invalid-email-address xxx

1. tiff file format

1.1 Editor!TMethodImplementationIntercept+0x68f6c2

(92c.134): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=06501ffe ecx=38370010 edx=00000000 esi=1fffe0ce edi=027311b0
eip=00b5acfa esp=0012fb70 ebp=0012fb8c iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210202
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe - Editor!TMethodImplementationIntercept+0x68f6c2:
00b5acfa 8904d9 mov dword ptr [ecx+ebx*8],eax ds:0023:6ab80000=00905a4d
0:000> !exploitable -v

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x6ab80000
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:00b5acfa mov dword ptr [ecx+ebx*8],eax

Exception Hash (Major/Minor): 0x439ec9fa.0x4fa93fdc

Hash Usage : Stack Trace:
Major+Minor : Editor!TMethodImplementationIntercept+0x68f6c2
Major+Minor : Editor!TMethodImplementationIntercept+0x3c74af
Major+Minor : Editor!TMethodImplementationIntercept+0x3c6d80
Major+Minor : Editor!TMethodImplementationIntercept+0x3ce322
Major+Minor : Editor!TMethodImplementationIntercept+0x6b9e7a
Minor : Editor!TMethodImplementationIntercept+0x6ba19c
Minor : Editor!TMethodImplementationIntercept+0x74ed76
Minor : Editor!TMethodImplementationIntercept+0x7455cb
Minor : Editor!TMethodImplementationIntercept+0x30a223
Minor : Editor!TMethodImplementationIntercept+0x3094f8
Minor : Editor!TMethodImplementationIntercept+0x77b249
Minor : kernel32!BaseThreadInitThunk+0x12
Minor : ntdll!__RtlUserThreadStart+0x70
Minor : ntdll!_RtlUserThreadStart+0x1b
Instruction Address: 0x0000000000b5acfa

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor!TMethodImplementationIntercept+0x000000000068f6c2
(Hash=0x439ec9fa.0x4fa93fdc)

1.2 Editor!TMethodImplementationIntercept+0x3c3682

(f48.e08): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000084 ebx=0556ffd8 ecx=ffff4838 edx=02576898 esi=0012fc98 edi=0261f380
eip=0088ecba esp=0012f8b0 ebp=0012f9d8 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210202
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor!TMethodImplementationIntercept+0x3c3682:
0088ecba 66890b mov word ptr [ebx],cx ds:0023:0556ffd8=????
0:000> !exploitable -v

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x556ffd8
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:0088ecba mov word ptr [ebx],cx

Exception Hash (Major/Minor): 0x439ec9fa.0xa53808a3

Hash Usage : Stack Trace:
Major+Minor : Editor!TMethodImplementationIntercept+0x3c3682
Major+Minor : Editor!TMethodImplementationIntercept+0x3c129d
Major+Minor : Editor!TMethodImplementationIntercept+0x3c8fef
Major+Minor : Editor!TMethodImplementationIntercept+0x3c6d80
Major+Minor : Editor!TMethodImplementationIntercept+0x550987
Minor : Editor!TMethodImplementationIntercept+0x550b74
Minor : Editor!TMethodImplementationIntercept+0x550fe5
Minor : Editor!TMethodImplementationIntercept+0x5514a3
Minor : Editor!TMethodImplementationIntercept+0x74eeb9
Minor : Editor!TMethodImplementationIntercept+0x7455cb
Minor : Editor!TMethodImplementationIntercept+0x30a223
Minor : Editor!TMethodImplementationIntercept+0x3094f8
Minor : Editor!TMethodImplementationIntercept+0x77b249
Minor : kernel32!BaseThreadInitThunk+0x12
Minor : ntdll!__RtlUserThreadStart+0x70
Minor : ntdll!_RtlUserThreadStart+0x1b
Instruction Address: 0x000000000088ecba

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor!TMethodImplementationIntercept+0x00000000003c3682
(Hash=0x439ec9fa.0xa53808a3)

1.3 Editor+0x5cd7

(5ac.cbc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0000001f ebx=00c476c4 ecx=000003ff edx=547c3a2e esi=03a12a80 edi=00c84b74
eip=00405cd7 esp=0012fbb8 ebp=0012fbe4 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210202
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor+0x5cd7:
00405cd7 893a mov dword ptr [edx],edi ds:0023:547c3a2e=????????
0:000> !exploitable -v

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\USER32.dll -
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x547c3a2e
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:00405cd7 mov dword ptr [edx],edi

