Talos Vulnerability Report

TALOS-2020-1041

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

JULY 14, 2020

CVE NUMBER

CVE-2020-6101

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[2].xyzw, immediateIndexed
dcl_input_ps_siv linear noperspective v0.xy, position
dcl_output o10662625.xyzw
dcl_temps 2
...
```

`DCL_OUTPUT oN[.mask]` is an instruction which declares a shader-output register (where `oN` is an output data register; `N` is an integer that denotes the register number.). By forcing the `N` value to be larger than the typical output register maximum number, it is possible to trigger a memory corruption in AMD driver. An attacker can control the destination memory address by modifying the shader bytecode.

```
0:000> r
rax=000000000000b2e1 rbx=000001dfaf21f718 rcx=000001dfaf21f718
rdx=0000000000000000 rsi=000001dfaf21f908 rdi=000001dfaf2150a0
rip=00007ffb69a1f1ba rsp=000000dd9a3778a0 rbp=0000000000000009
 r8=000001dfaf21f980  r9=000001dfaf1f2a70 r10=000001dfaf21efd0
r11=000001dfaf21fa58 r12=000001dfaf1f2a70 r13=0000000000000000
r14=000001dfaf210ab8 r15=000001dfaf21f5b8
iopl=0         nv up ei pl zr na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
atidxx64!AmdDxGsaFreeCompiledShader+0x44dcba:
00007ffb`69a1f1ba 49899cc698440000 mov     qword ptr [r14+rax*8+4498h],rbx ds:000001df`af26e658=????????????????
```

Stack trace:

