1. tga file format

1.1 Editor!TMethodImplementationIntercept+0x54dcec

(254.150c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=056abdc8 ebx=03530b10 ecx=00000000 edx=b9a34641 esi=034c4ac0 edi=0000150c
eip=00a19324 esp=0012fbf0 ebp=0012fc10 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210246
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor!TMethodImplementationIntercept+0x54dcec:
00a19324 ff12 call dword ptr [edx] ds:0023:b9a34641=????????
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: 0xffffffffb9a34641
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Read Access Violation

Faulting Instruction:00a19324 call dword ptr [edx]

Exception Hash (Major/Minor): 0x439ec9fa.0x6ee5cdac

Hash Usage : Stack Trace:
Major+Minor : Editor!TMethodImplementationIntercept+0x54dcec
Major+Minor : Editor!TMethodImplementationIntercept+0x56014c
Major+Minor : Editor!TMethodImplementationIntercept+0x5352b6
Major+Minor : Editor!TMethodImplementationIntercept+0x552c73
Major+Minor : Editor!TMethodImplementationIntercept+0x552da8
Minor : Editor!TMethodImplementationIntercept+0x5510bc
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: 0x0000000000a19324

Description: Read Access Violation on Control Flow
Short Description: ReadAVonControlFlow
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - Read Access Violation on Control Flow starting at
Editor!TMethodImplementationIntercept+0x000000000054dcec (Hash=0x439ec9fa.0x6ee5cdac)

1.2 Editor!TMethodImplementationIntercept+0x57a3b

(10ec.680): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled. eax=5765578f ebx=038d2a81 ecx=0012fbd8 edx=00000000 esi=00000000 edi=00000000
eip=00523073 esp=0012fbd0 ebp=0012fbd8 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210246
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor!TMethodImplementationIntercept+0x57a3b:
00523073 8b08 mov ecx,dword ptr [eax] ds:0023:5765578f=????????
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: 0x5765578f
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Read Access Violation

Faulting Instruction:00523073 mov ecx,dword ptr [eax]

Basic Block:
00523073 mov ecx,dword ptr [eax]
Tainted Input operands: 'eax'
00523075 call dword ptr [ecx+28h]
Tainted Input operands: 'ecx'

Exception Hash (Major/Minor): 0x439ec9fa.0x692a1abd

Hash Usage : Stack Trace:
Major+Minor : Editor!TMethodImplementationIntercept+0x57a3b
Major+Minor : Editor!TMethodImplementationIntercept+0x6d5e78
Major+Minor : Editor!TMethodImplementationIntercept+0x67f82f
Major+Minor : Editor!TMethodImplementationIntercept+0x535250
Major+Minor : Editor!TMethodImplementationIntercept+0x552c73
Minor : Editor!TMethodImplementationIntercept+0x552da8
Minor : Editor!TMethodImplementationIntercept+0x5510bc
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: 0x0000000000523073

Description: Data from Faulting Address controls Code Flow
Short Description: TaintedDataControlsCodeFlow
Exploitability Classification: PROBABLY_EXPLOITABLE
Recommended Bug Title: Probably Exploitable - Data from Faulting Address controls Code Flow starting at
Editor!TMethodImplementationIntercept+0x0000000000057a3b (Hash=0x439ec9fa.0x692a1abd)

1.3 Editor!TMethodImplementationIntercept+0x528a3

(458.1280): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=5229a992 ebx=056a3890 ecx=00000000 edx=00000000 esi=00000000 edi=2d953b2d
eip=0051dedb esp=0012eb54 ebp=0012eb94 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210206
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor!TMethodImplementationIntercept+0x528a3:
0051dedb 8b04b0 mov eax,dword ptr [eax+esi*4] ds:0023:5229a992=????????
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\uxtheme.dll -
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\COMCTL32.dll -
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\kernel32.dll -
Exception Faulting Address: 0x5229a992
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Read Access Violation

Faulting Instruction:0051dedb mov eax,dword ptr [eax+esi*4]

