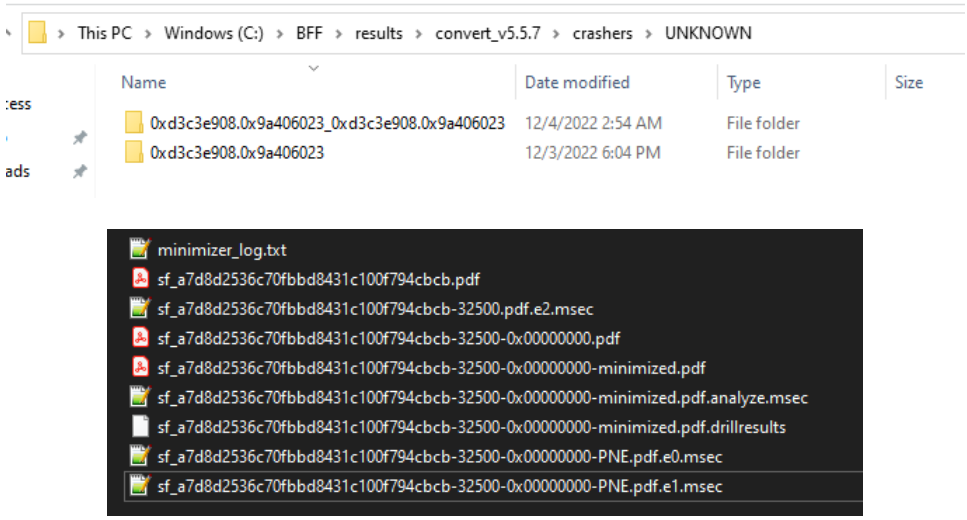
Fuzzing Summary (Choo & Teng)

Windows Fuzzing Task
Vulnerability: Read Access Violation near NULL
We found 2 UNKNOWN crash after running the BFF fuzzer for almost 10 hours.




```
06284be6 3909            cmp     dword ptr [ecx],ecx  ds:002b:00000000=????????
1:017:x86> g;$$Found_with_CERT_BFF_2.8;r;!exploitable -v;q
```

We can see from the picture above, when comparing the dereferencing pointer of ecx, it crashes the program.

This line can be written in C as below:

```c
unsigned long int ecx;

if(*(int*)ecx == ecx){
    //Perform some action
}
```

When we analyze deeper into the result MSEC file, it does not actually crash within the software itself but outside the library. This is because we have checked the address of the crashed instruction located with the debugger and it does not tally. We further confirmed the instructions that crashes the program does not exist within the program itself.

```
Recommended Bug Title: Read Access Violation near NULL starting at Unknown Symbol @ 0x0000000003754be6
called from mscorlib_ni+0x00000000003cd137 (Hash=0xd3c3e908.0x9a406023)
```

After digging through the MSEC files (sf_a7d8d2536c70fbbd8431c100f794cbcb-32500-0x00000000-PNE.pdf.e0.msec), we found out that the called function is from mscorlib.dll file that is located at `C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll`

The stack trace of the crash:

```
 Hash Usage : Stack Trace:
Major+Minor : Unknown
Major+Minor : mscorlib_ni+0x3cd137
Major+Minor : mscorlib_ni+0x3d2e01
Major+Minor : mscorlib_ni+0x3f8604
Major+Minor : mscorlib_ni+0x3f8537
Minor       : mscorlib_ni+0x3f84f4
Minor       : mscorlib_ni+0x3d2d5b
Minor       : clr+0x10556
Minor       : clr!LogHelp_TerminateOnAssert+0x91a
Minor       : clr!LogHelp_TerminateOnAssert+0x6cbb
Minor       : clr!GetPrivateContextsPerfCounters+0x47e7
Minor       : clr!DllCanUnloadNowInternal+0x5c76
Minor       : clr!DllCanUnloadNowInternal+0x5d01
Minor       : clr!DllCanUnloadNowInternal+0x5bf2
Minor       : clr!DllCanUnloadNowInternal+0x5b05
Minor       : clr!DllCanUnloadNowInternal+0x5a91
Minor       : clr!DllCanUnloadNowInternal+0x5b30
Minor       : clr!DllCanUnloadNowInternal+0x5d01
Minor       : clr!DllCanUnloadNowInternal+0x5bf2
Minor       : clr!DllCanUnloadNowInternal+0x5de1
Minor       : clr!GetPrivateContextsPerfCounters+0x4698
Minor       : clr!InstallCustomModule+0x4adb7
Minor       : KERNEL32!BaseThreadInitThunk+0x19
Minor       : ntdll_773c0000!RtlGetAppContainerNamedObjectPath+0x11e
Minor       : ntdll_773c0000!RtlGetAppContainerNamedObjectPath+0xee
Instruction Address: 0x0000000006284d64
```