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
*******************************************************************************
***
*
*
*                        Exception Analysis
*
*
*
*******************************************************************************
***

*** 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 ffffd8f0 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
0018f85c 41414141 41414141 41414141 41414141 0x41414141
0018f860 41414141 41414141 41414141 41414141 0x41414141
0018f864 41414141 41414141 41414141 41414141 0x41414141
0018f868 41414141 41414141 41414141 41414141 0x41414141
```

```
0018f86c 41414141 41414141 41414141 41414141 0x41414141
0018f870 41414141 41414141 41414141 41414141 0x41414141
0018f874 41414141 41414141 41414141 41414141 0x41414141
0018f878 41414141 41414141 41414141 41414141 0x41414141
0018f87c 41414141 41414141 41414141 41414141 0x41414141
0018f880 41414141 41414141 41414141 41414141 0x41414141
0018f884 41414141 41414141 41414141 41414141 0x41414141
0018f888 41414141 41414141 41414141 41414141 0x41414141
0018f88c 41414141 41414141 41414141 41414141 0x41414141
0018f890 41414141 41414141 41414141 41414141 0x41414141
0018f894 41414141 41414141 41414141 41414141 0x41414141
0018f898 41414141 41414141 41414141 41414141 0x41414141
0018f89c 41414141 41414141 41414141 41414141 0x41414141
0018f8a0 41414141 41414141 41414141 41414141 0x41414141
0018f8a4 41414141 41414141 41414141 41414141 0x41414141
0018f8a8 41414141 41414141 41414141 41414141 0x41414141
0018f8ac 41414141 41414141 41414141 41414141 0x41414141
0018f8b0 41414141 41414141 41414141 41414141 0x41414141
0018f8b4 41414141 41414141 41414141 41414141 0x41414141
0018f8b8 41414141 41414141 41414141 41414141 0x41414141
0018f8bc 41414141 41414141 41414141 41414141 0x41414141
0018f8c0 41414141 41414141 41414141 41414141 0x41414141
0018f8c4 41414141 41414141 41414141 41414141 0x41414141
0018f8c8 41414141 41414141 41414141 41414141 0x41414141
0018f8cc 41414141 41414141 41414141 41414141 0x41414141
0018f8d0 41414141 41414141 41414141 41414141 0x41414141
0018f8d4 41414141 41414141 41414141 41414141 0x41414141
0018f8d8 41414141 41414141 41414141 41414141 0x41414141
0018f8dc 41414141 41414141 41414141 41414141 0x41414141
0018f8e0 41414141 41414141 41414141 41414141 0x41414141
0018f8e4 41414141 41414141 41414141 41414141 0x41414141
0018f8e8 41414141 41414141 41414141 41414141 0x41414141
0018f8ec 41414141 41414141 41414141 41414141 0x41414141
0018f8f0 41414141 41414141 41414141 41414141 0x41414141
0018f8f4 41414141 41414141 41414141 41414141 0x41414141
0018f8f8 41414141 41414141 41414141 41414141 0x41414141
0018f8fc 41414141 41414141 41414141 41414141 0x41414141
0018f900 41414141 41414141 41414141 41414141 0x41414141
0018f904 41414141 41414141 41414141 41414141 0x41414141
0018f908 41414141 41414141 41414141 41414141 0x41414141
0018f90c 41414141 41414141 41414141 41414141 0x41414141
0018f910 41414141 41414141 41414141 41414141 0x41414141
0018f914 41414141 41414141 41414141 41414141 0x41414141
0018f918 41414141 41414141 41414141 41414141 0x41414141
0018f91c 41414141 41414141 41414141 41414141 0x41414141
0018f920 41414141 41414141 41414141 41414141 0x41414141
0018f924 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
0018f9ec 41414141 41414141 41414141 41414141 0x41414141
0018f9f0 41414141 41414141 41414141 41414141 0x41414141
0018f9f4 41414141 41414141 41414141 41414141 0x41414141
0018f9f8 41414141 41414141 41414141 41414141 0x41414141
0018f9fc 41414141 41414141 41414141 41414141 0x41414141
0018fa00 41414141 41414141 41414141 41414141 0x41414141
```

