Talos Vulnerability Report

TALOS-2020-1042

AMD Radeon DirectX 11 Driver atidxx64.dll Shader Functionality RESOURCE Code Execution Vulnerability

JULY 14, 2020

CVE NUMBER

CVE-2020-6102

Summary

An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide a a specially crafted shader file to trigger this vulnerability, resulting in code execution. This vulnerability can be triggered from a HYPER-V guest using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly).

Tested Versions

AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000

Product URLs

https://amd.com

CVSSv3 Score

8.5 - CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-787 - Out-of-bounds Write

Details

AMD Graphics drivers is a software for AMD Graphics GPU installed on the PC. It is a software used to communicate between the operating system and the GPU device. This software is required in most cases for the hardware device to function properly.

This vulnerability can be triggered by supplying a malformed pixel shader. This leads to a memory corruption issue in AMD graphics drivers.

Example of pixel shader triggering the bug:

```
ps_4_1
dcl_global_flags refactoringAllowed
dcl_constant_buffer cb0[1].xyzw, immediateIndexed
dcl_resource_texture2d resource[-1294532608]
dcl_output o0.xyzw
dcl_temps 2
...
```

By modifying the `dcl_resource_texture2d` (this instruction declares a non-multisampled shader-input resource) operand size (`resource[X]`), it is possible to trigger a memory corruption in AMD graphics driver.
Attacker can control the destination address by modifying the shader bytecode.

```
0:000> r
rax=00000000b2d70000 rbx=0000000000000002 rcx=0000000000000003
rdx=0000000000000020 rsi=0000000000000080 rdi=0000000000000000
rip=00007ffb695b1a88 rsp=0000000df253b760 rbp=0000000df253b860
 r8=0000000000000005  r9=0000000000000005 r10=0000000000000005
r11=0000000000000004 r12=0000000000000005 r13=0000000000000001
r14=000001b7d0390080 r15=0000000000000058
iopl=0         nv up ei ng nz ac po cy
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010297
atidxx64!XdxQueryTlsLookupTable+0x4bc98:
00007ffb`695b1a88 41898c86cc4e0000 mov     dword ptr [r14+rax*4+4ECCh],ecx ds:000001ba`9b954f4c=????????
```

