secluck Update 000078.md History

1 contributor

108 lines (102 sloc) | 6.88 KB

# ACDSee Photo Studio Pro 2021 - User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x00000000000031aa (Hash=0xd095e754.0xb65df7e2)

## Version

```
ACDSee Photo Studio Studio Professional 2021
Version 14.0 (Build 1705)
Copyright (c) 2020 ACD Systems International Inc.
```

## The bug

```
CommandLine: E:\acdsee\ACDSeePro14.exe e:\acdsee\bugs\id_000078.bmp

************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*
Symbol search path is: srv*
Executable search path is:
ModLoad: 00007ff7`a0810000 00007ff7`a0833000   ACDSeePro14.exe
ModLoad: 00007ffa`1c6a0000 00007ffa`1c890000   ntdll.dll
ModLoad: 00007ffa`14f80000 00007ffa`14ff1000   C:\Windows\System32\verifier.dll
Page heap: pid 0x7604: page heap enabled with flags 0x2.
ModLoad: 00007ffa`1afa0000 00007ffa`1b052000   C:\Windows\System32\KERNEL32.DLL
ModLoad: 00007ffa`19780000 00007ffa`19a23000   C:\Windows\System32\KERNELBASE.dll
(7604.75c8): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007ffa`1c7711dc cc              int     3
0:000> g
ModLoad: 00000001`80000000 00000001`80baf000   C:\Program Files\ACD Systems\ACDSee Pro\14.0\PlugIns\IDE_ACDStd.apl
ModLoad: 00007ffa`1b8e0000 00007ffa`1b932000   C:\Windows\System32\SHLWAPI.dll
ModLoad: 00007ffa`07a10000 00007ffa`07ab9000   C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.18362.476_none_2a2a02a24667b734\COMCTL32.dll
ModLoad: 00007ffa`1b940000 00007ffa`1b9de000   C:\Windows\System32\msvcrt.dll
ModLoad: 00007ffa`1b060000 00007ffa`1b103000   C:\Windows\System32\ADVAPI32.dll
ModLoad: 00007ffa`1c180000 00007ffa`1c4b6000   C:\Windows\System32\combase.dll
ModLoad: 00007ffa`1c060000 00007ffa`1c0f7000   C:\Windows\System32\sechost.dll
ModLoad: 00007ffa`19b60000 00007ffa`19c5a000   C:\Windows\System32\ucrtbase.dll
ModLoad: 00007ffa`1b560000 00007ffa`1b680000   C:\Windows\System32\RPCRT4.dll
ModLoad: 000001e3`9a770000 000001e3`9a890000   C:\Windows\System32\RPCRT4.dll
ModLoad: 00007ffa`1b9e0000 00007ffa`1ba06000   C:\Windows\System32\GDI32.dll
ModLoad: 00007ffa`19c60000 00007ffa`19ce0000   C:\Windows\System32\bcryptPrimitives.dll
ModLoad: 00007ffa`19a90000 00007ffa`19ab1000   C:\Windows\System32\win32u.dll
ModLoad: 00007ffa`1c4c0000 00007ffa`1c654000   C:\Windows\System32\USER32.dll
ModLoad: 00007ffa`1a5b0000 00007ffa`1a744000   C:\Windows\System32\gdi32full.dll
ModLoad: 00007ffa`196e0000 00007ffa`1977e000   C:\Windows\System32\msvcp_win.dll
ModLoad: 00007ffa`1b740000 00007ffa`1b810000   C:\Windows\System32\COMDLG32.dll
ModLoad: 00007ffa`1b680000 00007ffa`1b729000   C:\Windows\System32\shcore.dll
ModLoad: 00007ffa`09ed0000 00007ffa`09f59000   C:\Windows\SYSTEM32\WINSPOOL.DRV
ModLoad: 00007ffa`19610000 00007ffa`19621000   C:\Windows\System32\kernel.appcore.dll
ModLoad: 00007ffa`1a8b0000 00007ffa`1af95000   C:\Windows\System32\SHELL32.dll
ModLoad: 00007ffa`19b10000 00007ffa`19b5a000   C:\Windows\System32\cfgmgr32.dll
ModLoad: 00007ffa`19ac0000 00007ffa`19ae6000   C:\Windows\System32\bcrypt.dll
ModLoad: 00007ffa`18a90000 00007ffa`18aca000   C:\Windows\SYSTEM32\IPHLPAPI.DLL
ModLoad: 00007ffa`153a0000 00007ffa`1548f000   C:\Windows\SYSTEM32\PROPSYS.dll
ModLoad: 00007ffa`19ce0000 00007ffa`1a45e000   C:\Windows\System32\windows.storage.dll