Exception Hash (Major/Minor): 0xcbf27291.0x3aed456e

Hash Usage : Stack Trace:
Major+Minor : Editor+0x5cd7
Major+Minor : Editor!TMethodImplementationIntercept+0x67e84d
Major+Minor : Editor!TMethodImplementationIntercept+0x67e0cf
Major+Minor : Editor!TMethodImplementationIntercept+0x67ea5a
Major+Minor : Editor!TMethodImplementationIntercept+0x603338
Minor : Editor!TMethodImplementationIntercept+0x67d890
Minor : Editor!TMethodImplementationIntercept+0x50e8e2
Minor : Editor!TMethodImplementationIntercept+0x50e981
Minor : Editor!TMethodImplementationIntercept+0x4d5140
Minor : Editor!TMethodImplementationIntercept+0x4d574d
Minor : Editor!TMethodImplementationIntercept+0x282ebe
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!gapfnScSendMessage+0x901
Minor : USER32!DispatchMessageW+0xf
Minor : Editor!TMethodImplementationIntercept+0x3094a8
Minor : Editor!TMethodImplementationIntercept+0x3094eb
Minor : Editor!TMethodImplementationIntercept+0x30981e
Minor : Editor!TMethodImplementationIntercept+0x77b249
Minor : kernel32!BaseThreadInitThunk+0x12
Minor : ntdll!__RtlUserThreadStart+0x70
Minor : ntdll!_RtlUserThreadStart+0x1b
Instruction Address: 0x0000000000405cd7

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor+0x0000000000005cd7 (Hash=0xcbf27291.0x3aed456e)

1.4 Editor+0x576b

(166c.bc4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=05685260 ebx=43324070 ecx=6a474d3a edx=6f312443 esi=05684230 edi=00b9e1ac
eip=0040576b esp=0012fc44 ebp=0012fc58 iopl=0 nv up ei ng nz na po cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210283
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor+0x576b:
0040576b 8911 mov dword ptr [ecx],edx ds:0023:6a474d3a=????????
0:000> !exploitable -v

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\USER32.dll -
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x6a474d3a
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:0040576b mov dword ptr [ecx],edx

Exception Hash (Major/Minor): 0xcbf27291.0x9f4a1b16

Hash Usage : Stack Trace:
Major+Minor : Editor+0x576b
Major+Minor : Editor!TMethodImplementationIntercept+0x6d5f39
Major+Minor : Editor!TMethodImplementationIntercept+0x67792d
Major+Minor : Editor!TMethodImplementationIntercept+0x6778ea
Major+Minor : Editor!TMethodImplementationIntercept+0x679234
Minor : Editor!TMethodImplementationIntercept+0x6b1081
Minor : Editor!TMethodImplementationIntercept+0x5c1c59
Minor : Editor!TMethodImplementationIntercept+0x5c1d29
Minor : Editor!TMethodImplementationIntercept+0x5cd121
Minor : Editor!TMethodImplementationIntercept+0x5cd0f0
Minor : Editor!TMethodImplementationIntercept+0x4d4f78
Minor : Editor!TMethodImplementationIntercept+0x4d574d
Minor : Editor!TMethodImplementationIntercept+0x282ebe
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!gapfnScSendMessage+0x901
Minor : USER32!DispatchMessageW+0xf
Minor : Editor!TMethodImplementationIntercept+0x3094a8
Minor : Editor!TMethodImplementationIntercept+0x3094eb
Minor : Editor!TMethodImplementationIntercept+0x30981e
Minor : Editor!TMethodImplementationIntercept+0x77b249
Minor : kernel32!BaseThreadInitThunk+0x12
Minor : ntdll!__RtlUserThreadStart+0x70
Minor : ntdll!_RtlUserThreadStart+0x1b
Instruction Address: 0x000000000040576b

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor+0x000000000000576b (Hash=0xcbf27291.0x9f4a1b16)

1.5 Editor+0x76af

(1508.161c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=025aec47 ebx=7fc7f8c8 ecx=fffff899 edx=7fc80037 esi=0000027d edi=00000000
eip=004076af esp=0012f85c ebp=0012f86c iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210202
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor+0x76af:
004076af df3c11 fistp qword ptr [ecx+edx] ds:0023:7fc7f8d0=????????????????
0:000> !exploitable -v

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x7fc7f8d0
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:004076af fistp qword ptr [ecx+edx]

