULT_BUCKET_ID (Failure Bucket ID prefix)
       BUCKET_ID
Name: Add
Data: Omit
PID: [Unspecified]
TID: [0xdbc]
Frame: [0] : msvcrt!_get_printf_count_output
```

BUGCHECK\_STR: APPLICATION\_FAULT\_INVALID\_POINTER\_WRITE

PRIMARY\_PROBLEM\_CLASS: APPLICATION\_FAULT

LAST\_CONTROL\_TRANSFER: from 76c3d0ef to 76c3c886

STACK\_TEXT:

```
0018f208 76c3d0ef 004b11a7 fffffd8f0 0018f4a8
msvcrt!_get_printf_count_output+0x2e
0018f218 76c3d0ba 00001c2c 0233a138 ffffffff
msvcrt!_get_printf_count_output+0xa8
0018f4a8 76c4d399 0018f4c8 004b1190 00000000 msvcrt!_output_l+0xb57
0018f4e8 0041d884 0018f508 004b1190 02368b58 msvcrt!sprintf+0x5a
WARNING: Stack unwind information not available. Following frames may be
wrong.
```

```
0018f818 41414141 41414141 41414141 41414141 DevManBE+0x1d884
0018f81c 41414141 41414141 41414141 41414141 0x41414141
0018f820 41414141 41414141 41414141 41414141 0x41414141
0018f824 41414141 41414141 41414141 41414141 0x41414141
0018f828 41414141 41414141 41414141 41414141 0x41414141
0018f82c 41414141 41414141 41414141 41414141 0x41414141
0018f830 41414141 41414141 41414141 41414141 0x41414141
0018f834 41414141 41414141 41414141 41414141 0x41414141
0018f838 41414141 41414141 41414141 41414141 0x41414141
0018f83c 41414141 41414141 41414141 41414141 0x41414141
0018f840 41414141 41414141 41414141 41414141 0x41414141
0018f844 41414141 41414141 41414141 41414141 0x41414141
0018f848 41414141 41414141 41414141 41414141 0x41414141
0018f84c 41414141 41414141 41414141 41414141 0x41414141
0018f850 41414141 41414141 41414141 41414141 0x41414141
0018f854 41414141 41414141 41414141 41414141 0x41414141
0018f858 41414141 41414141 41414141 41414141 0x41414141
```



```
0018f928 41414141 41414141 41414141 41414141 0x41414141
0018f92c 41414141 41414141 41414141 41414141 0x41414141
0018f930 41414141 41414141 41414141 41414141 0x41414141
0018f934 41414141 41414141 41414141 41414141 0x41414141
0018f938 41414141 41414141 41414141 41414141 0x41414141
0018f93c 41414141 41414141 41414141 41414141 0x41414141
0018f940 41414141 41414141 41414141 41414141 0x41414141
0018f944 41414141 41414141 41414141 41414141 0x41414141
0018f948 41414141 41414141 41414141 41414141 0x41414141
0018f94c 41414141 41414141 41414141 41414141 0x41414141
0018f950 41414141 41414141 41414141 41414141 0x41414141
0018f954 41414141 41414141 41414141 41414141 0x41414141
0018f958 41414141 41414141 41414141 41414141 0x41414141
0018f95c 41414141 41414141 41414141 41414141 0x41414141
0018f960 41414141 41414141 41414141 41414141 0x41414141
0018f964 41414141 41414141 41414141 41414141 0x41414141
0018f968 41414141 41414141 41414141 41414141 0x41414141
0018f96c 41414141 41414141 41414141 41414141 0x41414141
0018f970 41414141 41414141 41414141 41414141 0x41414141
0018f974 41414141 41414141 41414141 41414141 0x41414141
0018f978 41414141 41414141 41414141 41414141 0x41414141
0018f97c 41414141 41414141 41414141 41414141 0x41414141
0018f980 41414141 41414141 41414141 41414141 0x41414141
0018f984 41414141 41414141 41414141 41414141 0x41414141
0018f988 41414141 41414141 41414141 41414141 0x41414141
0018f98c 41414141 41414141 41414141 41414141 0x41414141
0018f990 41414141 41414141 41414141 41414141 0x41414141
0018f994 41414141 41414141 41414141 41414141 0x41414141
0018f998 41414141 41414141 41414141 41414141 0x41414141
0018f99c 41414141 41414141 41414141 41414141 0x41414141
0018f9a0 41414141 41414141 41414141 41414141 0x41414141
0018f9a4 41414141 41414141 41414141 41414141 0x41414141
0018f9a8 41414141 41414141 41414141 41414141 0x41414141
0018f9ac 41414141 41414141 41414141 41414141 0x41414141
0018f9b0 41414141 41414141 41414141 41414141 0x41414141
0018f9b4 41414141 41414141 41414141 41414141 0x41414141
0018f9b8 41414141 41414141 41414141 41414141 0x41414141
0018f9bc 41414141 41414141 41414141 41414141 0x41414141
0018f9c0 41414141 41414141 41414141 41414141 0x41414141
0018f9c4 41414141 41414141 41414141 41414141 0x41414141
0018f9c8 41414141 41414141 41414141 41414141 0x41414141
0018f9cc 41414141 41414141 41414141 41414141 0x41414141
0018f9d0 41414141 41414141 41414141 41414141 0x41414141
0018f9d4 41414141 41414141 41414141 41414141 0x41414141
0018f9d8 41414141 41414141 41414141 41414141 0x41414141
0018f9dc 41414141 41414141 41414141 41414141 0x41414141
0018f9e0 41414141 41414141 41414141 41414141 0x41414141
0018f9e4 41414141 41414141 41414141 41414141 0x41414141
0018f9e8 41414141 41414141 41414141 41414141 0x41414141
```