```
0018fa04 41414141 41414141 41414141 41414141 0x41414141
0018fa08 41414141 41414141 41414141 41414141 0x41414141
0018fa0c 41414141 41414141 41414141 41414141 0x41414141
0018fa10 41414141 41414141 41414141 41414141 0x41414141
0018fa14 41414141 41414141 41414141 41414141 0x41414141
0018fa18 41414141 41414141 41414141 41414141 0x41414141
0018fa1c 41414141 41414141 41414141 41414141 0x41414141
0018fa20 41414141 41414141 41414141 41414141 0x41414141
0018fa24 41414141 41414141 41414141 41414141 0x41414141
0018fa28 41414141 41414141 41414141 41414141 0x41414141
0018fa2c 41414141 41414141 41414141 41414141 0x41414141
0018fa30 41414141 41414141 41414141 41414141 0x41414141
0018fa34 41414141 41414141 41414141 41414141 0x41414141
0018fa38 41414141 41414141 41414141 41414141 0x41414141
0018fa3c 41414141 41414141 41414141 41414141 0x41414141
0018fa40 41414141 41414141 41414141 41414141 0x41414141
0018fa44 41414141 41414141 41414141 41414141 0x41414141
0018fa48 41414141 41414141 41414141 41414141 0x41414141
0018fa4c 41414141 41414141 41414141 41414141 0x41414141
0018fa50 41414141 41414141 41414141 41414141 0x41414141
0018fa54 41414141 41414141 41414141 41414141 0x41414141
0018fa58 41414141 41414141 41414141 41414141 0x41414141
0018fa5c 41414141 41414141 41414141 41414141 0x41414141
0018fa60 41414141 41414141 41414141 41414141 0x41414141
0018fa64 41414141 41414141 41414141 41414141 0x41414141
0018fa68 41414141 41414141 41414141 41414141 0x41414141
0018fa6c 41414141 41414141 41414141 41414141 0x41414141
0018fa70 41414141 41414141 41414141 41414141 0x41414141
0018fa74 41414141 41414141 41414141 41414141 0x41414141
0018fa78 41414141 41414141 41414141 41414141 0x41414141
0018fa7c 41414141 41414141 41414141 41414141 0x41414141
0018fa80 41414141 41414141 41414141 41414141 0x41414141
0018fa84 41414141 41414141 41414141 41414141 0x41414141
0018fa88 41414141 41414141 41414141 41414141 0x41414141
0018fa8c 41414141 41414141 41414141 41414141 0x41414141
0018fa90 41414141 41414141 41414141 41414141 0x41414141
0018fa94 41414141 41414141 41414141 41414141 0x41414141
0018fa98 41414141 41414141 41414141 41414141 0x41414141
0018fa9c 41414141 41414141 41414141 41414141 0x41414141
0018faa0 41414141 41414141 41414141 41414141 0x41414141
0018faa4 41414141 41414141 41414141 41414141 0x41414141
0018faa8 41414141 41414141 41414141 41414141 0x41414141
0018faac 41414141 41414141 41414141 41414141 0x41414141
0018fab0 41414141 41414141 41414141 41414141 0x41414141
0018fab4 41414141 41414141 41414141 41414141 0x41414141
0018fab8 41414141 41414141 41414141 41414141 0x41414141
0018fabc 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_MODTIMEDATESTAMP:  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
```

```
0:000> !exchain
0018f80c: 41414141
Invalid exception stack at 41414141
```

Exploitable?