Exception Hash (Major/Minor): 0xcbf27291.0x4014e60e

Hash Usage : Stack Trace:
Major+Minor : Editor+0x76af
Major+Minor : Editor!TMethodImplementationIntercept+0x6b50f7
Major+Minor : Editor!TMethodImplementationIntercept+0x3c2604
Major+Minor : Editor!TMethodImplementationIntercept+0x3c129d
Major+Minor : Editor!TMethodImplementationIntercept+0x3c8fef
Minor : Editor!TMethodImplementationIntercept+0x3c6d80
Minor : Editor!TMethodImplementationIntercept+0x550987
Minor : Editor!TMethodImplementationIntercept+0x550b74
Minor : Editor!TMethodImplementationIntercept+0x550fe5
Minor : Editor!TMethodImplementationIntercept+0x5514a3
Minor : Editor!TMethodImplementationIntercept+0x74eeb9
Minor : Editor!TMethodImplementationIntercept+0x7455cb
Minor : Editor!TMethodImplementationIntercept+0x30a223
Minor : Editor!TMethodImplementationIntercept+0x3094f8
Minor : Editor!TMethodImplementationIntercept+0x77b249
Minor : kernel32!BaseThreadInitThunk+0x12
Minor : ntdll!__RtlUserThreadStart+0x70
Minor : ntdll!_RtlUserThreadStart+0x1b
Instruction Address: 0x00000000004076af

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor+0x00000000000076af (Hash=0xcbf27291.0x4014e60e)

1.6 ntdll!RtlpCoalesceFreeBlocks+0x268

(1258.16dc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0561d0f0 ebx=05694228 ecx=547c3a2e edx=48385a56 esi=0561d0e8 edi=002b0000
eip=776c6b0d esp=0012fab8 ebp=0012fae0 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210246
ntdll!RtlpCoalesceFreeBlocks+0x268:
776c6b0d 8b4904 mov ecx,dword ptr [ecx+4] ds:0023:547c3a32=????????
0:000> !exploitable -v

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\KERNELBASE.dll -
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe - *** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\USER32.dll -
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x547c3a32
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Read Access Violation

Faulting Instruction:776c6b0d mov ecx,dword ptr [ecx+4]

Basic Block:
776c6b0d mov ecx,dword ptr [ecx+4]
Tainted Input operands: 'ecx'
776c6b10 mov dword ptr [ebp-14h],edx
776c6b13 mov edx,dword ptr [edx]
776c6b15 cmp edx,ecx
Tainted Input operands: 'ecx'
776c6b17 jne ntdll!rtlpcoalescefreeblocks+0x3bc (776f9a12)
Tainted Input operands: 'ZeroFlag'

Exception Hash (Major/Minor): 0xfc3f1cdb.0xafe50d71

Hash Usage : Stack Trace:
Major+Minor : ntdll!RtlpCoalesceFreeBlocks+0x268
Excluded : ntdll!RtlpFreeHeap+0x1f4
Excluded : ntdll!RtlFreeHeap+0x142
Major+Minor : KERNELBASE!GlobalFree+0x2b
Major+Minor : Editor!TMethodImplementationIntercept+0x6e4512
Major+Minor : Editor!TMethodImplementationIntercept+0x6e45d1
Major+Minor : Editor!TMethodImplementationIntercept+0x6d5f39
Minor : Editor!TMethodImplementationIntercept+0x67792d
Minor : Editor!TMethodImplementationIntercept+0x6778ea
Minor : Editor!TMethodImplementationIntercept+0x679234
Minor : Editor!TMethodImplementationIntercept+0x6b1081
Minor : Editor!TMethodImplementationIntercept+0x5c1c59
Minor : Editor!TMethodImplementationIntercept+0x5c1d29
Minor : Editor!TMethodImplementationIntercept+0x5cd121
Minor : Editor!TMethodImplementationIntercept+0x5cd0f0
Minor : Editor!TMethodImplementationIntercept+0x4d4f78
Minor : Editor!TMethodImplementationIntercept+0x4d574d
Minor : Editor!TMethodImplementationIntercept+0x282ebe
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!gapfnScSendMessage+0x901
Minor : USER32!DispatchMessageW+0xf
Minor : Editor!TMethodImplementationIntercept+0x3094a8
Minor : Editor!TMethodImplementationIntercept+0x3094eb
Minor : Editor!TMethodImplementationIntercept+0x30981e
Minor : Editor!TMethodImplementationIntercept+0x77b249
Minor : kernel32!BaseThreadInitThunk+0x12
Minor : ntdll!__RtlUserThreadStart+0x70
Minor : ntdll!_RtlUserThreadStart+0x1b
Instruction Address: 0x00000000776c6b0d

Description: Data from Faulting Address controls Branch Selection
Short Description: TaintedDataControlsBranchSelection
Exploitability Classification: UNKNOWN
Recommended Bug Title: Data from Faulting Address controls Branch Selection starting at ntdll!RtlpCoalesceFreeBlocks+0x0000000000000268 (Hash=0xfc3f1cdb.0xafe50d71)