TALOS VULNERABILITY REPORT

TALOS-2016-0087

INTEL HD GRAPHICS WINDOWS KERNEL DRIVER (IGDKMD64) CODE EXECUTION VULNERABILITY

JULY 11, 2016

REPORT ID

CVE-2016-5647

SUMMARY

A vulnerability exists in the communication functionality of Intel Graphics Kernel Mode Driver. A specially crafted message can cause a vulnerability resulting in executing arbitrary code. An attacker can send specific message to trigger this vulnerability and escalate his privileges on the local system.

TESTED VERSIONS

- Intel HD Graphics Windows Kernel Mode Driver, Version 10.18.14.4264 (requires physical machine)

PRODUCT URLS

http://intel.com

CVSSV3 SCORE

8.4 - CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:U/RC:C

DETAILS

This vulnerability can be triggered by sending specially crafted D3DKMTEscape request to the Intel HD graphics driver.

The faulting code is located in the Intel Graphics Kernel Mode Driver driver (igdkmd64 module):

```
.text:00000000001BE910 loc_1BE910:                             ; CODE XREF: sub_1BE4F0+43E
j
.text:00000000001BE910                 mov     edx, [rdi+rbx*4+4]
.text:00000000001BE914                 mov     rcx, rsi
.text:00000000001BE917                 call    qword ptr [rsi+0C8h]
.text:00000000001BE91D                 mov     rcx, rax
.text:00000000001BE920                 call    qword ptr [rax+250h]     * arbitrary code e
xecution here*
```

Instruction at 0x1BE920 tries to execute a memory location pointed by qword value located at @rax+0x250. In this case @rax value points to NULL (memory location at address 0).

CRASH INFORMATION

Additional information from the crash dump:

```
FOLLOWUP_IP:
igdkmd64!hybDriverEntry+1485b0
fffff801`61fd0920 ff9050020000    call    qword ptr [rax+250h]
SYMBOL_STACK_INDEX:  0
SYMBOL_NAME:  igdkmd64!hybDriverEntry+1485b0
FOLLOWUP_NAME:  MachineOwner
MODULE_NAME: igdkmd64
IMAGE_NAME:  igdkmd64.sys
DEBUG_FLR_IMAGE_TIMESTAMP:  55c196be
STACK_COMMAND:  .cxr 0xffffd00031747590 ; kb
BUCKET_ID_FUNC_OFFSET:  1485b0
FAILURE_BUCKET_ID:  0x3B_igdkmd64!hybDriverEntry
BUCKET_ID:  0x3B_igdkmd64!hybDriverEntry
ANALYSIS_SOURCE:  KM
FAILURE_ID_HASH_STRING:  km:0x3b_igdkmd64!hybdriverentry
FAILURE_ID_HASH:  {b388e4ef-f5cc-39ba-96af-1f55e1c7ae40}
etAddr           : Args to Child
 : Call Site
fffff801`61fb33b1 : ffffd000`31748320 ffffe001`00000003 ffffd000`317480c0 00000000`0000004
6 : igdkmd64!hybDriverEntry+0x1485b0
fffff801`61ee4166 : ffffd000`31748320 00000025`000f003f ffffe001`7209e080 ffffc001`a13db10
0 : igdkmd64!hybDriverEntry+0x12b041
fffff801`61edfa4a : ffffc001`00000000 00000000`00000000 00000000`00000000 00000000`0000000
0 : igdkmd64!hybDriverEntry+0x5bdf6
fffff801`61ed5b1f : 00000000`00000001 00000000`00000000 ffffc001`a5198900 00000000`00007ff
f : igdkmd64!hybDriverEntry+0x576da
fffff801`61edc798 : ffff23ff`00000000 00000000`00000000 00000000`00000001 ffffc001`a519894
0 : igdkmd64!hybDriverEntry+0x4d7af
fffff801`61ed51b5 : 00000000`00000000 00000000`00000204 ffffc001`a5198740 00000000`0000000
0 : igdkmd64!hybDriverEntry+0x54428
fffff801`61e48613 : ffffd000`31748768 00000000`00000000 ffffe001`6dcd1000 ffffe001`6dcd100
0 : igdkmd64!hybDriverEntry+0x4ce45
fffff801`61e48507 : ffffe001`6ddc4140 ffffd000`31748ad0 ffffe001`6ddc4140 00000000`0000000
1 : igdkmd64+0x26613
fffff801`60d1ea34 : ffffd000`31748768 ffffe001`6ddc4140 ffffd000`31748768 ffffe001`6ddc414
0 : igdkmd64+0x26507
fffff801`60ceffef : ffffe001`6ddc4140 ffffd000`31748b80 ffffc001`a51d9000 fffff800`0000000
0 : dxgkrnl!DXGADAPTER::DdiEscape+0x48
fffff960`002c563b : ffffe001`6ddc4140 ffffe001`7209e080 00000000`7f5ac000 ffffe001`6ddc414
0 : dxgkrnl!DxgkEscape+0x54f
fffff800`ac5d41b3 : ffffe001`7209e080 00000000`7f5aa000 00000000`00e6fdb0 00000000`0000000
0 : win32k!NtGdiDdDDIEscape+0x53
00000000`770574aa : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`0000000
0 : nt!KiSystemServiceCopyEnd+0x13
00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`0000000
0 : 0x770574aa
```

CREDIT

Discovered by Piotr Bania of Cisco Talos.

TIMELINE

2016-03-07 - Vendor Notification
2016-07-11 – Public Disclosure