Stack trace:

```
0:000> kb
 # RetAddr           : Args to Child                                                           : Call Site
00 00007ffb`695b0b9b : 000001b7`00000000 00000000`00000000 00000000`00000000 00000000`00000058 : atidxx64!XdxQueryTlsLookupTable+0x4bc98
01 00007ffb`695c370e : 00000000`00000000 000001b7`d03955b0 00000000`00000001 000001b7`d0390080 : atidxx64!XdxQueryTlsLookupTable+0x4adab
02 00007ffb`695abd1e : 000001b7`d03955b0 00000000`00000000 00000000`00000000 0000000d`f253c700 : atidxx64!XdxQueryTlsLookupTable+0x5d91e
03 00007ffb`695abb12 : 000001b7`d0171b40 000001b7`d0217a00 0000000d`f253c700 00000000`00000000 : atidxx64!XdxQueryTlsLookupTable+0x45f2e
04 00007ffb`69ee1e71 : 00000000`00000000 0000000d`f253c700 000001b7`d0171b40 0000000d`f253c390 : atidxx64!XdxQueryTlsLookupTable+0x45d22
05 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 0000000d`f253c700 00000000`00000020 :
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
06 00007ffb`695ec033 : 000001b7`d038e590 00000000`00000003 00000000`00000003 00000000`00000000 : atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
07 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 000001b7`c9fa0000 000001b7`00000003 : atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
08 00007ffb`69d8dde5 : 00007ffb`69560000 000001b7`d0120208 00000000`00000000 ffffffff`ffffffff : atidxx64!XdxQueryTlsLookupTable+0x75ee
09 00007ffb`69d897f3 : 00000000`00000000 0000000d`f253c610 000001b7`d038c540 000001b7`cb9148b8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
0a 00007ffb`69df4a59 : 00000000`00000000 0000000d`f253c700 000001b7`d038bec0 000001b7`cff738f0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
0b 00007ffb`69581220 : 000001b7`cff73a08 000001b7`cff8d410 000001b7`ca04d718 000001b7`cff24660 :
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
0c 00007ffb`75588edc : 00000000`00000000 0000000d`f253c8f0 000001b7`cff739f8 000001b7`cff72a18 : atidxx64!XdxQueryTlsLookupTable+0x1b430
0d 00007ffb`7559295f : 0000000d`00000001 000001b7`cff89828 000001b7`cff739f8 000001b7`cff7f910 :
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
0e 00007ffb`7559289a : 0000000d`f253e280 00007ffb`1edb7a18 000001b7`cff73650 00007ffb`1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
0f 00007ffb`7557ee58 : 000001b7`cff738e8 0000000d`f253e280 0000000d`f253e200 00007ffb`1edb7a18 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
10 00007ffb`7558b17d : 00000000`0000006b 000001b7`cff73698 000001b7`c9fa0000 00000000`40000062 : d3d11!CDevice::CreateLayeredChild+0xc88
11 00007ffb`1ed43ade : 000001b7`cff73698 00000000`00000000 000001b7`ca061c10 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
12 00007ffb`1ed30d83 : 000001b7`cff73748 00000000`00000000 00000000`00000000 000001b7`cff73650 :
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
13 00007ffb`1eceda23 : 000001b7`cff73680 000001b7`cff73678 000001b7`cff73678 000001b7`cff73650 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
14 00007ffb`7558b950 : 000001b7`cff73650 00000000`00000030 0000000d`f253e370 000001b7`c9fa0000 :
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
15 00007ffb`755714f4 : 000001b7`ca04bad0 0000000d`00000009 000001b7`cff72d40 000001b7`ca04c968 :
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
16 00007ffb`75571463 : 000001b7`cff72d40 00000000`0000c000 00000000`00000000 00000000`00000001 :
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
17 00007ffb`755711e8 : 000001b7`ca04c968 000001b7`cff72d40 00000000`00000438 00000000`00000000 :
d3d11!CDevice::CreatePixelShader_Worker+0x203
18 00007ffb`1ed19f85 : 000001b7`ca04bb28 000001b7`00000001 000001b7`ca04bb28 000001b7`ca04bb30 : d3d11!CDevice::CreatePixelShader+0x28
*** WARNING: Unable to verify checksum for POC_EXEC11.exe
19 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000 0000000d`f253e858 000001b7`cff72d54 :
D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115
1a 00007ff6`7fbd8c3c : 000001b7`ca04bb30 000001b7`cff72d40 00000000`00000438 cdcdcdcd`00000000 : POC_EXEC11+0x1872d
1b 00007ff6`7fbd61b8 : 000001b7`ca04bb30 000001b7`c9fdd300 000001b7`00000000 00007ff6`42de0387 : POC_EXEC11+0x18c3c
1c 00007ff6`7fbeaa50 : 000001b7`ca04bb30 000001b7`c9fe0030 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8
1d 00007ff6`7fbe6e22 : 000001b7`ca006a00 000001b7`ca006a01 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50
1e 00007ff6`7fbe319c : 000001b7`ca006a00 00310043`00000201 00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22
1f 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 : POC_EXEC11+0x2319c
20 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 000001b7`c9fa3300 00007ff6`0000000a : POC_EXEC11+0x147dd
21 00007ff6`7fc833fe : 00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d
22 00007ff6`7fc832be : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe
23 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc32be
24 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9
25 00007ffb`7b3aced1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
26 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
```