Basic Block:
0051dedb mov eax,dword ptr [eax+esi*4]
Tainted Input operands: 'eax','esi'
0051dede pop esi
0051dedf pop ebx
0051dee0 ret

 Tainted Input operands: 'eax'

Exception Hash (Major/Minor): 0x439ec9fa.0x179818e4
```

Hash Usage : Stack Trace:
Major+Minor : Editor!TMethodImplementationIntercept+0x528a3
Major+Minor : Editor!TMethodImplementationIntercept+0x2109ee
Major+Minor : Editor!TMethodImplementationIntercept+0x2150c0
Major+Minor : Editor!TMethodImplementationIntercept+0x20bc91
Major+Minor : Editor!TMethodImplementationIntercept+0x210748
Minor : Editor!TMethodImplementationIntercept+0x20fd13
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!DefWindowProcW+0x217
Minor : USER32!SendMessageW+0x49
Minor : uxtheme!DrawThemeParentBackgroundEx+0x123
Minor : COMCTL32!GetEffectiveClientRect+0x2c7b
Minor : COMCTL32!GetEffectiveClientRect+0x2ca1
Minor : COMCTL32!GetEffectiveClientRect+0x2e88
Minor : COMCTL32!GetEffectiveClientRect+0x2dba
Minor : COMCTL32!GetEffectiveClientRect+0x2d27
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!PeekMessageA+0x18c
Minor : USER32!CallWindowProcW+0x1b
Minor : Editor!TMethodImplementationIntercept+0x210857
Minor : Editor!TMethodImplementationIntercept+0x2150c0
Minor : Editor!TMethodImplementationIntercept+0x20bc91
Minor : Editor!TMethodImplementationIntercept+0x210748
Minor : Editor!TMethodImplementationIntercept+0x20b8cb
Minor : Editor!TMethodImplementationIntercept+0x21117c
Minor : Editor!TMethodImplementationIntercept+0x20bc91
Minor : Editor!TMethodImplementationIntercept+0x210748
Minor : Editor!TMethodImplementationIntercept+0x20fd13
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!SetPropW+0x1da
Minor : USER32!GetScrollBarInfo+0xfd
Minor : USER32!GetScrollBarInfo+0x16c
Minor : ntdll!KiUserCallbackDispatcher+0x2e
Minor : USER32!RedrawWindow+0xc
Minor : COMCTL32!GetEffectiveClientRect+0x29d7
Minor : COMCTL32!GetEffectiveClientRect+0x28b7
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!PeekMessageA+0x18c
Minor : USER32!CallWindowProcW+0x1b
Minor : Editor!TMethodImplementationIntercept+0x210857
Minor : Editor!TMethodImplementationIntercept+0x210748
Minor : Editor!TMethodImplementationIntercept+0x20fd13
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!gapfnScSendMessage+0x2cf
Minor : USER32!DefWindowProcW+0x217
Minor : USER32!SendMessageW+0x49
Minor : Editor!TMethodImplementationIntercept+0x259660
Minor : Editor!TMethodImplementationIntercept+0x560192
Minor : Editor!TMethodImplementationIntercept+0x5352b6
Minor : Editor!TMethodImplementationIntercept+0x552c73
Minor : Editor!TMethodImplementationIntercept+0x552da8
Minor : Editor!TMethodImplementationIntercept+0x5510bc
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
Instruction Address: 0x000000000051dedb

Description: Data from Faulting Address may be used as a return value
Short Description: TaintedDataReturnedFromFunction
Exploitability Classification: UNKNOWN
Recommended Bug Title: Data from Faulting Address may be used as a return value starting at Editor!TMethodImplementationIntercept+0x00000000000528a3 (Hash=0x439ec9fa.0x179818e4)

1.4 Editor+0x5f91

(edc.107c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000100 ebx=f0f0f0f0 ecx=035c7a90 edx=035c5a30 esi=035c7a90 edi=0278e500
eip=00405f91 esp=0012fcd8 ebp=0012fcf8 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+0x5f91:
00405f91 f00fb023 lock cmpxchg byte ptr [ebx],ah ds:0023:f0f0f0f0=??
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: 0xffffffff0f0f0f0
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:00405f91 lock cmpxchg byte ptr [ebx],ah

