Talos Vulnerability Report

TALOS-2020-1040

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

JULY 14, 2020

CVE NUMBER

CVE-2020-6100

Summary

An exploitable memory corruption vulnerability exists in AMD atidxx64.dll graphics driver. A specially crafted pixel shader can cause memory corruption vulnerability. An attacker can provide a specially crafted shader file to trigger this vulnerability. This vulnerability potentially could be triggered from guest machines running virtualization environments (ie. VMware, qemu, VirtualBox etc.) in order to perform guest-to-host escape - as it was demonstrated before (TALOS-2018-0533, TALOS-2018-0568, etc.). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly). We were able to trigger this vulnerability from HYPER-V guest using RemoteFX feature leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process).

Tested Versions

AMD atidxx64.dll (26.20.15019.19000)

Product URLs

http://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 memory corruption problem in AMD graphics driver:

example of pixel shader triggering the bug: ps_4_1 dcl_global_flags refactoringAllowed dcl_constant_buffer cb0[1].xyzw, immediateIndexed dcl_input_ps_siv linear noperspective v0.xy, position dcl_output o0.xyzw dcl_temps 3 … mov o385613824.w, l(), r ret

By modifying the “mov” Output Register operand in the mov instruction attacker is able to trigger a memory corruption vulnerability in the AMD graphics driver. Typically each output register operand should be declared by DLC_OUTPUT instruction. In following example output register is used out of the declared range. Attacker can control the memory address which will be used for write operation (RAX register) by modifying shader bytecode.

```
atidxx64!XdxQueryTlsLookupTable+0x522f1:
00007ffb`695b80e1 099c85a84e0000  or      dword ptr [rbp+rax*4+4EA8h],ebx ss:000001fe`6c2c8808=????????
0:000> r
rax=00000000cccbf000 rbx=0000000000000040 rcx=0000000000000000
rdx=0000000000000000 rsi=0000000000000000 rdi=000001fb38fc7960
rip=00007ffb695b80e1 rsp=000000184fafb5d0 rbp=000001fb38fc7960
 r8=0000000000000080  r9=0000000000000001 r10=0000000000000002
r11=0000000000000000 r12=0000000000000000 r13=0000000000000001
r14=000000184fafb960 r15=0000000000000004
iopl=0         nv up ei ng nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010286
atidxx64!XdxQueryTlsLookupTable+0x522f1:
00007ffb`695b80e1 099c85a84e0000  or      dword ptr [rbp+rax*4+4EA8h],ebx ss:000001fe`6c2c8808=????????
```