Crash Information

0:000> !analyze -v *************************** * * * Exception Analysis * * * ***************************

```
KEY_VALUES_STRING: 1

        Key  : AV.Fault
        Value: Write

        Key  : Timeline.OS.Boot.DeltaSec
        Value: 4549

        Key  : Timeline.Process.Start.DeltaSec
        Value: 88


PROCESSES_ANALYSIS: 1

SERVICE_ANALYSIS: 1

STACKHASH_ANALYSIS: 1

TIMELINE_ANALYSIS: 1

Timeline: !analyze.Start
        Name: <blank>
        Time: 2020-03-21T18:47:40.944Z
        Diff: 55 mSec

Timeline: Dump.Current
        Name: <blank>
        Time: 2020-03-21T18:47:41.0Z
        Diff: 0 mSec

Timeline: Process.Start
        Name: <blank>
        Time: 2020-03-21T18:46:13.0Z
        Diff: 88000 mSec

Timeline: OS.Boot
        Name: <blank>
        Time: 2020-03-21T17:31:52.0Z
        Diff: 4549000 mSec


DUMP_CLASS: 2

DUMP_QUALIFIER: 0

FAULTING_IP: 
atidxx64!XdxQueryTlsLookupTable+4bc98
00007ffb`695b1a88 41898c86cc4e0000 mov     dword ptr [r14+rax*4+4ECCh],ecx

EXCEPTION_RECORD:  (.exr -1)
ExceptionAddress: 00007ffb695b1a88 (atidxx64!XdxQueryTlsLookupTable+0x000000000004bc98)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000001
   Parameter[1]: 000001ba9b954f4c
Attempt to write to address 000001ba9b954f4c

FAULTING_THREAD:  000037f4

PROCESS_NAME:  POC_EXEC11.exe

FOLLOWUP_IP: 
atidxx64!XdxQueryTlsLookupTable+4bc98
00007ffb`695b1a88 41898c86cc4e0000 mov     dword ptr [r14+rax*4+4ECCh],ecx

WRITE_ADDRESS:  000001ba9b954f4c 

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

EXCEPTION_CODE_STR:  c0000005

EXCEPTION_PARAMETER1:  0000000000000001

EXCEPTION_PARAMETER2:  000001ba9b954f4c

WATSON_BKT_PROCSTAMP:  5e1a142e

WATSON_BKT_MODULE:  atidxx64.dll

WATSON_BKT_MODSTAMP:  5e59a28f

WATSON_BKT_MODOFFSET:  51a88

WATSON_BKT_MODVER:  26.20.15019.19000

MODULE_VER_PRODUCT:  Advanced Micro Devices, Inc. Radeon DirectX 11 Driver

BUILD_VERSION_STRING:  18362.1.amd64fre.19h1_release.190318-1202

MODLIST_WITH_TSCHKSUM_HASH:  a73f1234b36e2e664580e5ad78c3af0f4f4150cb

MODLIST_SHA1_HASH:  9031f8459f7e5fc3a138b523cf0b4253bd77b7b8

NTGLOBALFLAG:  470

PROCESS_BAM_CURRENT_THROTTLED: 0

PROCESS_BAM_PREVIOUS_THROTTLED: 0

APPLICATION_VERIFIER_FLAGS:  0

PRODUCT_TYPE:  1

SUITE_MASK:  272

DUMP_TYPE:  fe

ANALYSIS_SESSION_HOST:  CLAB

ANALYSIS_SESSION_TIME:  03-21-2020 19:47:40.0944

ANALYSIS_VERSION: 10.0.18362.1 amd64fre

THREAD_ATTRIBUTES: 
```

```
OS_LOCALE:  ENU

BUGCHECK_STR:  APPLICATION_FAULT_INVALID_POINTER_WRITE_EXPLOITABLE

DEFAULT_BUCKET_ID:  INVALID_POINTER_WRITE_EXPLOITABLE

PRIMARY_PROBLEM_CLASS:  APPLICATION_FAULT

PROBLEM_CLASSES: 

        ID:     [0n313]
        Type:   [@ACCESS_VIOLATION]
        Class:  Addendum
        Scope:  BUCKET_ID
        Name:   Omit
        Data:   Omit
        PID:    [Unspecified]
        TID:    [0x37f4]
        Frame:  [0] : atidxx64!XdxQueryTlsLookupTable

        ID:     [0n286]
        Type:   [INVALID_POINTER_WRITE]
        Class:  Primary
        Scope:  DEFAULT_BUCKET_ID (Failure Bucket ID prefix)
                BUCKET_ID
        Name:   Add
        Data:   Omit
        PID:    [Unspecified]
        TID:    [0x37f4]
        Frame:  [0] : atidxx64!XdxQueryTlsLookupTable

        ID:     [0n117]
        Type:   [EXPLOITABLE]
        Class:  Addendum
        Scope:  DEFAULT_BUCKET_ID (Failure Bucket ID prefix)
                BUCKET_ID
        Name:   Add
        Data:   Omit
        PID:    [0x12dc]
        TID:    [0x37f4]
        Frame:  [0] : atidxx64!XdxQueryTlsLookupTable

LAST_CONTROL_TRANSFER:  from 00007ffb695b0b9b to 00007ffb695b1a88

STACK_TEXT:  
0000000d`f253b760 00007ffb`695b0b9b : 000001b7`00000000 00000000`00000000 00000000`00000000 00000000`00000058 :
atidxx64!XdxQueryTlsLookupTable+0x4bc98