```
0018fab8 41414141 41414141 41414141 41414141 0x41414141
0018fac0 41414141 41414141 41414141 41414141 0x41414141
0018fac4 41414141 41414141 41414141 41414141 0x41414141
0018fac8 41414141 41414141 41414141 41414141 0x41414141
0018facc 41414141 41414141 41414141 41414141 0x41414141
0018fad0 41414141 41414141 41414141 41414141 0x41414141
0018fad4 41414141 41414141 41414141 41414141 0x41414141
0018fad8 41414141 41414141 41414141 41414141 0x41414141
0018fadc 41414141 41414141 41414141 41414141 0x41414141
0018fae0 41414141 41414141 41414141 41414141 0x41414141
0018fae4 41414141 41414141 41414141 41414141 0x41414141
0018fae8 41414141 41414141 41414141 41414141 0x41414141
0018faec 41414141 41414141 41414141 41414141 0x41414141
0018faf0 41414141 41414141 41414141 41414141 0x41414141
0018faf4 41414141 41414141 41414141 41414141 0x41414141
0018faf8 41414141 41414141 41414141 41414141 0x41414141
0018fafc 41414141 41414141 41414141 41414141 0x41414141
0018fb00 41414141 41414141 41414141 41414141 0x41414141
0018fb04 41414141 41414141 41414141 41414141 0x41414141
0018fb08 41414141 41414141 41414141 41414141 0x41414141
0018fb0c 41414141 41414141 41414141 41414141 0x41414141
0018fb10 41414141 41414141 41414141 41414141 0x41414141
0018fb14 41414141 41414141 41414141 41414141 0x41414141
0018fb18 41414141 41414141 41414141 41414141 0x41414141
0018fb1c 41414141 41414141 41414141 41414141 0x41414141
0018fb20 41414141 41414141 41414141 41414141 0x41414141
0018fb24 41414141 41414141 41414141 41414141 0x41414141
0018fb28 41414141 41414141 41414141 41414141 0x41414141
0018fb2c 41414141 41414141 41414141 41414141 0x41414141
0018fb30 41414141 41414141 41414141 41414141 0x41414141
0018fb34 41414141 41414141 41414141 41414141 0x41414141
0018fb38 41414141 41414141 41414141 41414141 0x41414141
0018fb3c 41414141 41414141 41414141 41414141 0x41414141
0018fb40 41414141 41414141 41414141 41414141 0x41414141
0018fb44 41414141 41414141 41414141 41414141 0x41414141
0018fb48 41414141 41414141 41414141 41414141 0x41414141
0018fb4c 41414141 41414141 41414141 41414141 0x41414141
0018fb50 41414141 41414141 41414141 41414141 0x41414141
0018fb54 41414141 41414141 41414141 41414141 0x41414141
0018fb58 41414141 41414141 41414141 41414141 0x41414141
0018fb5c 41414141 41414141 41414141 41414141 0x41414141
0018fb60 41414141 41414141 41414141 41414141 0x41414141
0018fb64 41414141 41414141 41414141 41414141 0x41414141
```

STACK\_COMMAND: ~0s ; .cxr ; kb

THREAD\_SHA1\_HASH\_MOD\_FUNC: ccb6a9afab45f7e6c9b2418fac1b99e53ff7cb39

THREAD\_SHA1\_HASH\_MOD\_FUNC\_OFFSET: 32a659d6d84c16508a38f4e27162fc87ceb011a2

THREAD\_SHA1\_HASH\_MOD: 9c3b26ee1fe3f096862e62f6ce7af8a259f7d9c8

FAULT\_INSTR\_CODE: 1ff0288

SYMBOL\_STACK\_INDEX: 0

SYMBOL\_NAME: msvcrt!\_get\_printf\_count\_output+2e

FOLLOWUP\_NAME: MachineOwner

MODULE\_NAME: msvcrt

IMAGE\_NAME: msvcrt.dll

DEBUG\_FLR\_IMAGE\_TIMESTAMP: 4eeaf722

FAILURE\_BUCKET\_ID:  
INVALID\_POINTER\_WRITE\_c0000005\_msvcrt.dll!\_get\_printf\_count\_output

BUCKET\_ID:  
APPLICATION\_FAULT\_INVALID\_POINTER\_WRITE\_msvcrt!\_get\_printf\_count\_output+2e

FAILURE\_EXCEPTION\_CODE: c0000005

FAILURE\_IMAGE\_NAME: msvcrt.dll

BUCKET\_ID\_IMAGE\_STR: msvcrt.dll

FAILURE\_MODULE\_NAME: msvcrt

BUCKET\_ID\_MODULE\_STR: msvcrt

FAILURE\_FUNCTION\_NAME: \_get\_printf\_count\_output

BUCKET\_ID\_FUNCTION\_STR: \_get\_printf\_count\_output

BUCKET\_ID\_OFFSET: 2e

BUCKET\_ID\_MODTIMESTAMP: 4eeaf722

BUCKET\_ID\_MODCHECKSUM: a8f06

BUCKET\_ID\_MODVER\_STR: 7.0.7601.17744

BUCKET\_ID\_PREFIX\_STR: APPLICATION\_FAULT\_INVALID\_POINTER\_WRITE\_

FAILURE\_PROBLEM\_CLASS: APPLICATION\_FAULT

FAILURE\_SYMBOL\_NAME: msvcrt.dll!\_get\_printf\_count\_output

