PIĄTEK, 3 CZERWCA 2022

Night fuzzing session - IdaPro 6.6 - part 2

Last time during one of the "Night Fuzzing Sessions" I found few bugs in IdaPro 6.6. I decided to continue this adventure but with a 'new approach'. So I changed my *input files*. ;) Below you will find the details about it. Here we go...

This time we'll start here:

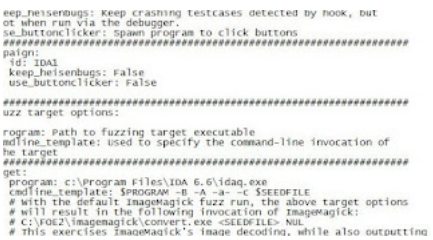
Just like during the previous part - I used similar environment (and settings for the FOE2 fuzzer) as I did before. Only thing I changed here was:

- run Kali VM and

- prepare 'payload/input file' using *msfvenom*.

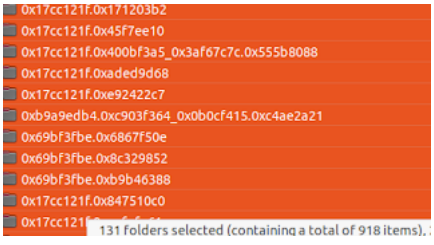
If you're not familiar with *msfvenom* I will always recommend you to read the fantastic manual:

My goal was to prepare a "reverse shell" for various "platforms" (linux/bsd/macos and so on...) and run it in the same way I did before with IdaPro:



TL;DR:

After a while we should be somewhere here:



O MNIE

code16

Cody Sixteen

Wyświetl mój profil

For example:

Case #01:

---<cut>---

(...)
Microsoft (R) Windows Debugger Version 6.11.0001.404 X86
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: "C:\Program Files\IDA 6.6\idaq.exe" -B -A -a- -c C:\FOE2\fuzzdir\campaign_ijatnp\iteration_m_yrvq\foe-crash-l0mnvu\sf_0d75862d5d90166274cc61a363c74828-576.exe
(...)
Executable search path is:
ModLoad: 00090000 003a3000   idaq.exe
(...)
(12a0.1334): 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=07de0ba8 ecx=00000007 edx=00000000 esi=02532fe8 edi=005bc114
eip=77559966 esp=005bbdf4 ebp=005bbdfc iopl=0   nv up ei ng nz ac pe cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000   efl=00010297
msvcrt!memcpy+0x56:
77559966 8b448efc   mov   eax,dword ptr [esi+ecx*4-4] ds:0023:02533000=????????

0:000> r;r;!exploitable -v;kb;r;q
eax=00000000 ebx=07de0ba8 ecx=00000007 edx=00000000 esi=02532fe8 edi=005bc114
eip=77559966 esp=005bbdf4 ebp=005bbdfc iopl=0   nv up ei ng nz ac pe cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000   efl=00010297
msvcrt!memcpy+0x56:
77559966 8b448efc   mov   eax,dword ptr [esi+ecx*4-4] ds:0023:02533000=????????
eax=00000000 ebx=07de0ba8 ecx=00000007 edx=00000000 esi=02532fe8 edi=005bc114
eip=77559966 esp=005bbdf4 ebp=005bbdfc iopl=0   nv up ei ng nz ac pe cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000   efl=00010297
msvcrt!memcpy+0x56:
77559966 8b448efc   mov   eax,dword ptr [esi+ecx*4-4] ds:0023:02533000=????????

!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
Exception Faulting Address: 0x2533000
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Read Access Violation

Faulting Instruction:77559966 mov eax,dword ptr [esi+ecx*4-4]

Basic Block:
  77559966 mov eax,dword ptr [esi+ecx*4-4]
    Tainted Input operands: 'ecx','esi'
  7755996a mov dword ptr [edi+ecx*4-4],eax
    Tainted Input operands: 'eax','ecx'
  7755996e lea eax,[ecx*4]
    Tainted Input operands: 'ecx'
  77559975 add esi,eax
    Tainted Input operands: 'eax','esi'
  77559977 add edi,eax
    Tainted Input operands: 'eax'
  77559979 jmp dword ptr msvcrt!memcpy+0xa8 (775599b8)[edx*4]

Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b

 Hash Usage : Stack Trace:
Major+Minor : msvcrt!memcpy+0x56
Major+Minor : dbghelp!StackWalk64+0x1bba
Major+Minor : dbghelp!SymGetModuleInfoW64+0x549
Major+Minor : dbghelp!FindExecutableImage+0x80e
Major+Minor : dbghelp!StackWalk64+0x2a85