0000000d`f253c0a0 00007ffb`695c370e : 00000000`00000000 000001b7`d03955b0 00000000`00000001 000001b7`d0390080 :
atidxx64!XdxQueryTlsLookupTable+0x4adab
0000000d`f253c150 00007ffb`695abd1e : 000001b7`d03955b0 00000000`00000000 00000000`00000000 0000000d`f253c700 :
atidxx64!XdxQueryTlsLookupTable+0x5d91e
0000000d`f253c180 00007ffb`695abb12 : 000001b7`d0171b40 000001b7`d0217a00 0000000d`f253c700 00000000`00000000 :
atidxx64!XdxQueryTlsLookupTable+0x45f2e
0000000d`f253c260 00007ffb`69ee1e71 : 00000000`00000000 0000000d`f253c700 000001b7`d0171b40 0000000d`f253c390 :
atidxx64!XdxQueryTlsLookupTable+0x45d22
0000000d`f253c290 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 0000000d`f253c700 00000000`00000020 :
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
0000000d`f253c2d0 00007ffb`695ec033 : 000001b7`d038e590 00000000`00000003 00000000`00000003 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
0000000d`f253c310 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 000001b7`c9fa0000 000001b7`00000003 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
0000000d`f253c3a0 00007ffb`69d8dde5 : 00007ffb`69560000 000001b7`d0120208 00000000`00000000 ffffffff`ffffffff :
atidxx64!XdxQueryTlsLookupTable+0x75ee
0000000d`f253c3e0 00007ffb`69d897f3 : 00000000`00000000 0000000d`f253c610 000001b7`d038c540 000001b7`cb9148b8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
0000000d`f253c510 00007ffb`69df4a59 : 00000000`00000000 0000000d`f253c700 000001b7`d038bec0 000001b7`cff738f0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
0000000d`f253c6b0 00007ffb`69581220 : 000001b7`cff73a08 000001b7`cff8d410 000001b7`ca04d718 000001b7`cff24660 :
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
0000000d`f253c6e0 00007ffb`75588edc : 00000000`00000000 0000000d`f253c8f0 000001b7`cff739f8 000001b7`cff72a18 :
atidxx64!XdxQueryTlsLookupTable+0x1b430
0000000d`f253c7f0 00007ffb`7559295f : 0000000d`00000001 000001b7`cff89828 000001b7`cff739f8 000001b7`cff7f910 :
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
0000000d`f253ca50 00007ffb`7559289a : 0000000d`f253e280 00007ffb`1edb7a18 000001b7`cff73650 00007ffb`1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
0000000d`f253cae0 00007ffb`7557ee58 : 000001b7`cff738e8 0000000d`f253e280 0000000d`f253e200 00007ffb`1edb7a18 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
0000000d`f253cb40 00007ffb`7558b17d : 00000000`0000006b 000001b7`cff73698 000001b7`c9fa0000 00000000`40000062 :
d3d11!CDevice::CreateLayeredChild+0xc88
0000000d`f253cf80 00007ffb`1ed43ade : 000001b7`cff73698 00000000`00000000 000001b7`ca061c10 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
0000000d`f253d0f0 00007ffb`1ed30d83 : 000001b7`cff73748 00000000`00000000 00000000`00000000 000001b7`cff73650 :
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
0000000d`f253e180 00007ffb`1eceda23 : 000001b7`cff73680 000001b7`cff73678 000001b7`cff73678 000001b7`cff73650 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
0000000d`f253e240 00007ffb`7558b950 : 000001b7`cff73650 00000000`00000030 0000000d`f253e370 000001b7`c9fa0000 :
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
0000000d`f253e330 00007ffb`755714f4 : 000001b7`ca04bad0 0000000d`00000009 000001b7`cff72d40 000001b7`ca04c968 :
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
0000000d`f253e520 00007ffb`75571463 : 000001b7`cff72d40 00000000`0000c000 00000000`00000000 00000000`00000001 :
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
0000000d`f253e580 00007ffb`755711e8 : 000001b7`ca04c968 000001b7`cff72d40 00000000`00000438 00000000`00000000 :
d3d11!CDevice::CreatePixelShader_Worker+0x203
0000000d`f253e730 00007ffb`1ed19f85 : 000001b7`ca04bb28 000001b7`00000001 000001b7`ca04bb28 000001b7`ca04bb30 :
d3d11!CDevice::CreatePixelShader+0x28
