

Breakpoint on pop pop ret

61602ADB	5F	POP EDI
61602ADC	5E	POP ESI
61602ADD	C3	RETN

Inspect seh chain

SEH chain of main thread	
Address	SE handler
0012F5B8	EPG.61602ADB
909006EB	*** CORRUPT ENTRY ***

addr of pop pop ret

nop 2 times and jump short 6 bytes

Overflow triggers an exception

Registers (FPU)

ESI 0110FC78  
EDI 6405362C MediaPla.6405362C  
EIP 41414141  
C 0 ES 0023 32bit 0(FFFFFFFF)  
P 1 CS 001B 32bit 0(FFFFFFFF)  
A 0 SS 0023 32bit 0(FFFFFFFF)  
Z 0 DS 0023 32bit 0(FFFFFFFF)  
S 0 FS 003B 32bit 7FFDE000(FFF)  
T 0 GS 0000 NULL  
D 0  
0 0 LastErr ERROR\_SUCCESS (00000000)  
EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)  
ST0 empty  
ST1 empty  
ST2 empty  
ST3 empty  
ST4 empty  
ST5 empty  
ST6 empty  
ST7 empty  
3 2 1 0 ESPUOZDI

0012F470 41414141 AAAA  
0012F474 41414141 AAAA  
0012F478 41414141 AAAA  
0012F47C 41414141 AAAA

Error

Don't know how to continue because memory at address 41414141 is not readable. Try to change EIP or pass exception to program.

OK

When exception is triggered it will pass on execution to the exception handler which was overwritten with pop pop ret

[22:44:16] Access violation when executing [41414141] - use Shift+F7/F8/F9 to pass exception to program

Number of threads running when exception is triggered

Ident	Entry	Data block	Last error	Status	Priority	User time	System time
00000164	7C8106E9	7FFDC000	ERROR_NO_TOKEN (0)	Active	32 + 0	0.0156 s	0.0000 s
000004E8	7C8106E9	7FFDE000	ERROR_SUCCESS (00)	Active	32 + 0	0.0000 s	0.0000 s
000005A4	7C8106E9	7FFDD000	ERROR_SUCCESS (00)	Active	32 + 0	0.0000 s	0.0000 s
000007D0	0047F6BC	7FFDF000	ERROR_SUCCESS (00)	Active	32 + 0	0.3437 s	10.3906 s

Return to 0x0012F5B8

Registers (FPU)

EAX	00000000
ECX	61602ADB EPG.61602ADB
EDX	7C9032BC ntdll.7C9032BC
EBX	00000000
ESP	0012F0A0
EBP	0012F0C0
ESI	00000000
EDI	00000000
EIP	61602ADB EPG.61602ADB

Address	SE handler
0012F0B4	ntdll.7C9032BC
0012F5B8	EPG.61602ADB
909006EB	*** CORRUPT ENTRY ***

0012F5B8	909006EB	00000000	Pointer to next SEH record
0012F5BC	61602ADB	00000000	SE handler
0012F5C0	CCCCCCCC	00000000	
0012F5C4	CCCCCCCC	00000000	
0012F5C8	CCCCCCCC	00000000	
0012F5CC	CCCCCCCC	00000000	
0012F5D0	CCCCCCCC	00000000	
0012F5D4	CCCCCCCC	00000000	
0012F5D8	CCCCCCCC	00000000	
0012F5DC	CCCCCCCC	00000000	
0012F5E0	CCCCCCCC	00000000	
0012F5E4	CCCCCCCC	00000000	
0012F5E8	CCCCCCCC	00000000	
0012F5EC	CCCCCCCC	00000000	
0012F5F0	CCCCCCCC	00000000	
0012F5F4	CCCCCCCC	00000000	

return to instr containing short jmp

Debug instr

ESP 0012F0AC

EBP 0012F0C0

ESI 0012F188

EDI 7C9032A8 ntdll.7C9032A8

EIP 0012F5B8