Minor : dbghelp!StackWalk64+0x2cff

Minor : dbghelp!SymLoadModuleEx+0x44

Minor : dbghelp!SymLoadModule64+0x23

Minor : pdb+0x1a8d7

Minor : IDA!run_plugin+0x3a

Minor : dbg+0x8277

Minor : dbg+0x9f2f

Minor : SYSFER+0x45b1b

Minor : SYSFER+0x45b1b

Minor : SYSFER+0x45a1c

Minor : idaq+0x70000

Minor : idaq+0x70000

Minor : idaq+0x70000

Minor : dbg+0xa175

Instruction Address: 0x0000000077559966

Description: Data from Faulting Address controls subsequent Write Address

Short Description: TaintedDataControlsWriteAddress

Exploitability Classification: PROBABLY_EXPLOITABLE

Recommended Bug Title: Probably Exploitable - Data from Faulting Address controls subsequent Write Address starting at msvcrt!memcpy+0x0000000000000056 (Hash=0x17cc121f.0x62867b4b)

The data from the faulting address is later used as the target for a later write.

ChildEBP RetAddr Args to Child

WARNING: Stack unwind information not available. Following frames may be wrong.

005bbdfc 66345b61 005bc114 02532fe8 0000001c msvcrt!memcpy+0x56

005bbe10 66341059 07de0ba8 00000000 02520000 dbghelp!StackWalk64+0x1bba

005bc1bc 66368036 07de0ba8 00000002 00000000 dbghelp!SymGetModuleInfoW64+0x549

005bc1d4 66346a2c 07de0ba8 3be9e1ee 00000000 dbghelp!FindExecutableImage+0x80e

005bc664 66346ca6 beeffeed 07ddb518 00400000 dbghelp!StackWalk64+0x2a85

005bcac8 66363a0e beeffeed 07ddb430 00000000 dbghelp!StackWalk64+0x2cff

005bcb28 66363aa4 beeffeed 00000000 07ddb430 dbghelp!SymLoadModuleEx+0x44

005bcb54 70cea8d7 beeffeed 00000000 02f74320 dbghelp!SymLoadModule64+0x23

005bcc28 66ad515a 00000001 00000010 03108d70 pdb+0x1a8d7

005bceb0 726a8277 03108d70 0000004a 00000001 IDA!run_plugin+0x3a

005bcee0 726a9f2f 66bff840 00000000 3bf980a6 dbg+0x8277

005bcf04 753d5b1b 00000006 753d5b1b 0000077f dbg+0x9f2f

005bcf0c 753d5b1b 0000077f 031596a0 3fe84430 SYSFER+0x45b1b

005bcf44 753d5a1c 00000006 3fe844c4 0000000f SYSFER+0x45b1b

005bcfc0 00100000 00001000 00000000 00000010 SYSFER+0x45a1c

005bd0b0 00100000 00001000 00100000 00001000 idaq+0x70000

005bd0b8 00100000 00001000 00000000 00000010 idaq+0x70000

005bd174 726aa175 66bff840 000000e8 031597c0 idaq+0x70000

00000000 00000000 00000000 00000000 00000000 dbg+0xa175

eax=00000000 ebx=07de0ba8 ecx=00000007 edx=00000000 esi=02532fe8 edi=005bc114

eip=77559966 esp=005bbdf4 ebp=005bbdfc iopl=0 nv up ei ng nz ac pe cy

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010297

msvcrt!memcpy+0x56:

77559966 8b448efc mov eax,dword ptr [esi+ecx*4-4] ds:0023:02533000=????????

---<cut>---

Next case below.

Case #02:

---<cut>---

(...)

Microsoft (R) Windows Debugger Version 6.11.0001.404 X86

Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: "C:\Program Files\IDA 6.6\idaq.exe" -B -A -a- -c C:\FOE2\fuzzdir\campaign_ijatnp\iteration_uw_mli\foe-crash-reinn3\sf_0d75862d5d90166274cc61a363c74828-492.exe

(...)

Executable search path is:

ModLoad: 013c0000 016d3000 idaq.exe

(...)

(15a8.12b8): Access violation - code c0000005 (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

eax=06bac1fc ebx=08250ba8 ecx=00000007 edx=00000000 esi=06bac1e0 edi=0025be54

eip=77559dbd esp=0025bb34 ebp=0025bb3c iopl=0 nv up ei ng nz ac pe cy

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010297

msvcrt!malloc+0xcf:

77559dbd 8b448ee4 mov eax,dword ptr [esi+ecx*4-1Ch] ds:0023:06bac1e0=????????