0000000d`f253e780 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000 0000000d`f253e858 000001b7`cff72d54 :
D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115
0000000d`f253e7f0 00007ff6`7fbd8c3c : 000001b7`ca04bb30 000001b7`cff72d40 00000000`00000438 cdcdcdcd`00000000 : POC_EXEC11+0x1872d
0000000d`f253ea40 00007ff6`7fbd61b8 : 000001b7`ca04bb30 000001b7`c9fdd300 000001b7`00000000 00007ff6`42de0387 : POC_EXEC11+0x18c3c
0000000d`f253ea80 00007ff6`7fbeaa50 : 000001b7`ca04bb30 000001b7`c9fe0030 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8
0000000d`f253ef20 00007ff6`7fbe6e22 : 000001b7`ca006a00 000001b7`ca006a01 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50
0000000d`f253f1c0 00007ff6`7fbe319c : 000001b7`ca006a00 00310043`00000201 00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22
0000000d`f253f5b0 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 : POC_EXEC11+0x2319c
0000000d`f253f7b0 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 000001b7`c9fa3300 00007ff6`0000000a : POC_EXEC11+0x147dd
0000000d`f253f860 00007ff6`7fc833fe : 00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d
0000000d`f253f8a0 00007ff6`7fc832be : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe
0000000d`f253f910 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc32be
0000000d`f253f940 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9
0000000d`f253f970 00007ffb`7b3aced1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
KERNEL32!BaseThreadInitThunk+0x14
0000000d`f253f9a0 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
ntdll!RtlUserThreadStart+0x21


STACK_COMMAND:  ~0s ; .cxr ; kb

THREAD_SHA1_HASH_MOD_FUNC:  8afa9ed70477445bbc2f78d45b744ddd187a1fb5
```

```
THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  787ce9e55cabeb31aced9c79845b30d395d5ea7f

THREAD_SHA1_HASH_MOD:  12643792dd68a375a1d54d10cbd44c347ace88c4

FAULT_INSTR_CODE:  868c8941

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  atidxx64!XdxQueryTlsLookupTable+4bc98

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME: atidxx64

IMAGE_NAME:  atidxx64.dll

DEBUG_FLR_IMAGE_TIMESTAMP:  5e59a28f

FAILURE_BUCKET_ID:  INVALID_POINTER_WRITE_EXPLOITABLE_c0000005_atidxx64.dll!XdxQueryTlsLookupTable

BUCKET_ID:  APPLICATION_FAULT_INVALID_POINTER_WRITE_EXPLOITABLE_atidxx64!XdxQueryTlsLookupTable+4bc98

FAILURE_EXCEPTION_CODE:  c0000005

FAILURE_IMAGE_NAME:  atidxx64.dll

BUCKET_ID_IMAGE_STR:  atidxx64.dll

FAILURE_MODULE_NAME:  atidxx64

BUCKET_ID_MODULE_STR:  atidxx64

FAILURE_FUNCTION_NAME:  XdxQueryTlsLookupTable

BUCKET_ID_FUNCTION_STR:  XdxQueryTlsLookupTable

BUCKET_ID_OFFSET:  4bc98

BUCKET_ID_MODTIMEDATESTAMP:  5e59a28f

BUCKET_ID_MODCHECKSUM:  19151d4

BUCKET_ID_MODVER_STR:  0.0.0.0

BUCKET_ID_PREFIX_STR:  APPLICATION_FAULT_INVALID_POINTER_WRITE_EXPLOITABLE_

FAILURE_PROBLEM_CLASS:  APPLICATION_FAULT

FAILURE_SYMBOL_NAME:  atidxx64.dll!XdxQueryTlsLookupTable

TARGET_TIME:  2020-03-21T18:48:29.000Z

OSBUILD:  18363

OSSERVICEPACK:  329

SERVICEPACK_NUMBER: 0

OS_REVISION: 0

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 10

OSEDITION:  Windows 10 WinNt SingleUserTS

USER_LCID:  0

OSBUILD_TIMESTAMP:  unknown_date

BUILDDATESTAMP_STR:  190318-1202

BUILDLAB_STR:  19h1_release

BUILDOSVER_STR:  10.0.18362.1.amd64fre.19h1_release.190318-1202

ANALYSIS_SESSION_ELAPSED_TIME:  bbfa

ANALYSIS_SOURCE:  UM

FAILURE_ID_HASH_STRING:  um:invalid_pointer_write_exploitable_c0000005_atidxx64.dll!xdxquerytlslookuptable

FAILURE_ID_HASH:  {e90f63d0-92d3-f76d-e643-415c3b3a001b}

Followup:     MachineOwner
---------
```

Timeline

2020-03-31 - Vendor Disclosure

2020-07-14 - Public Release

CREDIT

Discovered by Piotr Bania of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2020-1041

NEXT REPORT
TALOS-2020-1043