stack trace: 0:000> kb # RetAddr : Args to Child : Call Site 00 00007ffb695b7ecd : 000001fb00000040 000001fb38fcc708 0000000000000000 0000000000000000 : atidxx64!XdxQueryTlsLookupTable+0x522f1 01 00007ffb695b71b9 : 0000000000000000 0000000000000000 0000000000000000 0000000000000000 : atidxx64!XdxQueryTlsLookupTable+0x520dd 02 00007ffb695b0b9b : 000001fb00000000 0000000000000000 0000000000000000 0000000000000000 : atidxx64!XdxQueryTlsLookupTable+0x513c9 03 00007ffb695c370e : 0000000000000000 000001fb3907d5f0 0000000000000001 000001fb38fc7960 : atidxx64!XdxQueryTlsLookupTable+0x4adab 04 00007ffb695abd1e : 000001fb3907d5f0 0000000000000000 0000000000000000 000000184fafc870 : atidxx64!XdxQueryTlsLookupTable+0x5d91e 05 00007ffb695abb12 : 000001fb38f31b40 000001fb3907d2c0 000000184fafc870 0000000000000000 : atidxx64!XdxQueryTlsLookupTable+0x45f2e 06 00007ffb69ee1e71 : 0000000000000000 000000184fafc870 000001fb38f31b40 000000184fafc500 : atidxx64!XdxQueryTlsLookupTable+0x45d22 07 00007ffb695ec1ea : 0000000000000000 0000000000000000 000000184fafc870 0000000000000020 : atidxx64!AmdDxGsaFreeCompiledShader+0x910971 08 00007ffb695ec033 : 000001fb3906e590 0000000000000003 0000000000000003 0000000000000000 : atidxx64!AmdDxGsaFreeCompiledShader+0x1acea 09 00007ffb6956d3de : 0000000000000001 0000000000000000 000001fb32c20000 000001fb00000003 : atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33 0a 00007ffb69d8dde5 : 00007ffb69560000 000001fb38ee0208 0000000000000000 ffffffffffffffff : atidxx64!XdxQueryTlsLookupTable+0x75ee 0b 00007ffb69d897f3 : 0000000000000000 000000184fafc780 000001fb3906c540 000001fb346d6b48 : atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5 0c 00007ffb69df4a59 : 0000000000000000 000000184fafc870 000001fb3906bec0 000001fb32cdf3b0 : atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3 0d 00007ffb69581220 : 000001fb32cdf4c8 000001fb34c0f1f0 000001fb32caf3d8 000001fb32cb32a0 : atidxx64!AmdDxGsaFreeCompiledShader+0x823559 0e 00007ffb75588edc : 0000000000000000 000000184fafca60 000001fb32cdf4b8 000001fb32cde498 : atidxx64!XdxQueryTlsLookupTable+0x1b430 0f 00007ffb7559295f : 0000001800000001 000001fb34c0b608 000001fb32cdf4b8 000001fb34c016f0 :

```
d3d11!CPixelShader::CLS::FinalConstruct+0x23c 10 00007ffb7559289a : 000000184fafe3f0 00007ffb1edb7a18 000001fb32cdf100 00007ffb1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3 11 00007ffb7557ee58 : 000001fb32cdf3a8 000000184fafe3f0 000000184fafe370
00007ffb1edb7a18 : d3d11!CLayeredObjectWithCLS::CreateInstance+0x152 12 00007ffb`7558b17d : 00000000`00000036 000001fb`32cdf148 000001fb`32c20000 00000000`40000062 :
d3d11!CDevice::CreateLayeredChild+0xc88 13 00007ffb`1ed43ade : 000001fb`32cdf148 00000000`00000000 000001fb`34c17410 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d 14 00007ffb`1ed30d83 : 000001fb`32cdf1f8 00000000`00000000 00000000`00000000 000001fb`32cdf100 :
D3D11_3SDKLayers!NDebug::CDeviceChild::FinalConstruct+0x82 15 00007ffb`1eceda23 : 000001fb`32cdf130 000001fb`32cdf128 000001fb`32cdf128 000001fb`32cdf100 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167 16 00007ffb`7558b950 : 000001fb`32cdf100 00000000`00000030 00000018`4fafe4e0
000001fb`32c20000 : D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773 17 00007ffb`755714f4 : 000001fb`32cad790 00000018`00000009 000001fb`32cde750
000001fb`32cae628 : d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0 18 00007ffb`75571463 : 000001fb`32cde750 00000000`0000c000 00000000`00000000
00000000`00000001 : d3d11!CDevice::CreateAndRecreateLayeredChild+0x64 19 00007ffb`755711e8 : 000001fb`32cae628 000001fb`32cde750 00000000`00000488 00000000`00000000
: d3d11!CDevice::CreatePixelShader_Worker+0x203 1a 00007ffb`1ed19f85 : 000001fb`32cad7e8 000001fb`00000001 000001fb`32cad7e8 000001fb`32cad7f0 :
d3d11!CDevice::CreatePixelShader+0x28 *** WARNING: Unable to verify checksum for POC_EXEC11.exe 1b 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000
00000018`4fafe9c8 000001fb`32cde764 : D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115 1c 00007ff6`7fbd8c3c : 000001fb`32cad7f0 000001fb`32cde750
00000000`00000488 cdcdcdcd`00000000 : POC_EXEC11+0x1872d 1d 00007ff6`7fbd61b8 : 000001fb`32cad7f0 000001fb`32c5d280 000001fb`00000000 00007ff6`42de0387 :
POC_EXEC11+0x18c3c 1e 00007ff6`7fbeaa50 : 000001fb`32cad7f0 000001fb`32c60030 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8 1f 00007ff6`7fbe6e22 :
000001fb`32c869b0 000001fb`32c86901 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50 20 00007ff6`7fbe319c : 000001fb`32c869b0 00310043`00000201