0:000> r;r;!exploitable -v;kb;r;q

eax=06bac1fc ebx=08250ba8 ecx=00000007 edx=00000000 esi=06bac1e0 edi=0025be54

eip=77559dbd esp=0025bb34 ebp=0025bb3c iopl=0 nv up ei ng nz ac pe cy

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010297

msvcrt!malloc+0xcf:

77559dbd 8b448ee4 mov eax,dword ptr [esi+ecx*4-1Ch] ds:0023:06bac1e0=????????

eax=06bac1fc ebx=08250ba8 ecx=00000007 edx=00000000 esi=06bac1e0 edi=0025be54

eip=77559dbd esp=0025bb34 ebp=0025bb3c iopl=0 nv up ei ng nz ac pe cy

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010297

msvcrt!malloc+0xcf:

77559dbd 8b448ee4 mov eax,dword ptr [esi+ecx*4-1Ch] ds:0023:06bac1e0=????????

!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

Exception Faulting Address: 0x6bac1e0

First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)

Exception Sub-Type: Read Access Violation

Faulting Instruction:77559dbd mov eax,dword ptr [esi+ecx*4-1ch]

Basic Block:

77559dbd mov eax,dword ptr [esi+ecx*4-1ch]

Tainted Input operands: 'ecx','esi'

77559dc1 mov dword ptr [edi+ecx*4-1ch],eax

Tainted Input operands: 'eax','ecx'

77559dc5 jmp msvcrt!memset+0x8a (7755981a)

Exception Hash (Major/Minor): 0xa95bda97.0x1ca78871

Hash Usage : Stack Trace:

Excluded : msvcrt!malloc+0xcf

Major+Minor : dbghelp!StackWalk64+0x1bba

Major+Minor : dbghelp!SymGetModuleInfoW64+0x549

Major+Minor : dbghelp!FindExecutableImage+0x80e

Major+Minor : dbghelp!StackWalk64+0x2a85

Major+Minor : dbghelp!StackWalk64+0x2cff

Minor : dbghelp!SymLoadModuleEx+0x44

Minor : dbghelp!SymLoadModule64+0x23

Minor : pdb+0x1a8d7

Minor : IDA!run_plugin+0x3a

Minor : dbg+0x8277

Minor : dbg+0x9f2f

Minor : SYSFER+0x45b1b

Minor : SYSFER+0x45b1b

Minor : SYSFER+0x45a1c

Instruction Address: 0x0000000077559dbd

Description: Data from Faulting Address controls subsequent Write Address

Short Description: TaintedDataControlsWriteAddress

Exploitability Classification: PROBABLY_EXPLOITABLE

Recommended Bug Title: Probably Exploitable - Data from Faulting Address controls subsequent Write Address starting at msvcrt!malloc+0x00000000000000cf called from dbghelp!StackWalk64+0x0000000000001bba (Hash=0xa95bda97.0x1ca78871)

The data from the faulting address is later used as the target for a later write.

ChildEBP RetAddr Args to Child

WARNING: Stack unwind information not available. Following frames may be wrong.

0025bb3c 679a5b61 0025be54 06bac1e0 0000001c msvcrt!malloc+0xcf

0025bb50 679a1059 08250ba8 00000000 06790000 dbghelp!StackWalk64+0x1bba

0025befc 679c8036 08250ba8 00000002 00000000 dbghelp!SymGetModuleInfoW64+0x549

0025bf14 679a6a2c 08250ba8 4794d435 00000000 dbghelp!FindExecutableImage+0x80e

0025c3a4 679a6ca6 beeffeed 0824b518 00400000 dbghelp!StackWalk64+0x2a85

0025c808 679c3a0e beeffeed 0824b430 00000000 dbghelp!StackWalk64+0x2cff

0025c868 679c3aa4 beeffeed 00000000 0824b430 dbghelp!SymLoadModuleEx+0x44

0025c894 6a26a8d7 beeffeed 00000000 033aa130 dbghelp!SymLoadModule64+0x23

0025c968 6677515a 00000001 00000010 03359768 pdb+0x1a8d7

0025cbf0 70ce8277 03359768 0000004a 00000001 IDA!run_plugin+0x3a

0025cc20 70ce9f2f 6689f840 00000000 4795787b dbg+0x8277

0025cc44 753d5b1b 00000006 753d5b1b ffffffffe dbg+0x9f2f

0025cc4c 753d5b1b ffffffffe 0333aa21 47653451 SYSFER+0x45b1b

0025cc84 753d5a1c 00000006 47653425 0000000f SYSFER+0x45b1b

0025ccfc 00000000 00100000 00001000 00000000 SYSFER+0x45a1c

eax=06bac1fc ebx=08250ba8 ecx=00000007 edx=00000000 esi=06bac1e0 edi=0025be54

eip=77559dbd esp=0025bb34 ebp=0025bb3c iopl=0 nv up ei ng nz ac pe cy

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010297

msvcrt!malloc+0xcf:

77559dbd 8b448ee4 mov eax,dword ptr [esi+ecx*4-1Ch] ds:0023:06bac1e0=????????