```
0:000> kb
 # RetAddr           : Args to Child                                                           : Call Site
00 00007ffb`69d0cc54 : 000001df`af21f5b8 000001df`af20ed90 00000000`00000009 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x44dcba
01 00007ffb`69987b38 : 00000000`00000000 000000dd`9a3779f9 000001df`af21ad88 000001df`af20ed90 :
atidxx64!AmdDxGsaFreeCompiledShader+0x73b754
02 00007ffb`69d13694 : 000001df`af1fef28 000000dd`9a3779f9 00000000`00000006 00000000`0000b2e1 :
atidxx64!AmdDxGsaFreeCompiledShader+0x3b6638
03 00007ffb`69d1317b : 000001df`af21f1a0 000001df`00000009 000001df`0000b2e1 00007ffb`6999e075 :
atidxx64!AmdDxGsaFreeCompiledShader+0x742194
04 00007ffb`699cf012 : 000001df`af21ad88 000001df`af200034 00000000`0000007d 00007ffb`69a25db1 :
atidxx64!AmdDxGsaFreeCompiledShader+0x741c7b
05 00007ffb`699d984c : 000001df`af1fef28 000001df`00000006 000001df`af200030 000001df`af21ad88 :
atidxx64!AmdDxGsaFreeCompiledShader+0x3fdb12
06 00007ffb`69707beb : 000001df`af1fef28 000001df`af1f2a70 000001df`af20ed90 000001df`af21edf8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x40834c
07 00007ffb`696f3c86 : 000001df`af1f2a70 000001df`af1f6fe8 000001df`af1f0398 000001df`af1f2a70 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1366eb
08 00007ffb`696d2e6b : 000001df`af1f2a70 000001df`af1f0398 000000dd`9a378980 000001df`af1f2a70 :
atidxx64!AmdDxGsaFreeCompiledShader+0x122786
09 00007ffb`695f0964 : 00000000`00000001 000000dd`9a378980 000001df`af1f0398 000000dd`9a378980 :
atidxx64!AmdDxGsaFreeCompiledShader+0x10196b
0a 00007ffb`69e28fbf : 00000000`00000000 000000dd`9a378870 000000dd`9a378980 000001df`aee6feb0 : atidxx64!AmdDxGsaFreeCompiledShader+0x1f464
0b 00007ffb`69e0e23b : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x857abf
0c 00007ffb`69e0dd66 : 00000000`00000000 000001df`af1f0080 000001df`aee61b40 000000dd`9a37c610 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83cd3b
0d 00007ffb`69e3ec63 : 000001df`af1f0080 00000000`00000000 000001df`aeec99e0 000000dd`9a37c610 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83c866
0e 00007ffb`69e0dbf4 : 00000000`00000004 000001df`aef07a00 000001df`aeeb6cb0 000001df`aee6fca0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x86d763
0f 00007ffb`69ee1e71 : 00000000`00000000 000000dd`9a37cac0 00000000`00000000 000000dd`9a37c750 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83c6f4
10 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 000000dd`9a37cac0 00000000`00000020 :
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
11 00007ffb`695ec033 : 000001df`af1ee590 00000000`00000003 00000000`00000003 00000000`00000000 : atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
12 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 000001df`a8d80000 000001df`00000003 : atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
13 00007ffb`69d8dde5 : 00007ffb`69560000 000001df`aee10208 00000000`00000000 ffffffff`ffffffff : atidxx64!XdxQueryTlsLookupTable+0x75ee
14 00007ffb`69d897f3 : 00000000`00000000 000000dd`9a37c9d0 000001df`af1ec540 000001df`aa7b48b8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
15 00007ffb`69df4a59 : 00000000`00000000 000000dd`9a37cac0 000001df`af1ebec0 000001df`aab7e170 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
16 00007ffb`69581220 : 000001df`aab7e288 000001df`aec7d430 000001df`a8e14798 000001df`a8e1c6d0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
17 00007ffb`75588edc : 00000000`00000000 000000dd`9a37ccb0 000001df`aab7e278 000001df`aab900d8 : atidxx64!XdxQueryTlsLookupTable+0x1b430
18 00007ffb`7559295f : 000000dd`00000001 000001df`aec79848 000001df`aab7e278 000001df`aec6f930 :
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
19 00007ffb`7559289a : 000000dd`9a37e640 00007ffb`1edb7a18 000001df`aab7dec0 00007ffb`1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
1a 00007ffb`7557ee58 : 000001df`aab7e168 000000dd`9a37e640 000000dd`9a37e5c0 00007ffb`1edb7a18 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
1b 00007ffb`7558b17d : 00000000`0000006b 000001df`aab7df08 000001df`a8d80000 00000000`40000062 : d3d11!CDevice::CreateLayeredChild+0xc88
1c 00007ffb`1ed43ade : 000001df`aab7df08 00000000`00000000 000001df`a8e19d10 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
1d 00007ffb`1ed30d83 : 000001df`aab7dfb8 00000000`00000000 00000000`00000000 000001df`aab7dec0 :
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
1e 00007ffb`1eceda23 : 000001df`aab7def0 000001df`aab7dee8 000001df`aab7dee8 000001df`aab7dec0 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
1f 00007ffb`7558b950 : 000001df`aab7dec0 00000000`00000030 000000dd`9a37e730 000001df`a8d80000 :
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
20 00007ffb`755714f4 : 000001df`a8e12b50 000000dd`00000009 000001df`aab7d590 000001df`a8e139e8 :
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
21 00007ffb`75571463 : 000001df`aab7d590 00000000`0000c000 00000000`00000000 00000000`00000001 :
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
22 00007ffb`755711e8 : 000001df`a8e139e8 000001df`aab7d590 00000000`00000448 00000000`00000000 :
d3d11!CDevice::CreatePixelShader_Worker+0x203
23 00007ffb`1ed19f85 : 000001df`a8e12ba8 000001df`00000001 000001df`a8e12ba8 000001df`a8e12bb0 : d3d11!CDevice::CreatePixelShader+0x28
```

Crash Information

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

```
KEY_VALUES_STRING: 1

        Key  : AV.Fault
        Value: Write

        Key  : Timeline.OS.Boot.DeltaSec
        Value: 3559

        Key  : Timeline.Process.Start.DeltaSec
        Value: 56


PROCESSES_ANALYSIS: 1

SERVICE_ANALYSIS: 1

STACKHASH_ANALYSIS: 1

TIMELINE_ANALYSIS: 1

Timeline: !analyze.Start
        Name: <blank>
        Time: 2020-03-21T18:31:10.264Z
        Diff: 264 mSec