Exception Hash (Major/Minor): 0x9287d33d.0xed68e35e

Hash Usage : Stack Trace:
Major+Minor : Editor+0x5f91
Major+Minor : Editor+0x95ff
Major+Minor : Editor!TMethodImplementationIntercept+0x5510bc
Major+Minor : Editor!TMethodImplementationIntercept+0x5514a3
Major+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: 0x0000000000405f91

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor+0x0000000000005f91 (Hash=0x9287d33d.0xed68e35e)

1.5 Editor+0x5ea2

(1088.ce4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=a1b7b7b7 ebx=0002a130 ecx=000003ff edx=0000001f esi=0561cbb0 edi=00c84b74
eip=00405ea2 esp=0012fbac ebp=0012fbd8 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00210206
*** ERROR: Symbol file could not be found. Defaulted to export symbols for Editor.exe -
Editor+0x5ea2:
00405ea2 8938 mov dword ptr [eax],edi ds:0023:a1b7b7b7=????????
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: 0xffffffffa1b7b7b7
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:00405ea2 mov dword ptr [eax],edi

Exception Hash (Major/Minor): 0xcbf27291.0x3a595992

Hash Usage : Stack Trace:
Major+Minor : Editor+0x5ea2
Major+Minor : Editor!TMethodImplementationIntercept+0x6d5e57
Major+Minor : Editor!TMethodImplementationIntercept+0x67f82f
Major+Minor : Editor!TMethodImplementationIntercept+0x535250
Major+Minor : Editor!TMethodImplementationIntercept+0x552c73
Minor : Editor!TMethodImplementationIntercept+0x552da8
Minor : Editor!TMethodImplementationIntercept+0x5510bc
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: 0x0000000000405ea2

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor+0x0000000000005ea2 (Hash=0xcbf27291.0x3a595992)

1.6 Editor+0x5d15

(bdc.650): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=052dfde0 ebx=00c476e4 ecx=20595d23 edx=20595d20 esi=052d01b0 edi=0000fc30
eip=00405d15 esp=0012f538 ebp=0012f678 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+0x5d15:
00405d15 895402f8 mov dword ptr [edx+eax-8],edx ds:0023:25875af8=????????
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: 0x25875af8 First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:00405d15 mov dword ptr [edx+eax-8],edx

Exception Hash (Major/Minor): 0xcbf27291.0x4d6d62b0

Hash Usage : Stack Trace:
Major+Minor : Editor+0x5d15
Major+Minor : Editor!TMethodImplementationIntercept+0x687be8
Major+Minor : Editor!TMethodImplementationIntercept+0x50d8fc
Major+Minor : Editor!TMethodImplementationIntercept+0x50eae2
Major+Minor : Editor!TMethodImplementationIntercept+0x5963f7
Minor : Editor!TMethodImplementationIntercept+0x58200c
Minor : Editor!TMethodImplementationIntercept+0x582827
Minor : Editor!TMethodImplementationIntercept+0x216a99
Minor : Editor!TMethodImplementationIntercept+0x210913
Minor : Editor!TMethodImplementationIntercept+0x2110f9
Minor : Editor!TMethodImplementationIntercept+0x216a32
Minor : Editor!TMethodImplementationIntercept+0x20bc91
Minor : Editor!TMethodImplementationIntercept+0x210748
Minor : Editor!TMethodImplementationIntercept+0x5a0132
Minor : Editor!TMethodImplementationIntercept+0x20fd13
Minor : Editor!TMethodImplementationIntercept+0x6a882
Minor : USER32!gapfnScSendMessage+0x1cf
Minor : USER32!SetPropW+0x1da
Minor : USER32!GetScrollBarInfo+0xfd
Minor : USER32!GetScrollBarInfo+0x16c
Minor : ntdll!KiUserCallbackDispatcher+0x2e
Minor : USER32!MapWindowPoints+0x62
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: 0x0000000000405d15

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at Editor+0x0000000000005d15 (Hash=0xcbf27291.0x4d6d62b0)