```
TARGET_TIME: 2019-05-07T13:30:33.000Z

OSBUILD: 7601

OSSERVICEPACK: 1

SERVICEPACK_NUMBER: 0

OS_REVISION: 0

OSPLATFORM_TYPE: x86

OSNAME: Windows 7

OSEDITION: Windows 7 WinNt (Service Pack 1) SingleUserTS

USER_LCID: 0

OSBUILD_TIMESTAMP: 2017-09-13 08:11:54

BUILDDATESTAMP_STR: 170913-0600

BUILDLAB_STR: win7sp1_ldr

BUILDOSVER_STR: 6.1.7601.23915.amd64fre.win7sp1_ldr.170913-0600

ANALYSIS_SESSION_ELAPSED_TIME: 4903

ANALYSIS_SOURCE: UM

FAILURE_ID_HASH_STRING:
um:invalid_pointer_write_c0000005_msvcrt.dll!_get_printf_count_output

FAILURE_ID_HASH: {27f390ea-67a8-7817-6f47-dac620d9cece}

Followup: MachineOwner
-----
```

## Exception Handler

```
0:000> d fs:[0]
0053:00000000 0018f80c 00190000 0018b000 00000000
0053:00000010 00001e00 00000000 7efdd000 00000000
0053:00000020 00000c10 00000dbc 00000000 00625340
0053:00000030 7efde000 00000003 00000000 00000000
0053:00000040 00000000 00000000 00000000 00000000
```

```
0053:00000050 00000000 00000000 00000000 00000000
0053:00000060 00000000 00000000 00000000 00000000
0053:00000070 00000000 00000000 00000000 00000000
0:000> d 0018f80c
0018f80c 41414141 41414141 41414141 41414141
0018f81c 41414141 41414141 41414141 41414141
0018f82c 41414141 41414141 41414141 41414141
0018f83c 41414141 41414141 41414141 41414141
0018f84c 41414141 41414141 41414141 41414141
0018f85c 41414141 41414141 41414141 41414141
0018f86c 41414141 41414141 41414141 41414141
0018f87c 41414141 41414141 41414141 41414141
```

## Step

```
0:000> t
(c74.60c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=41414141 edx=778c34dd esi=00000000
edi=00000000
eip=41414141 esp=0018ec70 ebp=0018ec90 iopl=0          nv up ei pl zr na pe
nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b
efl=00010246
41414141 ??          ???
0:000> dp esp
0018ec70 778c34c9 0018ed58 0018f80c 0018eda8
0018ec80 0018ed2c 0018f80c 778c34dd 0018f80c
0018ec90 0018ed40 778c349b 0018ed58 0018f80c
0018eca0 0018eda8 0018ed2c 41414141 00000000
0018ecb0 0018ed58 0018f80c 778c343c 0018ed58
0018ecc0 0018f80c 0018eda8 0018ed2c 41414141
0018ecd0 0018f4c8 0018ed58 0018f280 00000000
0018ece0 00000000 00000000 00000000 00000000
```