Timeline: Dump.Current
        Name: <blank>
        Time: 2020-03-21T18:31:10.0Z
        Diff: 0 mSec

Timeline: Process.Start
        Name: <blank>
        Time: 2020-03-21T18:30:14.0Z
        Diff: 56000 mSec

Timeline: OS.Boot
        Name: <blank>
        Time: 2020-03-21T17:31:51.0Z
        Diff: 3559000 mSec


DUMP_CLASS: 2

DUMP_QUALIFIER: 0

FAULTING_IP: 
atidxx64!AmdDxGsaFreeCompiledShader+44dcba
00007ffb`69a1f1ba 49899cc698440000 mov     qword ptr [r14+rax*8+4498h],rbx

EXCEPTION_RECORD:  (.exr -1)
ExceptionAddress: 00007ffb69a1f1ba (atidxx64!AmdDxGsaFreeCompiledShader+0x000000000044dcba)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000001
   Parameter[1]: 000001dfaf26e658
Attempt to write to address 000001dfaf26e658

FAULTING_THREAD:  000032d4

PROCESS_NAME:  POC_EXEC11.exe

FOLLOWUP_IP: 
atidxx64!AmdDxGsaFreeCompiledShader+44dcba
00007ffb`69a1f1ba 49899cc698440000 mov     qword ptr [r14+rax*8+4498h],rbx

WRITE_ADDRESS:  000001dfaf26e658 

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:  000001dfaf26e658

WATSON_BKT_PROCSTAMP:  5e1a142e

WATSON_BKT_MODULE:  atidxx64.dll

WATSON_BKT_MODSTAMP:  5e59a28f

WATSON_BKT_MODOFFSET:  4bf1ba

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:  73bd09c01a49b574fbbaf835f054025ec92027e6

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 19:31:10.0264

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:    [0x32d4]
        Frame:  [0] : atidxx64!AmdDxGsaFreeCompiledShader

        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:    [0x32d4]
        Frame:  [0] : atidxx64!AmdDxGsaFreeCompiledShader

        ID:     [0n117]
        Type:   [EXPLOITABLE]
        Class:  Addendum
        Scope:  DEFAULT_BUCKET_ID (Failure Bucket ID prefix)
                BUCKET_ID
        Name:   Add
        Data:   Omit
        PID:    [0x2864]
        TID:    [0x32d4]
        Frame:  [0] : atidxx64!AmdDxGsaFreeCompiledShader