00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22 21 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 :
POC_EXEC11+0x2319c 22 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 000001fb`32c23300 00007ff6`0000000a : POC_EXEC11+0x147dd 23 00007ff6`7fc833fe :
00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d 24 00007ff6`7fc832be : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe 25 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
POC_EXEC11+0xc32be 26 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9 27 00007ffb`7b3aced1 :
00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14 28 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: 2489

        Key  : Timeline.Process.Start.DeltaSec
        Value: 108


PROCESSES_ANALYSIS: 1

SERVICE_ANALYSIS: 1

STACKHASH_ANALYSIS: 1

TIMELINE_ANALYSIS: 1

Timeline: !analyze.Start
        Name: <blank>
        Time: 2020-03-21T18:13:20.789Z
        Diff: 789 mSec

Timeline: Dump.Current
        Name: <blank>
        Time: 2020-03-21T18:13:20.0Z
        Diff: 0 mSec

Timeline: Process.Start
        Name: <blank>
        Time: 2020-03-21T18:11:32.0Z
        Diff: 108000 mSec

Timeline: OS.Boot
        Name: <blank>
        Time: 2020-03-21T17:31:51.0Z
        Diff: 2489000 mSec


DUMP_CLASS: 2

DUMP_QUALIFIER: 0

FAULTING_IP: 
atidxx64!XdxQueryTlsLookupTable+522f1
00007ffb`695b80e1 099c85a84e0000  or      dword ptr [rbp+rax*4+4EA8h],ebx

EXCEPTION_RECORD:  (.exr -1)
ExceptionAddress: 00007ffb695b80e1 (atidxx64!XdxQueryTlsLookupTable+0x00000000000522f1)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000001
   Parameter[1]: 000001fe6c2c8808
Attempt to write to address 000001fe6c2c8808

FAULTING_THREAD:  00002554

PROCESS_NAME:  POC_EXEC11.exe

FOLLOWUP_IP: 
atidxx64!XdxQueryTlsLookupTable+522f1
00007ffb`695b80e1 099c85a84e0000  or      dword ptr [rbp+rax*4+4EA8h],ebx

WRITE_ADDRESS:  000001fe6c2c8808 

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:  000001fe6c2c8808

WATSON_BKT_PROCSTAMP:  5e1a142e

WATSON_BKT_MODULE:  atidxx64.dll

WATSON_BKT_MODSTAMP:  5e59a28f

WATSON_BKT_MODOFFSET:  580e1

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:  576d53afe83c9dc19b47ba6e73c74c7156aa337c

MODLIST_SHA1_HASH:  d750f006ba2fb2ab3fbce41eead7680b98382016

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 19:13:20.0789

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:    [0x2554]
        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:    [0x2554]
        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:    [0x1bcc]
        TID:    [0x2554]
        Frame:  [0] : atidxx64!XdxQueryTlsLookupTable

LAST_CONTROL_TRANSFER:  from 00007ffb695b7ecd to 00007ffb695b80e1

STACK_TEXT:
00000018`4fafb5d0 00007ffb`695b7ecd : 000001fb`00000040 000001fb`38fcc708 00000000`00000000 00000000`00000000 :
atidxx64!XdxQueryTlsLookupTable+0x522f1
00000018`4fafb660 00007ffb`695b71b9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
atidxx64!XdxQueryTlsLookupTable+0x520dd
00000018`4fafb8d0 00007ffb`695b0b9b : 000001fb`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
atidxx64!XdxQueryTlsLookupTable+0x513c9
00000018`4fafc210 00007ffb`695c370e : 00000000`00000000 000001fb`3907d5f0 00000000`00000001 000001fb`38fc7960 :
atidxx64!XdxQueryTlsLookupTable+0x4adab
00000018`4fafc2c0 00007ffb`695abd1e : 000001fb`3907d5f0 00000000`00000000 00000000`00000000 00000018`4fafc870 :
atidxx64!XdxQueryTlsLookupTable+0x5d91e
00000018`4fafc2f0 00007ffb`695abb12 : 000001fb`38f31b40 000001fb`3907d2c0 00000018`4fafc870 00000000`00000000 :
atidxx64!XdxQueryTlsLookupTable+0x45f2e
00000018`4fafc3d0 00007ffb`69ee1e71 : 00000000`00000000 00000018`4fafc870 000001fb`38f31b40 00000018`4fafc500 :
atidxx64!XdxQueryTlsLookupTable+0x45d22
00000018`4fafc400 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 00000018`4fafc870 00000000`00000020 :
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
00000018`4fafc440 00007ffb`695ec033 : 000001fb`3906e590 00000000`00000003 00000000`00000003 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
00000018`4fafc480 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 000001fb`32c20000 000001fb`00000003 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
00000018`4fafc510 00007ffb`69d8dde5 : 00007ffb`69560000 000001fb`38ee0208 00000000`00000000 ffffffff`ffffffff :
atidxx64!XdxQueryTlsLookupTable+0x75ee
00000018`4fafc550 00007ffb`69d897f3 : 00000000`00000000 00000018`4fafc780 000001fb`3906c540 000001fb`346d6b48 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
00000018`4fafc680 00007ffb`69df4a59 : 00000000`00000000 00000018`4fafc870 000001fb`3906bec0 000001fb`32cdf3b0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