```
0:005> .load msec
0:005> !exploitable

!exploitable 1.6.0.0
*** 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
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - Exception Handler Chain Corrupted
starting at msvcrt!_get_printf_count_output+0x000000000000002e
(Hash=0x65c12afd.0x93798406)

Corruption of the exception handler chain is considered exploitable
```

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
```

SafeSEH exploit

```
0:005> .load pykd.pyd
0:005> !py mona seh
Hold on...
[+] Command used:
!py mona.py seh

---------- Mona command started on 2019-05-07 06:48:06 (v2.0, rev 585) -----
-----
[+] Processing arguments and criteria
    - Pointer access level : X
[+] Generating module info table, hang on...
    - Processing modules
    - Done. Let's rock 'n roll.
[+] Querying 3 modules
    - Querying module MSVCP60.dll
    - Querying module DevManBE.exe
    - Querying module DCL.dll
[+] Setting pointer access level criteria to 'R', to increase search results
    New pointer access level : R
[+] Preparing output file 'seh.txt'
    - (Re)setting logfile c:\_c\mona\seh.txt
[+] Writing results to c:\_c\mona\seh.txt
    - Number of pointers of type 'add esp,8 # ret 0x04' : 2
    - Number of pointers of type 'pop ebp # pop ebx # ret 0x04' : 4
    - Number of pointers of type 'pop edi # pop esi # ret 0x04' : 17
    - Number of pointers of type 'pop esi # pop ebx # ret 0x04' : 111
    - Number of pointers of type 'pop ecx # pop ecx # ret ' : 39
    - Number of pointers of type 'pop edi # pop esi # ret 0x08' : 13
    - Number of pointers of type 'pop esi # pop ebx # ret 0x08' : 6
    - Number of pointers of type 'add esp,8 # ret 0x08' : 20
    - Number of pointers of type 'pop ecx # pop ecx # ret 0x04' : 2
    - Number of pointers of type 'call dword ptr ss:[esp+08]' : 4
    - Number of pointers of type 'pop edi # pop esi # ret 0x20' : 4
    - Number of pointers of type 'pop esi # pop edi # ret ' : 1
    - Number of pointers of type 'pop ebx # pop ecx # ret 0x08' : 2
    - Number of pointers of type 'pop ebx # pop ebp # ret ' : 1
    - Number of pointers of type 'pop ebx # pop ecx # ret ' : 8
    - Number of pointers of type 'pop esi # pop ebp # ret 0x0c' : 4
    - Number of pointers of type 'pop ebx # pop ebp # ret 0x10' : 15
    - Number of pointers of type 'pop ebx # pop ecx # ret 0x04' : 6
    - Number of pointers of type 'call dword ptr ss:[esp+2c]' : 1
    - Number of pointers of type 'pop edi # pop ebp # ret 0x0c' : 1
    - Number of pointers of type 'pop ebp # pop ebx # ret 0x10' : 1
    - Number of pointers of type 'pop ebx # pop ebp # ret 0x0c' : 12
    - Number of pointers of type 'pop esi # pop ecx # ret ' : 10
    - Number of pointers of type 'pop ebp # pop ecx # ret 0x0c' : 1
    - Number of pointers of type 'pop edi # pop esi # ret 0x10' : 4
```

```
    - Number of pointers of type 'pop esi # pop ebx # ret 0x10' : 4
    - Number of pointers of type 'pop esi # pop edi # ret 0x04' : 1
    - Number of pointers of type 'pop edi # pop esi # ret ' : 27
    - Number of pointers of type 'pop esi # pop ebx # ret ' : 23
    - Number of pointers of type 'pop esi # pop ebx # ret 0x0c' : 8
    - Number of pointers of type 'pop edi # pop esi # ret 0x0c' : 19
    - Number of pointers of type 'pop esi # pop ebp # ret ' : 10
    - Number of pointers of type 'pop edi # pop ebx # ret 0x04' : 1
    - Number of pointers of type 'pop ebx # pop edi # ret ' : 3
    - Number of pointers of type 'pop edi # pop ebx # ret ' : 2
    - Number of pointers of type 'pop esi # pop ebp # ret 0x20' : 3
    - Number of pointers of type 'pop ebx # pop ebp # ret 0x20' : 1
    - Number of pointers of type 'pop edi # pop ebp # ret ' : 6
    - Number of pointers of type 'pop ebp # pop ebx # ret ' : 12
    - Number of pointers of type 'pop esi # pop ecx # ret 0x04' : 4