LAST_CONTROL_TRANSFER:  from 00007ffb69d0cc54 to 00007ffb69a1f1ba

STACK_TEXT:  
000000dd`9a3778a0 00007ffb`69d0cc54 : 000001df`af21f5b8 000001df`af20ed90 00000000`00000009 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x44dcba
000000dd`9a377910 00007ffb`69987b38 : 00000000`00000000 000000dd`9a3779f9 000001df`af21ad88 000001df`af20ed90 :
atidxx64!AmdDxGsaFreeCompiledShader+0x73b754
000000dd`9a377970 00007ffb`69d13694 : 000001df`af1fef28 000000dd`9a3779f9 00000000`00000006 00000000`0000b2e1 :
atidxx64!AmdDxGsaFreeCompiledShader+0x3b6638
000000dd`9a3779a0 00007ffb`69d1317b : 000001df`af21f1a0 000001df`00000009 000001df`0000b2e1 00007ffb`6999e075 :
atidxx64!AmdDxGsaFreeCompiledShader+0x742194
000000dd`9a377a60 00007ffb`699cf012 : 000001df`af21ad88 000001df`af200034 00000000`0000007d 00007ffb`69a25db1 :
atidxx64!AmdDxGsaFreeCompiledShader+0x741c7b
000000dd`9a377ac0 00007ffb`699d984c : 000001df`af1fef28 000001df`00000006 000001df`af200030 000001df`af21ad88 :
atidxx64!AmdDxGsaFreeCompiledShader+0x3fdb12
000000dd`9a377c30 00007ffb`69707beb : 000001df`af1fef28 000001df`af1f2a70 000001df`af20ed90 000001df`af21edf8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x40834c
000000dd`9a377ef0 00007ffb`696f3c86 : 000001df`af1f2a70 000001df`af1f6fe8 000001df`af1f0398 000001df`af1f2a70 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1366eb
000000dd`9a3780b0 00007ffb`696d2e6b : 000001df`af1f2a70 000001df`af1f0398 000000dd`9a378980 000001df`af1f2a70 :
atidxx64!AmdDxGsaFreeCompiledShader+0x122786
000000dd`9a378130 00007ffb`695f0964 : 00000000`00000001 000000dd`9a378980 000001df`af1f0398 000000dd`9a378980 :
atidxx64!AmdDxGsaFreeCompiledShader+0x10196b
000000dd`9a378740 00007ffb`69e28fbf : 00000000`00000000 000000dd`9a378870 000000dd`9a378980 000001df`aee6feb0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1f464
000000dd`9a378770 00007ffb`69e0e23b : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x857abf
000000dd`9a3788e0 00007ffb`69e0dd66 : 00000000`00000000 000001df`af1f0080 000001df`aee61b40 000000dd`9a37c610 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83cd3b
000000dd`9a378940 00007ffb`69e3ec63 : 000001df`af1f0080 00000000`00000000 000001df`aeec99e0 000000dd`9a37c610 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83c866
000000dd`9a37c5c0 00007ffb`69e0dbf4 : 00000000`00000004 000001df`aef07a00 000001df`aeeb6cb0 000001df`aee6fca0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x86d763
000000dd`9a37c5f0 00007ffb`69ee1e71 : 00000000`00000000 000000dd`9a37cac0 00000000`00000000 000000dd`9a37c750 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83c6f4
000000dd`9a37c650 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 000000dd`9a37cac0 00000000`00000020 :
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
000000dd`9a37c690 00007ffb`695ec033 : 000001df`af1ee590 00000000`00000003 00000000`00000003 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
000000dd`9a37c6d0 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 000001df`a8d80000 000001df`00000003 :
atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
000000dd`9a37c760 00007ffb`69d8dde5 : 00007ffb`69560000 000001df`aee10208 00000000`00000000 ffffffff`ffffffff :
atidxx64!XdxQueryTlsLookupTable+0x75ee
000000dd`9a37c7a0 00007ffb`69d897f3 : 00000000`00000000 000000dd`9a37c9d0 000001df`af1ec540 000001df`aa7b48b8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
000000dd`9a37c8d0 00007ffb`69df4a59 : 00000000`00000000 000000dd`9a37cac0 000001df`af1ebec0 000001df`aab7e170 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
000000dd`9a37ca70 00007ffb`69581220 : 000001df`aab7e288 000001df`aec7d430 000001df`a8e14798 000001df`a8e1c6d0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
000000dd`9a37caa0 00007ffb`75588edc : 00000000`00000000 000000dd`9a37ccb0 000001df`aab7e278 000001df`aab900d8 :
atidxx64!XdxQueryTlsLookupTable+0x1b430
000000dd`9a37cbb0 00007ffb`7559295f : 000000dd`00000001 000001df`aec79848 000001df`aab7e278 000001df`aec6f930 :
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
000000dd`9a37ce10 00007ffb`7559289a : 000000dd`9a37e640 00007ffb`1edb7a18 000001df`aab7dec0 00007ffb`1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
000000dd`9a37cea0 00007ffb`7557ee58 : 000001df`aab7e168 000000dd`9a37e640 000000dd`9a37e5c0 00007ffb`1edb7a18 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
000000dd`9a37cf00 00007ffb`7558b17d : 00000000`0000006b 000001df`aab7df08 000001df`a8d80000 00000000`40000062 :
d3d11!CDevice::CreateLayeredChild+0xc88
000000dd`9a37d340 00007ffb`1ed43ade : 000001df`aab7df08 00000000`00000000 000001df`a8e19d10 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
000000dd`9a37d4b0 00007ffb`1ed30d83 : 000001df`aab7dfb8 00000000`00000000 00000000`00000000 000001df`aab7dec0 :
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
000000dd`9a37e540 00007ffb`1eceda23 : 000001df`aab7def0 000001df`aab7dee8 000001df`aab7dee8 000001df`aab7dec0 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
000000dd`9a37e600 00007ffb`7558b950 : 000001df`aab7dec0 00000000`00000030 000000dd`9a37e730 000001df`a8d80000 :
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
000000dd`9a37e6f0 00007ffb`755714f4 : 000001df`a8e12b50 000000dd`00000009 000001df`aab7d590 000001df`a8e139e8 :
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
000000dd`9a37e8e0 00007ffb`75571463 : 000001df`aab7d590 00000000`0000c000 00000000`00000000 00000000`00000001 :
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
000000dd`9a37e940 00007ffb`755711e8 : 000001df`a8e139e8 000001df`aab7d590 00000000`00000448 00000000`00000000 :
d3d11!CDevice::CreatePixelShader_Worker+0x203
000000dd`9a37eaf0 00007ffb`1ed19f85 : 000001df`a8e12ba8 000001df`00000001 000001df`a8e12ba8 000001df`a8e12bb0 :
d3d11!CDevice::CreatePixelShader+0x28
000000dd`9a37eb40 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000 000000dd`9a37ec18 000001df`aab7d5a4 :
```