ModLoad: 00007ffa`1b460000 00007ffa`1b524000   C:\Windows\System32\OLEAUT32.dll
ModLoad: 00007ffa`195a0000 00007ffa`195bf000   C:\Windows\System32\profapi.dll
ModLoad: 00007ffa`195c0000 00007ffa`1960a000   C:\Windows\System32\powrprof.dll
ModLoad: 00007ffa`19570000 00007ffa`19580000   C:\Windows\System32\UMPDC.dll
ModLoad: 00007ffa`19af0000 00007ffa`19b07000   C:\Windows\System32\cryptsp.dll
ModLoad: 00007ffa`1a750000 00007ffa`1a8a6000   C:\Windows\System32\ole32.dll
ModLoad: 00007ffa`16460000 00007ffa`166bb000   C:\Windows\SYSTEM32\d3d11.dll
ModLoad: 00007ffa`168a0000 00007ffa`16e60000   C:\Windows\SYSTEM32\d2d1.dll
ModLoad: 00007ffa`18270000 00007ffa`1835b000   C:\Windows\SYSTEM32\dxgi.dll
ModLoad: 00007ffa`1b530000 00007ffa`1b55e000   C:\Windows\System32\IMM32.dll
ModLoad: 00007ffa`052d0000 00007ffa`05473000
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.18362.476_none_17afa4006da19f63\gdiplus.dll
```

```
ModLoad: 00007ffa`0a030000 00007ffa`0a095000   C:\Windows\SYSTEM32\OLEACC.dll
ModLoad: 00007ff9`fe460000 00007ff9`fe467000   C:\Windows\SYSTEM32\MSIMG32.dll
ModLoad: 00007ffa`15ef0000 00007ffa`15f14000   C:\Windows\SYSTEM32\WINMM.dll
ModLoad: 00007ffa`17c40000 00007ffa`17cd9000   C:\Windows\SYSTEM32\UxTheme.dll
ModLoad: 00007ffa`151f0000 00007ffa`151fa000   C:\Windows\SYSTEM32\VERSION.dll
ModLoad: 00007ff9`fbd90000 00007ff9`fbdb8000   C:\Windows\SYSTEM32\VCOMP140.DLL
ModLoad: 00007ffa`181e0000 00007ffa`18200000   C:\Windows\SYSTEM32\dxcore.dll
ModLoad: 00007ffa`15ec0000 00007ffa`15eed000   C:\Windows\SYSTEM32\winmmbase.dll
ModLoad: 000001e3`99550000 000001e3`9957d000   C:\Windows\SYSTEM32\WINMMBASE.dll
(7604.75c8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Program Files\ACD Systems\ACDSee
Pro\14.0\PlugIns\IDE_ACDStd.apl -
IDE_ACDStd!JPEGTransW+0x31aa:
00000001`8018116a 884301          mov     byte ptr [rbx+1],al ds:000001e3`a26cd000=??
0:000> r
rax=0000000000000000 rbx=000001e3a26ccfff rcx=0000000000000010
rdx=0000000000000002 rsi=000001e3a26caf30 rdi=00000000000000ff
rip=00000018018116a rsp=000000a4ef4fe660 rbp=0000000000000001
 r8=0000000000000010  r9=00000000000003e8 r10=000001e3a26ccf80
r11=000000a4ef4fe620 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=000001e3995b0001
iopl=0         nv up ei pl zr na po cy
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010247
IDE_ACDStd!JPEGTransW+0x31aa:
00000001`8018116a 884301          mov     byte ptr [rbx+1],al ds:000001e3`a26cd000=??
0:000> kb
 # RetAddr           : Args to Child                                                   : Call Site
00 00000001`80180d47 : 000001e3`a26caf30 00000000`00000000 00000000`00000000 000000a4`ef4fe790 : IDE_ACDStd!JPEGTransW+0x31aa
*** WARNING: Unable to verify checksum for ACDSeePro14.exe
01 00007ff7`a0811758 : 00007ff7`a082e3e8 00000000`00000000 00000000`00000000 000000a4`ef4fe790 : IDE_ACDStd!JPEGTransW+0x2d87
02 00007ff7`a0811909 : 000000a4`ef4ff7e0 000001e3`98627fe2 00007ff7`a082e3e8 00000000`00000000 : ACDSeePro14!parseFile+0x268
03 00007ff7`a0811b54 : 00000000`00000002 000001e3`98627fb0 00000000`00000000 00000000`00000000 : ACDSeePro14!main+0x149
0:000> .load msec
0:000> !exploitable

!exploitable 1.6.0.0
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x00000000000031aa
(Hash=0xd095e754.0xb65df7e2)

User mode write access violations that are not near NULL are exploitable.
```