    - Number of pointers of type 'pop ebp # pop ebx # ret 0x0c' : 1
    - Number of pointers of type 'pop ebp # pop ebx # ret 0x08' : 6
    - Number of pointers of type 'call dword ptr ss:[ebp-18]' : 1
    - Number of pointers of type 'pop ebx # pop esi # ret ' : 1
    - Number of pointers of type 'add esp,8 # ret ' : 42
    - Number of pointers of type 'add esp,4 # pop ebp # ret ' : 7
    - Number of pointers of type 'pop esi # pop ebp # ret 0x04' : 5
[+] Results :
0x1000672b |   0x1000672b : add esp,8 # ret 0x04 | null {PAGE_EXECUTE_READ}
[DCL.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0-
(C:\Program Files (x86)\HP\Power Manager\DCL.dll)
0x1000678d |   0x1000678d : add esp,8 # ret 0x04 | null {PAGE_EXECUTE_READ}
[DCL.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0-
(C:\Program Files (x86)\HP\Power Manager\DCL.dll)
0x0047001c |   0x0047001c : pop ebp # pop ebx # ret 0x04 |
startnull,unicode,asciiprint,ascii {PAGE_EXECUTE_READ} [DevManBE.exe] ASLR:
False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Program Files
(x86)\HP\Power Manager\DevManBE.exe)
0x0047f13d |   0x0047f13d : pop ebp # pop ebx # ret 0x04 | startnull
{PAGE_EXECUTE_READ} [DevManBE.exe] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v-1.0- (C:\Program Files (x86)\HP\Power
Manager\DevManBE.exe)
0x10002b0a |   0x10002b0a : pop ebp # pop ebx # ret 0x04 | null
{PAGE_EXECUTE_READ} [DCL.dll] ASLR: False, Rebase: False, SafeSEH: False,
OS: False, v-1.0- (C:\Program Files (x86)\HP\Power Manager\DCL.dll)
0x10002b64 |   0x10002b64 : pop ebp # pop ebx # ret 0x04 | null
{PAGE_EXECUTE_READ} [DCL.dll] ASLR: False, Rebase: False, SafeSEH: False,
OS: False, v-1.0- (C:\Program Files (x86)\HP\Power Manager\DCL.dll)
0x7608165a |   0x7608165a : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x7608573e |   0x7608573e : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
```

```
0x76085758 |   0x76085758 : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x760857cf |   0x760857cf : pop edi # pop esi # ret 0x04 |
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x760857e9 |   0x760857e9 : pop edi # pop esi # ret 0x04 |
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x76085815 |   0x76085815 : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x76085cdd |   0x76085cdd : pop edi # pop esi # ret 0x04 |
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x76097a75 |   0x76097a75 : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x76097aa5 |   0x76097aa5 : pop edi # pop esi # ret 0x04 |
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x76097f2f |   0x76097f2f : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x76097f60 |   0x76097f60 : pop edi # pop esi # ret 0x04 | ascii
{PAGE_EXECUTE_READ} [MSVCP60.dll] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v6.2.3104.0 (C:\Program Files (x86)\HP\Power
Manager\MSVCP60.dll)
0x00444527 |   0x00444527 : pop edi # pop esi # ret 0x04 |
startnull,asciiprint,ascii {PAGE_EXECUTE_READ} [DevManBE.exe] ASLR: False,
Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Program Files
(x86)\HP\Power Manager\DevManBE.exe)
0x00476b25 |   0x00476b25 : pop edi # pop esi # ret 0x04 |
startnull,asciiprint,ascii {PAGE_EXECUTE_READ} [DevManBE.exe] ASLR: False,
Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Program Files
(x86)\HP\Power Manager\DevManBE.exe)
0x004820d1 |   0x004820d1 : pop edi # pop esi # ret 0x04 | startnull
{PAGE_EXECUTE_READ} [DevManBE.exe] ASLR: False, Rebase: False, SafeSEH:
False, OS: False, v-1.0- (C:\Program Files (x86)\HP\Power
Manager\DevManBE.exe)
... Please wait while I'm processing all remaining results and writing
everything to file...
[+] Done. Only the first 20 pointers are shown here. For more pointers, open
```

```
c:\_c\mona\seh.txt...
    Found a total of 476 pointers

[+] This mona.py action took 0:00:02.870000
```