---<cut>---

Another variant below.

Case #03:

---<cut>---

(...)

Microsoft (R) Windows Debugger Version 6.11.0001.404 X86

Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: "C:\Program Files\IDA 6.6\idaq.exe" -B -A -a- -c C:\FOE2\fuzzdir\campaign_egm_o8\iteration_j1fril\foe-crash-oxqtdm\sf_76ffd62a1f8250f56b56d8aa211b31a9-252

(...)

Executable search path is:

ModLoad: 000f0000 00403000 idaq.exe

(...)

ModLoad: 69020000 6904c000 C:\Program Files\IDA 6.6\loaders\macho.ldw

(1594.1f2c): Access violation - code c0000005 (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

eax=03b8bba0 ebx=0a00001c ecx=02800007 edx=00000000 esi=f9b8bb84 edi=086a0020

eip=68ee1ed7 esp=0050d234 ebp=0050d23c iopl=0 nv up ei pl nz ac pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010216

MSVCR100!memcpy+0x57:

68ee1ed7 f3a5 rep movs dword ptr es:[edi],dword ptr [esi]

0:000> r;r;!exploitable -v;kb;r;q

eax=03b8bba0 ebx=0a00001c ecx=02800007 edx=00000000 esi=f9b8bb84 edi=086a0020

eip=68ee1ed7 esp=0050d234 ebp=0050d23c iopl=0 nv up ei pl nz ac pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010216

MSVCR100!memcpy+0x57:

68ee1ed7 f3a5 rep movs dword ptr es:[edi],dword ptr [esi]

eax=03b8bba0 ebx=0a00001c ecx=02800007 edx=00000000 esi=f9b8bb84 edi=086a0020

eip=68ee1ed7 esp=0050d234 ebp=0050d23c iopl=0 nv up ei pl nz ac pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010216

MSVCR100!memcpy+0x57:

68ee1ed7 f3a5 rep movs dword ptr es:[edi],dword ptr [esi]

!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

Exception Faulting Address: 0xffffffff9b8bb84

First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)

Exception Sub-Type: Read Access Violation

Faulting Instruction:68ee1ed7 rep movs dword ptr es:[edi],dword ptr [esi]

Exception Hash (Major/Minor): 0x37d7dcd9.0xba787c31

Hash Usage : Stack Trace:

Major+Minor : MSVCR100!memcpy+0x57

Major+Minor : macho+0xd468

Major+Minor : macho+0x106e9

Instruction Address: 0x0000000068ee1ed7

Description: Read Access Violation on Block Data Move

Short Description: ReadAVonBlockMove

Exploitability Classification: PROBABLY_EXPLOITABLE

Recommended Bug Title: Probably Exploitable - Read Access Violation on Block Data Move starting at MSVCR100!memcpy+0x0000000000000057 (Hash=0x37d7dcd9.0xba787c31)

This is a read access violation in a block data move, and is therefore classified as probably exploitable.

ChildEBP RetAddr Args to Child

WARNING: Stack unwind information not available. Following frames may be wrong.

0050d23c 6902d468 086a0020 f9b8bb84 0a00001c MSVCR100!memcpy+0x57

0050d26c 690306e9 f9b8bb84 0a00001c 6dc29131 macho+0xd468

00000000 00000000 00000000 00000000 00000000 macho+0x106e9

eax=03b8bba0 ebx=0a00001c ecx=02800007 edx=00000000 esi=f9b8bb84 edi=086a0020

eip=68ee1ed7 esp=0050d234 ebp=0050d23c iopl=0   nv up ei pl nz ac pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000   efl=00010216

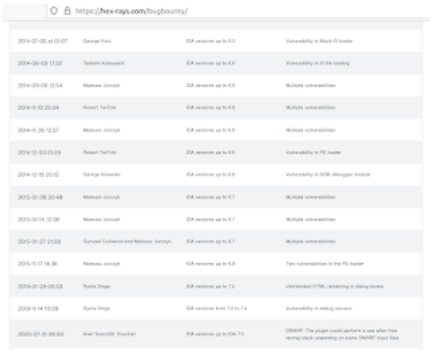
MSVCR100!memcpy+0x57:

68ee1ed7 f3a5   rep movs dword ptr es:[edi],dword ptr [esi]

---<cut>---

I think it should be enough to start your own 'Night Fuzzing Session' ;)

"Probably" *nihil novi* here... ;>



... "but" maybe you'll find it useful. ;)

If you'll have any questions or comments - feel free to ping me.

Have a nice weekend!

Cheers

Posted by code16 at 16:20

Labels: debug, fuzz, notes, RE, writeup

Brak komentarzy:

Prześlij komentarz

Wpisz komentarz

Nowszy post Strona główna Starszy post

Subskrybuj: Komentarze do posta (Atom)