00000018`4fafc820 00007ffb`69581220 : 000001fb`32cdf4c8 000001fb`34c0f1f0 000001fb`32caf3d8 000001fb`32cb32a0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
00000018`4fafc850 00007ffb`75588edc : 00000000`00000000 00000018`4fafca60 000001fb`32cdf4b8 000001fb`32cde498 :
atidxx64!XdxQueryTlsLookupTable+0x1b430
00000018`4fafc960 00007ffb`7559295f : 00000018`00000001 000001fb`34c0b608 000001fb`32cdf4b8 000001fb`34c016f0 :
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
00000018`4fafcbc0 00007ffb`7559289a : 00000018`4fafe3f0 00007ffb`1edb7a18 000001fb`32cdf100 00007ffb`1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
00000018`4fafcc50 00007ffb`7557ee58 : 000001fb`32cdf3a8 00000018`4fafe3f0 00000018`4fafe370 00007ffb`1edb7a18 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
00000018`4fafccb0 00007ffb`7558b17d : 00000000`00000036 000001fb`32cdf148 000001fb`32c20000 00000000`40000062 :
d3d11!CDevice::CreateLayeredChild+0xc88
00000018`4fafd0f0 00007ffb`1ed43ade : 000001fb`32cdf148 00000000`00000000 000001fb`34c17410 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
00000018`4fafd260 00007ffb`1ed30d83 : 000001fb`32cdf1f8 00000000`00000000 00000000`00000000 000001fb`32cdf100 :
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
00000018`4fafe2f0 00007ffb`1eceda23 : 000001fb`32cdf130 000001fb`32cdf128 000001fb`32cdf128 000001fb`32cdf100 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
00000018`4fafe3b0 00007ffb`7558b950 : 000001fb`32cdf100 00000000`00000030 00000018`4fafe4e0 000001fb`32c20000 :
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
00000018`4fafe4a0 00007ffb`755714f4 : 000001fb`32cad790 00000018`00000009 000001fb`32cde750 000001fb`32cae628 :
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
00000018`4fafe690 00007ffb`75571463 : 000001fb`32cde750 00000000`0000c000 00000000`00000000 00000000`00000001 :
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
00000018`4fafe6f0 00007ffb`755711e8 : 000001fb`32cae628 000001fb`32cde750 00000000`00000488 00000000`00000000 :
d3d11!CDevice::CreatePixelShader_Worker+0x203
00000018`4fafe8a0 00007ffb`1ed19f85 : 000001fb`32cad7e8 000001fb`00000001 000001fb`32cad7e8 000001fb`32cad7f0 :
d3d11!CDevice::CreatePixelShader+0x28
00000018`4fafe8f0 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000 00000018`4fafe9c8 000001fb`32cde764 :
D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115
00000018`4fafe960 00007ff6`7fbd8c3c : 000001fb`32cad7f0 000001fb`32cde750 00000000`00000488 cdcdcdcd`00000000 : POC_EXEC11+0x1872d
00000018`4fafebb0 00007ff6`7fbd61b8 : 000001fb`32cad7f0 000001fb`32c5d280 000001fb`00000000 00007ff6`42de0387 : POC_EXEC11+0x18c3c
00000018`4fafebf0 00007ff6`7fbeaa50 : 000001fb`32cad7f0 000001fb`32c60030 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8
00000018`4faff090 00007ff6`7fbe6e22 : 000001fb`32c869b0 000001fb`32c86901 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50
00000018`4faff330 00007ff6`7fbe319c : 000001fb`32c869b0 00310043`00000201 00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22
```

```
00000018`4faff720 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 : POC_EXEC11+0x2319c
00000018`4faff920 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 000001fb`32c23300 00007ff6`0000000a : POC_EXEC11+0x147dd
00000018`4faff9d0 00007ff6`7fc833fe : 00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d
00000018`4faffa10 00007ff6`7fc832be : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe
00000018`4faffa80 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc32be
00000018`4faffab0 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9
00000018`4faffae0 00007ffb`7b3aced1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
KERNEL32!BaseThreadInitThunk+0x14
00000018`4faffb10 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
ntdll!RtlUserThreadStart+0x21


STACK_COMMAND:  ~0s ; .cxr ; kb

THREAD_SHA1_HASH_MOD_FUNC:  db455b736689de60c4c23a4c2697e9c4f0fae1b7

THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  7034d2f81960171b25c391118b283930a8ba1b74

THREAD_SHA1_HASH_MOD:  3c299b252206567cd7b1b690e455f5a3ebdf6b61

FAULT_INSTR_CODE:  a8859c09

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  atidxx64!XdxQueryTlsLookupTable+522f1

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+522f1

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:  522f1

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:  2020-03-21T18:14:26.000Z

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:  10068

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-2020-0983

NEXT REPORT

TALOS-2020-1041