```
D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115
000000dd`9a37ebb0 00007ff6`7fbd8c3c : 000001df`a8e12bb0 000001df`aab7d590 00000000`00000448 cdcdcdcd`00000000 : POC_EXEC11+0x1872d
000000dd`9a37ee00 00007ff6`7fbd61b8 : 000001df`a8e12bb0 000001df`a8dbd280 000001df`00000000 00007ff6`42de0387 : POC_EXEC11+0x18c3c
000000dd`9a37ee40 00007ff6`7fbeaa50 : 000001df`a8e12bb0 000001df`a8dc0030 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8
000000dd`9a37f2e0 00007ff6`7fbe6e22 : 000001df`a8de69a0 000001df`a8de6901 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50
000000dd`9a37f580 00007ff6`7fbe319c : 000001df`a8de69a0 00310043`00000201 00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22
000000dd`9a37f970 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 : POC_EXEC11+0x2319c
000000dd`9a37fb70 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 000001df`a8d83300 00007ff6`0000000a : POC_EXEC11+0x147dd
000000dd`9a37fc20 00007ff6`7fc833fe : 00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d
000000dd`9a37fc60 00007ff6`7fc832be : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe
000000dd`9a37fcd0 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc32be
000000dd`9a37fd00 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9
000000dd`9a37fd30 00007ffb`7b3aced1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
KERNEL32!BaseThreadInitThunk+0x14
000000dd`9a37fd60 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
ntdll!RtlUserThreadStart+0x21


STACK_COMMAND:  ~0s ; .cxr ; kb

THREAD_SHA1_HASH_MOD_FUNC:  50ff80561b4376ebd56ffa97647e759f8cac7ea8

THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  5b8799729a6ae4322f3596b42b121abc34913b7d

THREAD_SHA1_HASH_MOD:  65bfb6ca7c7add101712898ff68806f75d7d3ca7

FAULT_INSTR_CODE:  c69c8949

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  atidxx64!AmdDxGsaFreeCompiledShader+44dcba

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!AmdDxGsaFreeCompiledShader

BUCKET_ID:  APPLICATION_FAULT_INVALID_POINTER_WRITE_EXPLOITABLE_atidxx64!AmdDxGsaFreeCompiledShader+44dcba

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:  AmdDxGsaFreeCompiledShader

BUCKET_ID_FUNCTION_STR:  AmdDxGsaFreeCompiledShader

BUCKET_ID_OFFSET:  44dcba

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!AmdDxGsaFreeCompiledShader

TARGET_TIME:  2020-03-21T18:31:43.000Z

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:  82fd

ANALYSIS_SOURCE:  UM

FAILURE_ID_HASH_STRING:  um:invalid_pointer_write_exploitable_c0000005_atidxx64.dll!amddxgsafreecompiledshader

FAILURE_ID_HASH:  {72016af8-990d-a858-b88f-3efa8bc6aa05}

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-2020-1040

NEXT REPORT

TALOS-2020-1042